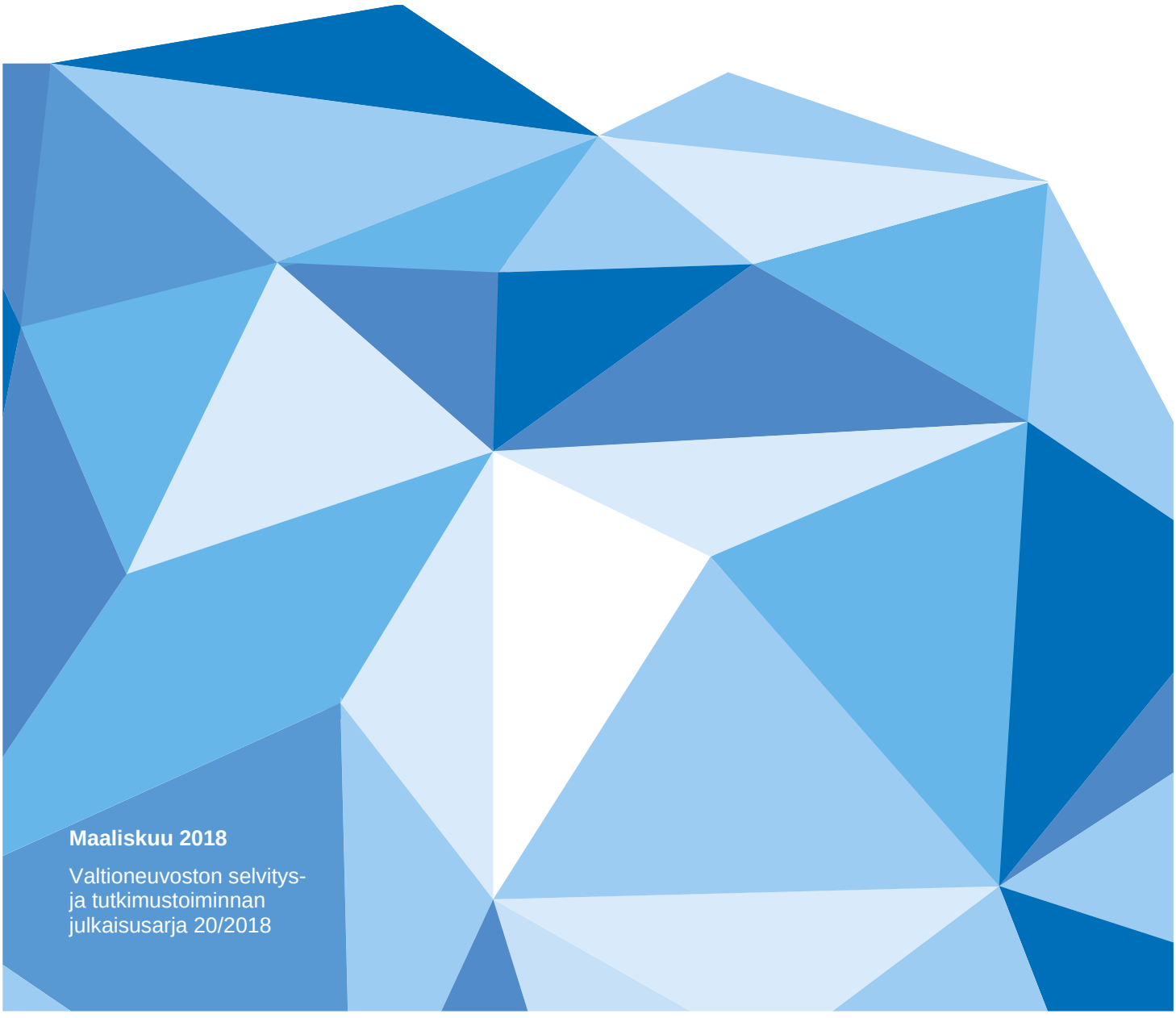
VALTIONEUVOSTON
SELVITYS- JA TUTKIMUSTOIMINTA

Suomi Reima, Koskinen Jani, Haukola Timo, Ahvenjärvi Samu, Andersson Jenna, Hartikainen Pauliina, Karhunen Joonas, Kulta Lotta, Niemimaa Marko, Pitkänen Jari, Turunen Samu, Wallgren Wanda

Digiwars – Keeping the Force

Digitaalisten hyödykkeiden ja liiketoimintamallien luotettavuuden parantaminen – parhaiden käytäntöjen määrittely



Maaliskuu 2018

Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 20/2018

KUVAILULEHTI

Julkaisija ja julkaisuaika	Valtioneuvoston kanslia, 23.03.2018
Tekijät	Suomi Reima, Koskinen Jani, Haukola Timo, Ahvenjärvi Samu, Andersson Jenna, Hartikainen Pauliina, Karhunen Joonas, Kulta Lotta, Niemimaa Marko, Pitkänen Jari, Turunen Samu, Wallgren Wanda
Julkaisun nimi	DIGIWARS – KEEPING THE FORCE Digitaalisten hyödykkeiden ja liiketoimintamallien luotettavuuden parantaminen – parhaiden käytäntöjen määrittely
Julkaisusarjan nimi ja numero	Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 20/2018
Asiasanat	Digitaalinen hyödyke, tietoturvapalvelu, avoin data, avoimet rajapinnat, sertifikaatti, vastuullisuus, parhaat käytännöt
Julkaisuaika	Maaliskuu 2018 **Sivuja**151 **Kieli** Suomi

Tiivistelmä

Suomi on toistaiseksi menestynyt hyvin yhteiskunnan digitalisoimisessa. Kehitettävää kuitenkin riittää, sillä kotimaassa digitalisaation mahdollisuuksia on hyödynnetty vasta pieneltä osalta, ja muutamaa poikkeusta lukuun ottamatta suuret digitaaliset vientimenestykset maailman markkinoille puuttuvat.

Ihmisten haluun omaksua uutta teknologiaa vaikuttaa ratkaisevasti ellei suorastaan kriittisesti heidän luottamukseensa tätä tekniikkaa kohtaan. Luottamus ansaitaan yleensä hitaasti, ja se on äärimmäisen helppo menettää. Kansalaisten luottamuksen ansaitsemiseksi kaikkien digitaalisten palveluiden tuottajien ja tarjoajien pitää ponnistella päivittäin. Luottamus ansaitaan johdonmukaisella ja ennustettavalla toiminnalla. Jos nämä eivät ole kunnossa, mitkään temput eivät auta. Kuitenkin digitaalisilla palvelujen tuottajilla on käytettävissään useita valmiita tekniikoita ja toimintatapoja luotettavuuden osoittamiseen. Näihin kuuluvat julkaistut tietoturvakäytännöt sekä ansaitut ja esitellyt laatua kuvaavat sertifikaatit. Tässä tutkimuksessa arvioidaan erilaisten luottamusta herättävien toimenpiteiden vaikuttavuutta.

Datan avoin julkaiseminen ja lisäarvon tuottaminen tähän dataan ovat keinoja tuottaa vaurautta ja hyvinvointia digitaalisessa yhteiskunnassa. Vain käytössä oleva data tuottaa lisäarvoa. Tälläkin rintamalla on paljon tehtävää, sillä avoimen datan potentiaalista on otettu käyttöön kaikkialla maailmassa vasta vain murto-osa. Avoimen datan hyödyntämisessä, kuten myös luottamuksen ansaitsemisessa, on muistettava, että kyse on elämäntavasta ja asenteesta, ei vain joukosta tekniikoita ja toimintatapoja. Tässä tutkimuksessa etsitään ja esitellään keinoja, joilla datan hyödyntämistä avoimena voidaan tehostaa entisestään.

Sekä avointa dataa että digitalisaatiota ja näihin kohdistuvaa luottamusta pyritään tukemaan laajalla ja osin melko monimutkaisella lainsäädännöllä. Tutkimus pyrkii myös antamaan kuvan regulaatioon liittyvistä mahdollisuuksista ja rajoitteista luottamuksen rakentamista ja avoimen datan hyödyntämistä koskevassa työssä.

Liite 1 Verkkokyselyssä esitetyt väittämät ja kysymykset

Liite 2 Haastatteluissa käsitellyt teemat ja tutkimusta varten haastatellut asiantuntijat

Tämä julkaisu on toteutettu osana valtioneuvoston vuoden 2016 selvitys- ja tutkimussuunnitelman toimeenpanoa (tietokayttoon.fi).

PRESENTATIONSBLAD

Utgivare & utgivningsdatum	Statsrådets kansli, 26.03.2018
Författare	Suomi Reima, Koskinen Jani, Haukola Timo, Ahvenjärvi Samu, Andersson Jenna, Hartikainen Pauliina, Karhunen Joonas, Kulta Lotta, Niemimaa Marko, Pitkänen Jari, Turunen Samu, Wallgren Wanda
Publikationens namn	DIGIWARS – KEEPING THE FORCE Förbättring av tillförlitligheten i digitala nyttigheter och affärsmodeller – definition av bästa praxis
Publikationsseriens namn och nummer	Publikationsserie för statsrådets utrednings- och forskningsverksamhet 20/2018
Nyckelord	Digital nyttighet, dataskyddstjänst, öppna data, öppna gränssnitt, certifikat, ansvarsfullhet, bästa praxis
Utgivningsdatum	Mars 2018 **Sidantal** 151 **Språk** Finska

Sammandrag

Finland har hittills lyckats bra med digitaliseringen av samhället. Det finns emellertid mycket kvar att utveckla. I Finland har digitaliseringens möjligheter endast till en liten del utnyttjats, och frånsett några få undantag har vi inte haft några stora digitala exportframgångar på världsmarknaderna.

Människans vilja att tillägna sig ny teknologi påverkas på ett avgörande om inte direkt kritiskt sätt av hennes förtroende för denna teknik. Förtroende tar i allmänhet lång tid att tjäna in, och det är extremt lätt att förlora. Alla digitala tjänster måste anstränga sig dagligen för att förtjäna medborgarnas förtroende. Förtroende förtjänas genom ett konsekvent och förutsägbart beteende. Om förutsättningarna saknas, hjälper inga knep. Ändå har de digitala tjänsterna tillgång till ett stort antal färdiga tekniker och metoder som de kan använda för att visa sin tillförlitlighet. Dit hör till exempel publicerade dataskyddsrutiner samt förtjänade och uppvisade kvalitetscertifikat. I denna studie bedöms effektiviteten hos olika förtroendeskapande åtgärder.

Öppet offentliggörande av data och produktion av mervärde i dessa data är metoder för att producera välstånd och välfärd i det digitala samhället. Endast data som sätts i arbete producerar mervärde. Även på det området finns det mycket att göra, eftersom endast en bråkdel av potentialen i öppna data har tagits i bruk i världen som helhet. Vid utnyttjade av öppna data måste man, liksom vid intjänande av förtroende, minnas att det handlar om levnadssätt och attityder, inte bara om en samling tekniker och verksamhetssätt. I denna studie söker vi finna och presentera metoder för att ytterligare effektivisera utnyttjandet av öppna data.

Såväl öppna data som digitalisering och förtroendet för dessa söker samhället stödja genom omfattande och delvis ganska komplicerad lagstiftning. Studien söker även ge en bild av regleringarnas möjligheter och begränsningar i arbetet med att bygga förtroende och utnyttja öppna data.

Bilaga 1 Verkkokyselyssä esitetyt väittämät ja kysymykset

Bilaga 2 Haastatteluissa käsitellyt teemat ja tutkimusta varten haastatellut asiantuntijat

Den här publikation är en del i genomförandet av statsrådets utrednings- och forskningsplan för 2016 (tietokayttoon.fi/sv).

DESCRIPTION

Publisher and release date	Prime Minister´s Office, 26.03.2018
Authors	Suomi Reima, Koskinen Jani, Haukola Timo, Ahvenjärvi Samu, Andersson Jenna, Hartikainen Pauliina, Karhunen Joonas, Kulta Lotta, Niemimaa Marko, Pitkänen Jari, Turunen Samu, Wallgren Wanda
Title of publication	DIGIWARS – KEEPING THE FORCE Improving trust in digital assets and business models – determining best practices
Name of series and number of publication	Publications of the Government´s analysis, assessment and research activities 20/2018
Keywords	Digital asset, data security services, open data, open interfaces, certificate, responsibility, best practices
Release date	March 2018 **Pages** 151 **Language** Finnish

Abstract

Finland has so far been reasonably successful in the digitalisation of society. However, there are still areas that need to be developed further: domestically, the opportunities of digitalisation remain largely unexploited, and in the global export arena major digital success stories are still few and far between.

Willingness to adopt new technology is significantly – perhaps critically – influenced by the level of trust people have in it. Trust tends to develop slowly and is very easy to lose.All digital services must make a constant effort in order to earn public trust. Trust is earned by consistent and predictable behaviour. If these fundamentals are missing, no amount of quick fixes will help. Digital services have access to a range of well-established technologies and practices that can be used to demonstrate confidentiality. They include data security statements and the publication of quality certificates granted to the organisation. This study evaluates the impact of various trust-promoting measures.

The publication of open data and the provision of added value in connection with the data help generate wealth and well-being in a digital society. Data cannot generate added value unless it is properly utilised. There is still a lot of work to be done in this area – only a fraction of the potential of open data has been unlocked globally. When utilising open data and seeking ways to earn trust, it is important to remember that we are dealing with lifestyles and attitudes, and not just technologies and practices. The study seeks to identify and present ways to enhance the utilisation of open data.

Both open data and digitalisation on one hand and the associated trust on the other hand are supported by extensive and, in some respects, rather complex legislation. The study also seeks to provide a picture of the possibilities and limitations of regulation in trust building and the use of open data.

Appendix 1 Web survey questions

Appendix 2 Themes used in survey and list of specialists that were intervieved

This publication is part of the implementation of the Government Plan for Analysis, Assessment and Research for 2016 (tietokayttoon.fi/en).

The content is the responsibility of the producers of the information and does not necessarily represent the view of the Government.

SISÄLLYS

ESIPUHE.

Digitaalisen yhteiskunnan lupaukset ja mahdollisuudet

Suomi Reima

Suomi on pieni maa, joka voi kehittyä vain olemalla avoin ja kansainvälinen. Suomalaisia menestystarinoita voi vain harvoin rakentaa kansallisen toiminnan varaan. Siksi tarvitaan avointa suhtautumista kansainvälisyyteen ja esimerkiksi Euroopan unionin yhdistymiskehitykseen. Kansainvälistymiselle on nyt onneksi avautunut aivan uusia kanavia digitalisaation kautta. Digitalisaatio avaa aidosti ja tehokkaasti kansainväliset markkinat suomalaisille toimijoille, pienyrityksiä myöten.

Suomen mahdollisuudet hyödyntää digitalisaatiota ovat erinomaiset korkean osaamisemme, väestömme korkean koulutustason, luovuutemme, uteliaisuutemme ja uudistumiskykymme kautta. Suomalainen yhteiskunta sallii myös epäonnistumiset, digitalisaatiossakin. Virheistä opitaan usein paremmin kuin onnistumisista.

Digitalisaatio ei ole helppoa, ja sen edistämisessä tullaan varmasti tekemään virheitä ja ylilyöntejä. Myös epäonnistumisen tulee olla sallittua. Digitalisaatiota pyrkivät hyödyntämään myös rikolliset terroristeja myöten. Keskeinen ongelma on se, miten hyvää digitalisaatiota voidaan edistää ja samalla torjua digitalisaation haittapuolia. Oikein käytettynä digitalisaatio pystyy tehostamaan sisäistä turvallisuutta ja oikeudenhoidon palvelutasoa.

Digitalisaatio ei ole itsenäinen ilmiö, vaan kantava ja läpileikkaava teema koko yhteiskunnassa. Digitalisaation kautta mahdollistuvat ja tehostuvat esim. teollinen Internet, yhteiskunnan rakennemuutoksen edistäminen, biotalous ja puhtaat teknologiat sekä kestävä kehitys.

Digitalisaatio on oiva väline byrokratian purkamiseen, sillä digitalisaatio suorastaan edellyttää palveluprosessien järkeistämistä ja virtaviivaistamista. Digitalisaatiota tulee ja voi hyödyntää turhan sääntelyn ja byrokratian purkamisessa. Samalla digitalisaatioon tarvitaan kuitenkin pelisääntöjä ja sääntelyä, joka tulisi pitää mahdollisimman vähäisenä ja selkeänä. Esim. kansainvälistä digitalisaation sääntelyä ei saisi monimutkaistaa tarpeettomalla kansallisella lisäsäätelyllä. Digitalisaatio myös edistää ja edellyttää viranomaisten välistä tiedonvaihtoa ja yhteistyötä aivan uudella tasolla.

Suomeen tulee luoda suotuinen liiketoimintaympäristö digitaalisille palveluille. Tämä koskee niin julkishallintoa, kolmatta sektoria kuin kaikenkokoisia yrityksiä. Digitalisaation keskiössä ovat digitaaliset palvelut ja teollinen Internet.

Digitalisaatio edellyttää johtamistapojen uudistamista. Innovatiivisuuden ja palvelukeskeisyyden tulee olla toiminnan lähtökohta kaikessa digitaalisessa toiminnassa, myös julkisella sektorilla. Julkishallinnolla on erityinen rooli eri toimintojen hallinnollisen taakan keventämisessä ja lupaprosessien sujuvoittamisessa. Hyvään digitaaliseen johtamiseen kuuluu myös tiedolla johtaminen ja tietopohjan laajentaminen päätöksenteon tueksi. Myös sen osalta avoin data tarjoaa paljon kehitysmahdollisuuksia.

Digitalisaatio on suurin piirtein ainoa mahdollisuutemme tuottavuusloikkaan. Informaatio, ja varsinkaan digitaalinen informaatio, ei kulu käytössä, pikemminkin se jalostuu. Digitalisaatiolla on aina myös vastustajansa, esim. digitalisaation myötä aikaisemman etuoikeutetun asemansa menettävät tahot. Monet kansalaiset ovat myös aidosti huolissaan digitalisaation riskeistä. Tällainen muutostilanne vaatii vahvaa muutosjohtamista. Koko maassa on vahvistettava kyvykkyyksiä digitaaliseen muutosjohtamiseen.

Kuten minkä tahansa palvelun tai hyödykkeen käyttö, myös digitaalisten palveluiden käyttö vaatii sääntelyä. Tätä sääntelyä tehdään mikrotasolla erilaisten hyödykkeiden ja palveluiden

käyttöehtojen kautta. Käyttöehdot ovat parhaimmillaan kuluttajaa voimaannuttavia ja hyödykkeiden käyttöä helpottavia, mutta pahimmillaan ne estävät kuluttajille hyödyllisten hyödykkeiden käytön kokonaan. Kuluttajien lisääntynyt valppaus ja käyttöehtoja koskeva tietoisuus, palvelutuottajien lisääntyvä panostus käyttöehtojen kehittämiseen sekä käyttöehtoihin liittyvä julkinen sääntely ja paine antavat syyn olettaa, että käyttöehdot tulevat vastaisuudessa kehittymään positiiviseen suuntaan. Käyttöehdoilla pyritään ja myös pystytään haluttaessa suojaamaan erityisesti kuluttajien yksityisyyttä ja tietosuojaa.

Digitaalisissa palveluissa tieto on keskeisessä roolissa, ja itse palvelutapahtumat generoivat uutta tietoa. Siksi tieto tulee suojata digitaalisissa palveluissa erityisen hyvin. Keskeisessä roolissa on kuluttajien kokema luottamus, joka ei aina ole sidoksissa palvelun tai hyödykkeen todelliseen laatuun. Kaikki vakavasti toimivat digitoimijat panostavat palveluidensa tiedonsuojausominaisuuksien kehittämiseen, eikä ole mitään syytä nähdä, että suomalaiset toimijat olisivat tässä kehityksessä jotenkin kansainvälistä parhaimmistoa jäljessä. Ilahduttavasti tämä koskee myös ja ehkä jopa erityisesti suomalaista julkishallintoa.

Digitalisaatiota kohtaan koettua luottamusta voidaan kehittää myös erilaisten sertifikaattien avulla. Kaikkien digitaalisilla markkinoilla toimivien tahojen tulee tutkia mahdollisuuksia palveluidensa sertifioimiseen. Samalla on kuitenkin muistettava, että sertifikaatti ei auta mitään, jos palvelu ja toiminta sen taustalla eivät ole sen veroisia. Suomalainen kuluttaja osaa nähdä kokonaisuuden ja arvostaa usein pitkällä aikavälillä kehitettyä kulttuuria ja brändiä, jotka siis usein ovat erilaisia sertifikaatteja arvokkaampaa pääomaa.

Tietosuojakäytännöt ovat lähimpänä käyttäjän ”ihoa” hänen käyttämäänsä laitteeseen tai sovelluksiin istutettuina. Käyttäjän oman konfiguraatiohallinnan merkitys tulee voimakkaasti kasvamaan lähiaikoina. Liian usein tietosuojaan ja -turvaan liittyvät asetukset kuitenkin ovat ota tai jätä -tyyppisiä vaihtoehtoja. Suomalaisilla toimijoilla on tässä hyvät mahdollisuudet kehittää innovatiivisia ratkaisuja ja osoittaa edelläkävijyyttä.

Turvallisuuteen liittyviä asetuksia ja käytäntöjä ei saa piilottaa käyttäjältä, vaan niiden tulee olla läpinäkyviä. Suomalainen, tunnetusti jäsentynyt ja innovatiivinen verkkoympäristö voi tarjota tietosuojaltaan edistyneille palveluille hyvän kasvualustan.

Ei pidä väheksyä esim. julkisen hallinnon omistamaan ja tuottamaan dataan sisältyvää arvopotentiaalia. Tieto pitää mahdollisimman pitkälle saattaa avoimeksi tuottamaan lisäarvoa ja palveluita liiketoiminnalle, muulle hallinnolle ja kansalaisille. Avointa dataa voivat tuottaa myös muut kuin julkishallinto, ja vaikka data olisi sinällään avointa, voi sen ympärille rakentaa kannattavaa liiketoimintaa, kuten esim. avoimesta lähdekoodista saadut kokemukset osoittavat.

Big data eli suuret tietomassat ovat yksi tämän päivän kuumista puheenaiheista. Avoin data ja suuret tietomassat eivät ole sama asia, mutta kohtaavat usein. Kun kohtaamiseen liittyy henkilötietoja tai muuta luottamuksellista tietoa, tietosuoja ja -turva ovat erityisesti uhattuina. Tästä huolimatta suuret datamassat tarjoavat suuria liiketoimintamahdollisuuksia, kun datan anonymisoinnista huolehditaan kunnolla. Suomella on hyvät mahdollisuudet olla edelläkävijä anonymisointiteknologioissa ja alan parhaiden käytäntöjen kehittämisessä – jotka myöhemmin saattavat jalostua vientituotteiksi.

Tietoturvariskit ovat digitalisaation syöpä. Kuten muutkin taudit, ne ovat hankalimmillaan silloin, kun niitä ei ole vielä edes diagnosoitu. Tietoturvariskien mahdollisimman nopea havaitseminen on kaikkien etu. Havainnoinnin lisäksi tarvitaan tehokasta riskeistä tiedottamista ja toimenpiteitä, usein suuren toimijayhteisön yhteistyönä. Yleensäkin kaikkien toimijoiden keskinäinen yhteistyö sekä keskustelu ja tiedonvaihto ovat tietoturvariskien hallinnan kriittisiä menestystekijöitä. Suomen kaltaisessa pienessä maassa tällainen toiminta saattaa onnistua paremmin ja tehokkaammin kuin suuressa maassa. Samalla pitää kuitenkin muistaa, että sekä tietoturvariskit että niiden torjuminen ovat globaaleita kysymyksiä ja vaativat globaalia yhteistyötä.

Suomalaisessa yhteiskunnassa käytetään laajasti hyväksi globaalien toimijoiden tietoturvatuotteita ja -palveluita. Suomesta on myös mahdollista ponnistaa globaaleille markkinoille uusien tuotteiden ja palveluiden avulla, mutta se on haastavaa. Globaalien toimijoiden saaminen toimimaan Suomessa olisi kuitenkin hyvä tapa hankkia alan osaamista. Tätä edesauttaa paitsi yritystoiminnan yleisten edellytysten kehittäminen, myös Suomen erityisten digitoimintoihin liittyvien vahvuuksien taiten tehty esiintuonti.

TUTKIMUSMENETELMÄT JA TOTEUTUSTAPA

Tutkimushankkeessa kartoitettiin työpakettikohtaisesti aiheeseen liittyvä kirjallisuus, ja tutkimuksen orientaatio on pääosin narratiivinen. Narratiivisella kirjallisuuskatsauksella tarkoitetaan eri lähteistä kerättyä tutkimuskohdetta koskevaa tietoa, jonka keinoin on mahdollista tuottaa laaja kuva käsiteltävän aiheen kehityskulusta ja jäsenneltyä ajankohtaista tietoa hajanaisenkin tutkimuskentän tuloksista. Kirjallisuuskatsauksien laadinnassa tietolähteinä käytettiin vapaasti saatavilla olevia ja kaupallisia tietokantoja (esim. Forrester.com ja Gartner.com) sekä tietoturvayhteisöjen verkkosivustoja (esim. sans.org, Isaca.org, www.securityforum.org, KPMG:n globaali verkosto) ja yleisiä akateemisia julkaisutietokantoja.

Tutkimushankkeen aikana toteutettiin kyselytutkimus sähköisesti joulukuun 2016 ja tammikuun 2017 välisenä aikana. Kysely sisälsi kymmenen luottamukseen, tietoturvaan ja tietosuojaan perustuvaa väittämää, joihin vastaajien tuli ottaa kantaa asteikolla 1–5, jossa 1 vastasi kantaa ’’täysin eri mieltä’’ ja 5 vastasi kantaa ’’täysin samaa mieltä’’. Lisäksi kysely sisälsi työpakettikohtaisia kysymyksiä, joiden arvosteluasteikkona käytettiin numerointia 1–5, jossa 1 vastasi kantaa ’’en koskaan’’ ja 5 vastasi kantaa ’’erittäin usein’’. Esitetyt väittämät ja kysymykset löytyvät liitteestä 1.

Kyselyyn vastaaminen oli vapaaehtoista, ja kyselyyn johtavaa linkkiä jaettiin sosiaalisen median lisäksi sähköpostitse muun muassa eri palvelualojen toimijoille ja oppilaitosten opiskelijoille. Kyselytutkimuksen suunnittelivat yhteistyössä KPMG Oy Ab ja Turun yliopisto ja toteuttamisesta vastasi Turun yliopisto. Tutkimukseen osallistui 152 vastaajaa. Vastaajista 56 oli naisia ja 96 miehiä, ja heidän keski-ikänsä oli 36 vuotta.

Osana tutkimusta haastateltiin seitsemää tietoturva-alan asiantuntijaa lokakuun 2016 ja tammikuun 2017 välisenä aikana. Haastattelut tehtiin teemahaastatteluina, jolloin haastattelu on puolistrukturoitu ja sen kulku rytmittyy teemoittain tiukasti määriteltyjen yksittäisten kysymysten sijaan. Haastatteluissa käytetty haastattelurunko ja haastatellut henkilöt on listattu liitteessä 2. Kaikki haastattelut nauhoitettiin ja niistä kirjoitettiin tarkat muistiinpanot.

LUKU 1.

Käyttöehdot ja tietosuoja käyttäjien kannalta

Koskinen Jani

Suomi Reima

Käyttöehtojen liittäminen digitaaliseen tuotteeseen on erilaista verrattuna hyödykkeisiin, joissa mukana on myös konkreettinen fyysinen komponentti. Nykyisin tilanne on monimutkaisempi, kun digitaalisen vaihdannan kohteena ei enää ole pelkkä esine, vaan palvelu tai tuote, joka perustuu vahvasti immateriaalisen asian – kuten ohjelman – käyttöön. Autoissa tai vaikkapa sähköporissa ei ole käyttöehtosopimusta, vaan niiden käyttöoikeus perustuu kyseisen tuotteen omistamiseen. Kun perinteisessä tuotteessa tuottaja ja myyjä antavat tuotteen asiakkaalle korvausta vastaan, digitaalisten tuotteiden kohdalla annetaan usein vain oikeus käyttää tuotetta sopimuksessa mainittujen käyttöehtojen ja/tai sopimuksen mukaisesti. Joidenkin tuotteiden kohdalla asiakas ei myöskään maksa tuotteen käytöstä mitään, vaan yrityksen ansaintalogiikka perustuu esimerkiksi käyttäjätietojen hyödyntämiseen tai käyttäjille suunnatusta markkinoinnista saatavaan tuloon.

Ihmiset käyttävät yhä enemmän erilaisia päätelaitteita, sovelluksia ja verkkopalveluita työssään ja vapaa-aikanaan. Tällaisten digitaalisten tuotteiden käyttäminen edellyttää käyttöehtojen[1] hyväksymistä, jotta käyttäjä voi ottaa uuden sovelluksen tai laitteen käyttöönsä. Usein käyttäjä ei omista käyttämäänsä sovellusta, vaan ainoastaan sen käyttöön oikeuttavan lisenssin. Lisäksi käyttö on sallittu vain käyttöehtojen mukaisesti. Ongelmana käyttöehtojen sisäistämisessä on myös se, että ihmisillä voi nykyään usein olla käytössään useita eri laitteita, esimerkiksi älypuhelin, tabletti, tietokone ja televisio[2]. Kun jokaisessa edellä mainitussa laitteessa saattaa olla eri käyttöjärjestelmä, niissä on käytettäviä sovelluksia yleensä vähintään useita kymmeniä, joista jokaisessa on vielä erilliset käyttöehdot. Kokonaisuudessaan puhutaan helposti jo yli sadasta käyttöehdosta, jotka henkilön tulee hyväksyä voidakseen käyttää omia laitteitaan ja niissä olevia sovelluksia.

Seuraava esimerkki osoittaa hyvin nykyisten käyttöehtojen haasteellisuuden (huomioimatta lainsäädännöllisiä rajoitteita, jotka saattavat muuttaa niiden sitovuutta): Vuonna 2015 Alex Hern (2015) luki läpi 33 käyttämänsä palvelun käyttöehdot. Tämä tarkoitti 146 000 sanaa lakitekstiä. Ehtojen lukeminen on välttämätöntä käyttöehtojen vastuullista hyväksymistä ajatellen. Hän sai lukea ne kaikki äidinkielellään, mikä ei aina vastaa sellaisten henkilöiden tilannetta, joiden äidinkieli ei ole englanti.

On siis tärkeää tarkastella, miten käyttäjä voi suojata tietojaan ja yksityisyyttään niin henkilökohtaisella tasolla kuin mahdollisesti liiketoiminnassaan. Ennen kuin tähän haasteeseen voidaan vastata luotettavasti, on pystyttävä vastaamaan kolmeen kysymykseen: Ensimmäiseksi tulee tietää, millaisia käyttöehtoja on olemassa ja mitä niiden sisältö tarkoittaa. Toiseksi tulee ymmärtää käyttöehtoja, käyttäjän/palvelun toimittajan oikeuksia ja velvollisuuksia koskevaa

[1] End User Licence agreement (EULA) ja Terms of Service (TOS)

[2] Tässä on mainittu vain esimerkinomaisesti yleisimmät. Käytössä on myös paljon muita: älykeloja, turvajärjestelmiä, paikannusjärjestelmiä, IoT-sovelluksia jne. Tarkoitus on kiinnittää huomio siihen, että teknologia on laajassa käytössä ja sen käyttö laajenee koko ajan.

lainsäädäntöä. Kolmanneksi tulee pohtia, mikä on käyttäjän ja palvelun tuottajan tietosuojan taso.

Kuten aiemmin mainittiin, käyttäjällä saattaa usein olla kymmeniä käyttöehtoa luettavanaan ja hyväksyttävänään. Tällöin syntyy helposti tilanne, jossa käyttäjä vain hyväksyy käyttöehdot ilman niiden lukemista saati niiden syvällistä sisäistämistä ja tarkkaa arviointia. Kuten käyttöehtojen hyväksymistestissä[3] osoitettiin, useat käyttäjät eivät lue käyttöehtoja tai he eivät välitä niistä. He vain yksinkertaisesti hyväksyvät ehdot, kunhan se mahdollistaa palvelun tai tuotteen käytön. Tämä on ymmärrettävää ottaen huomioon tuotteiden, palvelujen ja laitteiden määrän, käyttöehtojen vaikeaselkoisuutta unohtamatta. Osana edellä mainittua testiä käytettiin käyttöehtoa, joka käyttäjän tuli hyväksyä. Sen mukaan käyttäjä lupasi luopua esikoisestaan tai rakkaimmasta lemmikistään saadakseen käyttää Internetiä kyseisen lähiverkon (Wi-Fi) kautta.

Ongelmana on, että käyttöehtojen teksti on usein pitkästyttävää ja vaikeaselkoista (Waddell, Auriemma & Sundar 2016). Tällöin ihmiset joko osaamattomuuttaan tai välinpitämättömyyttään vain painavat hyväksy-painiketta, varsinkin kun ainoana vaihtoehtona hyväksymiselle on olla käyttämättä palvelua (Lahtiranta, Hyrynsalmi, & Koskinen 2017). Lisäksi, kun käyttöehtoja päivitetään joltain osin kertomatta, mikä oikeasti muuttui, ehdot täytyy usein lukea uudestaan kokonaisuudessaan. Tällöin muutosta on vaikea tai jopa mahdoton ymmärtää ja motivaatio lukea käyttöehdot laskee, vaikka alkuperäinen versio olisikin luettu ja ymmärretty.

1.1. Käyttöehdot ja lainsäädäntö

Käyttöehdot ja lainsäädäntö ovat käytännön lähtökohta ihmisten henkilötietojen suojaamiselle digitaalisia palveluja ja viestintävälineitä käytettäessä. Käyttöehtojen hyväksyminen kokonaisuudessaan on pääsääntöisesti ehdoton edellytys palvelun tai tuotteen käytölle. On tietenkin myös mahdollista olla käyttämättä palvelua tai hankkia käyttöönsä korvaavia tuotteita tai palveluita, joiden käyttöehdot ovat käyttäjän kannalta sopivampia. Tämä vaihtoehto on kuitenkin usein käytännössä mahdoton, koska määrätyt palvelut ja välineet ovat de facto oletusarvo. Tällöin niiden käyttämättä jättäminen saattaa aiheuttaa joko sosiaalista ja/tai taloudellista haittaa, joka voi olla merkittävää. Sosiaalisesta haitasta esimerkkinä on nuoren jääminen oman ikäryhmänsä sosiaalisten verkostojen ulkopuolelle, jos hän kieltäytyy käyttämästä sosiaalista mediaa tai pikaviestipalveluita, joiden käyttöaste nuorilla (16–24-vuotiailla) on jo noin 95 % ja joka kasvaa myös muissa ikäluokissa (Tilastokeskus 2016). Taloudellisena haittana ihmiselle taas voidaan nähdä esimerkiksi S-ryhmän tietojen keruusta kieltäytyminen. Tietojen keräämisen estäminen toteutuu vain olemalla käyttämättä jäsenkorttia – mikä puolestaan aiheuttaa taloudellisia menetyksiä.

Vaikka palveluntarjoajat eivät yleensä ole käyttäneet kaikkia oikeuksia, joita he käyttöehtojen avulla ovat itselleen varanneet, tulee ymmärtää, että he ovat siihen jostain syystä varautuneet. Tulevaisuudessa voidaankin nähdä sellaisia käyttäjistä kerätyn tiedon hyödyntämistapoja, johon käyttäjät eivät ole varautuneet tai joita he eivät hyväksyisi, jos niin toimittaisiin nyt. Yritykselle on helpompaa varata enemmän oikeuksia käyttöönsä kuin pyytää niitä lisää myöhemmin. Tämä on ymmärrettävää, kun käyttäjät usein antavat suostumuksen ehtoihin niihin tutustumatta tai haluavat joka tapauksessa käyttää palvelua tai tuotetta.

[3] F-Secure. Luettu 6.2.2017
https://safeandsavvy.f-secure.com/2014/09/29/danger-of-public-wifi/

Käyttöehdot ja käyttöoikeudet ovat usein vaikeaselkoisia ja niiden monimutkaisuus on tunnettu asia (Bakos, Marotta-Wurgler & Trossen 2014; Watkins, Denegri-Knott & Molesworth 2016). Kun käyttöehdot ovat siis pääsääntöisesti vaikeita ymmärtää ja lisäksi ota tai jätä -tyyppisiä, ihmiset on helppo saada vain hyväksymään ehdot ilman niiden lukemista tai ymmärtämistä. Lisäksi kun tuotteiden käyttämättä jättäminen ei ole käytännössä mahdollista, ei käyttäjällä usein ole mahdollisuutta suojata omia tietojaan kyseisten palvelujen ja tuotteiden kohdalla, vaan hän joutuu tyytymään käyttöehtojen asettamiin epäsuotuisiin ehtoihin.

Varsinkin suuremmilla yrityksillä on muita paremmat mahdollisuudet suojella omaa tietosuojaansa laajempien resurssiensa avulla. Lisäksi heille esim. sosiaalisen viestinnän käyttö on todennäköisesti markkinointia ja PR-toimintaa, kun taas yksilöillä sen käyttö on enemmän henkilökohtaista ja omaan sosiaaliseen elämään liittyvä toimintaa, ja saattaa näin ollen sisältää arkaluonteista tietoa.

Käyttöehtojen lisäksi lainsäädäntö on keskeinen asia, joka vaikuttaa ihmisten mahdollisuuteen suojata tietojaan – unohtamatta tietoturvapalveluita ja tietoturvallisia toimintatapoja. Sopimukset, kuten tässä tapauksessa käyttöehdot, perustuvat lakeihin ja asetuksiin, joita osapuolten tulee noudattaa. Tässä nousee esille merkittävä yhteiskunnallinen ongelma. Yksittäisillä ihmisillä tai toimijoilla ei ole yleensä tosiasiallista mahdollisuutta vaikuttaa lainsäädäntöön ja tätä kautta tietojensa suojaamisen perusteisiin. Tämä korostaa ihmisten kyvyttömyyttä suojella yksityisyyttään tehokkaasti. Ainoaksi varmaksi tavaksi jääkin vain päätös olla kokonaan käyttämättä palveluita tai tuotteita, jolloin käyttäjä saattaa kokea merkittävää haittaa. Tämä nostaa esiin tarpeen korostaa yksilön suojaa, mikä onneksi on ollut päämääränä erityisesti Euroopan unionin regulaatiossa ja osoittaa myös tarvetta erillisille toimijoille[4], joiden keskiössä on yksilöiden suojaaminen ja heidän asemansa vahvistaminen yhteiskunnassa. Tässä raportissa esitellään lyhyesti Euroopan unionin tietosuoja-asetus ja esitys uudeksi sähköisen viestinnän direktiiviksi, koska Euroopan unionin asetukset ja direktiivit asettavat vaatimukset niiden kansalliselle soveltamiselle ja harmonisoinnille[5].

Euroopan unionin tietosuoja-asetus (2016/679)

Vuonna 2016 hyväksyttyä tietosuoja-asetusta aletaan soveltaa kahden vuoden siirtymäajan jälkeen 25.5.2018. Sen keskeisiä tavoitteita ovat seuraavat:

- Luonnollisten henkilöiden tietosuoja-oikeuksien turvaaminen Euroopan unionissa.
- Vapaan henkilötietojen liikkuvuuden varmistaminen jäsenvaltioiden välillä, jotta palvelut voidaan taata missä tahansa jäsenvaltiossa.
- Digitaalisten sisämarkkinoiden kehittymisen edistäminen.
- Rekisteripitäjien velvollisuuksien ja lisääminen sekä niiden noudattamisen valvonta ja kontrolli.

Euroopan unionin tietosuoja-asetus asettaa tiukan vaatimuksen tietoiselle suostumukselle tietojen käsittelyyn, mikä on keskeinen asia, kun tarkastellaan käyttäjien mahdollisuutta suojata omia tietojaan:

”*Kun tietojenkäsittely perustuu rekisteröidyn suostumukseen, rekisterinpitäjän olisi voitava osoittaa, että rekisteröity on antanut suostumuksensa käsittelytoimiin. Etenkin, jos suostumus annetaan muuta seikkaa koskevan kirjallisen ilmoituksen yhteydessä, olisi varmistettava suojatoimin, että rekisteröity on tietoinen antamastaan suostumuksesta ja siitä, kuinka pitkälle menevästä suostumuksesta on kyse. Neuvoston direktiivin 93/13/ETY mukaisesti rekisterinpitäjän*

[4] Esimerkiksi Tietosuojavaltuutettu ja Electronic Frontier Finland ry

[5] https://europa.eu/european-union/eu-law/legal-acts_fi

ennalta muotoilema ilmoitus suostumuksesta olisi annettava helposti ymmärrettävässä ja helposti saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä eikä siihen pitäisi sisältyä kohtuuttomia ehtoja. Tietoisen suostumuksen antamiseksi rekisteröidyn olisi tiedettävä vähintään rekisterinpitäjän henkilöllisyys ja tarkoitukset, joita varten henkilötietoja on määrä käsitellä. Suostumusta ei voida pitää vapaaehtoisesti annettuna, jos rekisteröidyllä ei ole todellista vapaan valinnan mahdollisuutta ja jos hän ei voi myöhemmin kieltäytyä suostumuksen antamisesta tai peruuttaa sitä ilman, että siitä aiheutuu hänelle haittaa." (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679)

Tämän perusteella voidaan tulkita, että nykyisen kaltaiset käyttäjäehdot, joissa käytön ehtona on ehtojen hyväksyntä ilman neuvottelumahdollisuutta, eivät ole tämän asetuksen kirjaimen ja hengen mukaisia. Suostumusta ei voida pitää vapaan valinnan tuloksena, koska käyttäjällä ei ole mahdollisuutta kieltäytyä siitä, ja usein suostumusta ei ole enää mahdollista peruttaa[6]. Tähän ongelmaan voi ja tulisi puuttua kansallisen lainsäädännön ja ohjeistuksen tasolla, korostamalla kyseisten käyttäjäehtojen pätemättömyyttä ja vaatimalla niiden muokkaamista ymmärrettäviksi ja tietosuoja-asetuksen vaatimusten mukaisiksi. Tähän olisi tartuttava välittömästi ainakin sellaisten palvelujen kohdalla, jotka ovat viranomaisten tarjoamia tai joiden käyttö on riittävän yleistä ja joiden käyttämättä jättämisellä voisi olla merkittäviä negatiivisia vaikutuksia yksilölle.

Kuten edellä oleva tietosuoja-asetuksen tietoista suostumusta koskeva vaatimus osoittaa, asetus myös edellyttää käyttäjäehtojen olevan sellaisia, että ne ovat ymmärrettävässä muodossa käyttäjille – muillekin kuin niihin syvällisesti perehtyneille lakimiehille tai muille alan asiantuntijoille. Hyvänä ja poikkeuksellisena esimerkkinä tästä markkinoilla on käyttäjäystävällisiä lähestymistapoja. Käyttäjäystävällisyys ja ymmärrettävyyden tavoittelu ilmenevät hyvin selkeistä, ymmärrettävistä käyttöehdoista ja helposti saatavilla olevista tietosuojakäytännöistä sekä niiden lisäksi niistä tarjolla olevista tiivistetyistä versioista.

1.2. Esimerkkejä käyttöehdoista

Tässä työpaketissa käytiin läpi kahdeksan eri sovelluksen tai palvelun käyttöehdot ja yksityisyysperiaatteet. Käyttöjärjestelmistä mukaan otettiin kaksi yleistä käyttöjärjestelmää (Microsoft Windows 10 ja Applen mobiilikäyttöjärjestelmä iOS10), jotka edustavat kahta eri tyyppiä – perinteistä tietokonetta ja selkeää mobiililaitetta – vaikka näiden ero ei olekaan täysin yksiselitteinen. Internet-selaimista mukaan otettiin myös kaksi eri tuotetta, joista Googlen Chrome on maailman käytetyin Internet-selain ja Mozillan Firefox taas vastaavasti suurin avoimen puolen Internet-selain[7]. Hakukoneista valittiin ylivertaisesti suosituin, Google, josta ei kylläkään ole erillistä dokumenttia, vaan se sisältyy Googlen yleiseen tietosuojadokumenttiin. Sosiaalisen median sovelluksena tarkasteltiin Facebookia, ja vastaavasti viestisovelluksista valittiin WhatsApp niiden vahvan aseman vuoksi Suomessa. Viimeisenä mobiilipeleistä valittiin tarkasteltavaksi Pokemon Go, joka edustaa laajalti käytössä olevaa viihdesovellusta.

Käyttäjäehdoista nostettiin esille taulukon 1 työpakettiin keskeisiä asioita esimerkinomaisesti. Taulukko ei ole kattava, vaan sen tarkoituksena on havainnollistaa tietosuojan nykytilaa yleisellä tasolla.

[6] Kerättyjen tietojen käytön estäminen on usein käyttöehdoissa suljettu pois tai vaihtoehtoisesti tehty hyvin vaikeaksi käyttäjälle.

[7] Kummastakin otettiin testiin Windows 7 -käyttöjärjestelmälle suunnattu tuote.

Lähes kaikkien palveluiden kohdalla käyttöehdot ovat samankaltaisia (poissulkien Mozilla, jota käsitellään tarkemmin seuraavassa kappaleessa). Käyttöehdot ovat niin kutsuttuja ota tai jätä -tyyppisiä, eli jos tuotetta halutaan käyttää, käyttöehdot tulee hyväksyä. Käyttöehtoihin ei ole mahdollista tehdä muutoksia tai rajauksia, vaan ne hyväksytään sellaisenaan. Käyttöehdot mahdollistavat henkilökohtaisten tietojen keräämisen käytön aikana ja niiden jakamisen (poissulkien WhatsApp) myös kolmansien osapuolien kanssa. Poikkeuksena ovat alle 13-vuotiaat, joista kukaan ei kerää henkilötietoja. Jos käy ilmi, että käyttäjä on alle 13-vuotias, kaikki hänen tietonsa poistetaan. Sijaintitietojen kerääminen on valinnaista kaikissa palveluissa, paitsi Applen iOS:n kohdalla. Applen iOS seuraa käyttäjien sijaintia aina joko GPS:n tai tukiasemien kautta. Käyttäjä voi ainoastaan valita, seurataanko häntä anonyymisti vai ei. Koska sijaintia tarkastellaan myös tukiasemien kautta, ei GPS:n pois päältä sulkeminen estä seurantaa.

Ainoan selkeän poikkeuksen tekee Firefox, joka edustaa avoimen lähdekoodin tuotetta. Firefoxin käyttö perustuu lisenssiin, eikä käytön ehtona ole erillistä käyttöehtosopimusta. Tuotetta saa siis käyttää, muokata ja jakaa vapaasti lisenssin ehtojen mukaisesti. Tietosuoja esitellään omassa dokumentissaan, ja siinä todetaan, että tietoja kerätään, mutta vain niihin tarkoituksiin, joihin käyttäjä antaa luvan. Poikkeuksena tähän ovat lain asettamat vaatimukset, esimerkiksi oikeudenkäynteihin sekä käyttäjien oikeuksien ja turvallisuuden suojelemiseen tarvittavien tietojen kerääminen. Alle 13-vuotiaiden tietoja ei kerätä. Sijaintitietojen kerääminen ja käyttö ovat käyttäjän määriteltävissä. Yleisesti ottaen Firefox antaa käyttäjälle mahdollisuuden päättää tuotteen käytöstä. Tämä piirre on yleinen vapaan lähdekoodin järjestelmissä, ja se on sisäänrakennettu vapaan lähdekoodin ohjelmistojen yleisesti käyttämiin lisensseihin.

Taulukko 1: Käyttöehtojen keskeisiä kohtia.

Sovellus tai palvelut	Apple iOS	Windows 10	Firefox	Chrome	Google	Facebook	WhatsApp	Pokemon Go
Mahdollisuus mukauttaa käyttöehtoja (ota tai jätä -vaihtoehdot)	Ei	Ei	Ainoastaan vapaan lähdekoodin lisenssin rajoitukset	Ei	Ei	Ei	Ei	Ei
Kerätäänkö henkilökohtaisia tietoja käytön aikana?	Kyllä	Kyllä	Valinnainen	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
Kerätäänkö alle 13 v. lasten henkilötietoja?	Ei	Ei	Ei	Ei	Ei	Ei	Ei	Ei
Jaetaanko tietoja kolmansien osapuolien kanssa?	Kyllä	Kyllä	Valinnainen	Kyllä	Kyllä	Kyllä	Ei	Kyllä
Sijainnin seuranta	Kyllä (vähintään anonyymisti)	Valinnainen	Valinnainen	Valinnainen	Valinnainen	Valinnainen	Valinnainen	Valinnainen

1.3. Kyselytutkimus

Kyselytutkimus suoritettiin sähköisesti jakamalla linkkiä muun muassa tunnetuille eri palvelualojen toimittajille ja oppilaitosten opiskelijoille. Kyselytutkimuksen suunnittelivat yhteistyössä KPMG Oy Ab ja Turun yliopisto, ja toteuttamisesta vastasi Turun yliopisto. Kyselyssä oli seit-

semän (7) tähän työpakettiin kuuluvaa luottamukseen, käyttöehtoihin ja tietosuojaan perustuvaa kysymystä, ja niistä saatuja tuloksia on analysoitu. Arvosteluasteikkona käytettiin Likert-asteikkoa arvoilla 1–5. Tutkimukseen osallistui 152 vastaajaa. Vastaajista 56 oli naisia ja 96 miehiä, ja heidän keski-ikänsä oli 36 vuotta.

Kysymykset tässä työpaketissa:

Kysymys 1: Se, miten palveluntarjoaja käyttää palveluun tallentamiani henkilötietoja, vaikuttaa päätökseeni käyttää palvelua.

	1	2	3	4	5		Yhteensä	Keskiarvo
Täysin eri mieltä	1	15	20	67	49	Täysin samaa mieltä	152	3,97
	0,66 %	9,87 %	13,16 %	44,08 %	32,24 %			

Kysymys 2: Koen voivani riittävissä määrin vaikuttaa siihen, kuinka palveluntarjoaja käyttää palveluun tallentamiani tietoja.

	1	2	3	4	5		Yhteensä	Keskiarvo
Täysin eri mieltä	49	69	25	8	1	Täysin samaa mieltä	152	1,97
	32,24 %	45,39 %	16,45 %	5,26 %	0,66 %			

Kysymys 3: Koen, että sähköisissä palveluissa ilmaistaan selkeästi, millaisia tietosuojakäytänteitä palvelu soveltaa.

	1	2	3	4	5		Yhteensä	Keskiarvo
Täysin eri mieltä	27	69	39	15	2	Täysin samaa mieltä	152	2,32
	17,76 %	45,39 %	25,66 %	9,87 %	1,32 %			

Kysymys 4: Tunnen tietosuojalainsäädännön vaikutuksen tietojeni käsittelyyn.

	1	2	3	4	5		Yhteensä	Keski-arvo
Täysin eri mieltä	15	56	32	35	14	Täysin samaa mieltä	152	2,85
	9,87 %	36,84 %	21,05 %	23,03 %	9,21 %			

Kysymys 5: Kuinka tarkkaan tutustut käyttämiesi ohjelmien ja sovellusten käyttöehtoihin?

	1	2	3	4	5		Yht-eensä	Keski-arvo
En tutustu lainkaan	24	66	35	21	6	Tutustun hyvin tarkkaan	152	2,47
	15,79 %	43,42 %	23,03 %	13,82 %	3,95 %			

Kysymys 6: Kuinka hyvin olet ymmärryttänyt lukemisesi ohjelmien ja sovellusten käyttöehtojen sisällön?

	1	2	3	4	5		Yht-eensä	Keski-arvo
En ymmärrä niitä	13	46	49	28	16	Ymmärrän ne hyvin	152	2,92
	8,55 %	30,26 %	32,24 %	18,42 %	10,53 %			

Kysymys 7: Kuinka hyvin tunnet käyttämiesi ohjelmien ja sovellusten tietosuojaominaisuudet?

	1	2	3	4	5		Yht-eensä	Keski-arvo
En tunne niitä lainkaan	14	63	46	25	4	Tunnen ne hyvin	152	2,62
	9,21 %	41,45 %	30,26 %	16,45 %	2,63 %			

Vastaajat kokivat (kysymys 1), että se, miten heidän henkilötietojaan käytetään, vaikuttaa vahvasti palvelun käyttöön. Tästä nousee esiin ristiriita erilaisten palvelujen käyttöasteen suuruuden suhteen. Tiedetään, että vaikka useat palvelut perustuvat henkilökohtaisten tietojen käyttöön, näitä palveluita käytetään silti laajasti. Syynä saattaa olla se, että todellista vaihtoehtoista palvelua ei ole, tai sen käyttämättä jättäminen nähdään huonompana vaihtoehtona kuin tietojen mahdollinen käyttö. Tämä ristiriita puoltaa tarvetta tietoisen suostumuksen tarkasteluun ja korostaa tarvetta uusiin ratkaisuihin yksipuolisten ota tai jätä -sopimusten sijaan. Vastaajien (kysymys 2) mukaan heillä ei ole riittävää mahdollisuutta päättää omien tietojensa käytöstä.

Tämän lisäksi palvelujen tietosuojakäytänteet on ilmoitettu epäselvästi (kysymys 3), mikä vaikeuttaa tietoisen suostumuksen antamista, mitä Euroopan unionin tietosuoja-asetus edellyttää. Ottaen huomioon nämä seikat sekä sen, että vastaajien mielestä sähköisissä palveluissa ei ilmaista selkeästi, millaisia tietosuojakäytänteitä palvelu soveltaa, ei ole yllättävää, että ihmisten voi olla vaikeaa ottaa tietosuojaa haltuunsa ja muodostaa käsitystä omien tietojensa mahdollisista käyttötavoista.

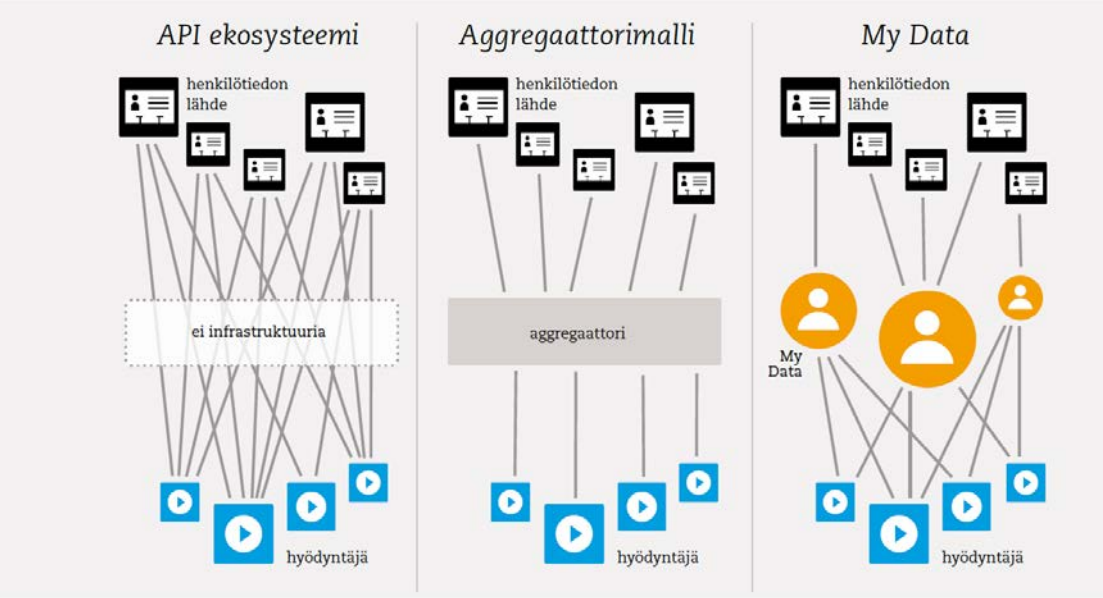
Tämä on linjassa vastaajien näkemysten kanssa (kysymykset 5–7). He eivät ole tutustuneet hyvin käyttämiensä ohjelmien tai palvelujen käyttöehtoihin tai tietosuojaominaisuuksiin. Lisäksi tietosuojaominaisuuden tuntemus oli heikkoa. Nykyään tietosuojaa pidetään kriittisenä osana yhteiskuntaa, ja sen puute tarkoittaa luottamuksen puutetta. Tämä on este digitaalisten markkinoiden kehittymiselle ja on näin ollen käyttäjien ja palvelujen tuottajien edun vastaista laajassa mittakaavassa, vaikka tietyt toimijat voivat hyötyä tilanteesta, jossa tietosuoja ei ole tiukasti kontrollissa

1.4. Mahdollisuudet käyttäjien tietojen suojaamiseen

EU:n tietosuoja-asetus tulee olemaan Suomessa suoraan sovellettavaa lainsäädäntöä. Oikeusministeriö vastaa Suomessa asetuksen täytäntöönpanon edellyttämistä lainsäädäntötoimista. Joiltakin osin asetus antaa kuitenkin tilaa tarkemmille säännöksille kansallisessa lainsäädännössä, ja näin ollen niihin voidaan tehdä joitakin muutoksia ja tarkennuksia. Tästä syystä Suomen henkilötietojen käsittelyä koskevat säännökset voivat olla myös jatkossa voimassa joillakin aloilla.

Julkiselta sektorilta löytyy hyvä esimerkki tietosuojan ottamisesta vakavasti: Kanta-palvelut. Omakannassa kansalaisen tietoturva on suojattu teknisesti ja lisäksi kansalaisella on mahdollisuus rajata, miten hänen tietonsa näkyvät terveydenhuollon ammattilaisille. Lisäksi kansalaisella on oikeus tietoon siitä, missä hänen reseptitietojaan on katsottu ja käsitelty tai mihin hänen potilastietojaan on luovutettu.

Mahdollinen lähestymistapa kansalaisen tietosuojaan on MyData-konsepti (Poikola ym. 2014), jonka keskeisenä ideana on keskittää yksilön tietojen jakaminen yhteen pisteeseen, MyData-palveluun, käyttäjän itsensä hallittavaksi. MyData on infrastruktuuritason ratkaisu tietojen jakoon ja hallintaan (kuva 1). Käyttäjien lisäksi tästä ratkaisusta voisivat hyötyä vastuulliseen digitaaliseen liiketoimintaan keskittyvät yritykset. Käyttäjillä olisi keskitetty ja luotettava tapa hallita yksityisyyttään ja myös mahdollisuus luovuttaa tietoja tietoisella suostumuksella yritysten käyttöön.



Kuva 1 MyData-konsepti (Poikola ym. 2014)

Alkuperäisessä lähteessä (Poikola ym. 2014) kuviota kommentoidaan seuraavasti: ”Erilaisia henkilötiedon yhdistämisen mahdollistavia organisointitapoja: vasemmalla infrastruktuuriton API-ekosysteemi, jossa kaikki datalähteiden ja sovellusten suhteet määritellään erikseen datalähteiden yksityisyysasetuksista, keskellä aggregaattorimalli, jossa yksittäinen toimija kerää ja harmonisoi dataa useasta lähteestä ja jakelee eteenpäin, oikealla avoin My Data -infrastruktuuri, jossa välittäjäorganisaatioita voi olla useita, ja ne ovat kaikki yksilön palveluksessa. Huom. kuvassa viivat voivat kuvata datan liikkumista tai luottamussuhdetta. Osa datasta on käytännöllistä kerätä yhteen (datapankki), mutta osa tallennetaan syntypaikassa ja välittäjäorganisaatio ainoastaan huolehtii käyttöluvista (dataoperaattori). Tarpeettomien datakopioiden tekemistä pyritään välttämään.” (Poikola ym. 2014, 38.)

Varteenotettava on myös ehdotus tiedon herruudesta (Kainu & Koskinen 2012). Tiedon herruus on juridinen ratkaisuehdotus, jossa henkilökohtaisen tiedon kokonaisvaltainen, luovuttamaton kontrolli annetaan henkilölle jolta tieto on peräisin. Tätä ehdotusta on analysoitu tarkemmin eettisesti terveydenhuollon kontekstissa, ja se edistäisi esimerkiksi potilaskeskeisyyttä ja potilaan asemaa terveydenhuollossa (Koskinen 2016; Koskinen, Kainu & Kimppa 2016).

1.5. Johtopäätöksiä

Käyttäjien mahdollisuudet kontrolloida henkilötietojensa käyttöä ovat rajalliset, vaikka lainsäädäntö ja direktiivit yrittävät suojata kuluttajia. Pienyritysten kohdalla tilanne voi olla vielä vaikeampi, koska yrityksillä ei ole samanlaista suojaa kuin kuluttajilla ja kansalaisilla. Tarvitaanko vahvempaa suojaa kuin mitä nyt on tarjolla? Vahvempi kansallinen tietosuoja voi olla rasite yrityksille, jotka toimittavat sähköisiä palveluita, mutta samalla se voi olla kilpailuetu yrityksille, jotka haluavat palvella asiakasta käyttäjien tietoturvan suojelun lähtökohdista. Tietosuojan kiristäminen saattaa haitata toimijoita, joiden liiketoimintamalleissa käyttäjien tietojen käyttö tai jakaminen kolmansille osapuolille on ydintoimintaa tai vähintään keskeinen osa sitä.

Tietosuojan korostaminen yhdessä vakaan ja demokraattisen toimintaympäristön kanssa on selkeä mahdollisuus liiketoiminnalle nykymaailmassa, jossa digitalisointiin liittyvät negatiiviset seikat ovat nousseet selkeästi esille. Yhtenä lähtökohtana olisi lisätä käyttäjien kontrollia omista tiedoistaan ja lisätä näin luottamusta digitaaliseen liiketoimintaan. Kun käyttäjien ymmärrys ja kontrolli olisivat paremmat, yritykset tietäisivät, mihin käyttäjät ovat sitoutuneet ja voisivat toteuttaa vastuullisempaa liiketoimintaa, joka noudattaisi paremmin myös uutta tietosuoja-asetusta. Tähän on jo olemassa ratkaisuehdotus: MyData, jonka avulla käyttäjätietojen jakoa voidaan kontrolloida.

Edellisiin verrattuna paljon helpommin käyttöön otettava parannus olisi kodinkoneiden energiatehokkuudessa käytetun asteikon tapainen havainnollistus kuvaamaan tietosuojan tasoa. Asteikko antaisi käsityksen siitä, millä tasolla tietosuoja kyseisen palvelun tai tuotteen kohdalla on, ja auttaisi tällöin käyttäjää tarkastelemaan tietosuojaa silloin, kun hän kokee sen tärkeäksi. Tietosuojavaltuutetun toimisto voisi olla toimija, joka sopisi kyseisen asteikon edistäjäksi.

On myös olemassa palveluita, jotka määrittelevät omat tuotteensa siten, että ne täyttävät tietosuoja-asetuksen vaatimukset. Tämän tulee olla ehdoton vaatimus palveluille, joita halutaan käyttää julkisissa organisaatioissa Suomessa. Vastuullisen tietosuojan edellyttäminen luo painetta markkinoille tuottaa haluttuja ratkaisuja tai ainakin tehdä niistä versio käytettäväksi Euroopassa. Tavoitteena tulisi olla kuitenkin sellaisten palveluiden vaatiminen, jotka eivät pelkästään noudata tietosuoja-asetusta, vaan tavoittelevat vieläkin korkeampaa tietosuojaa aina kun mahdollista.

Vastuullinen kehittäminen (Resbonsible Research and Innovation, RRI) on lähestymistapa, jossa yhteiskunnan eri toimijat, kuten tutkijat, kansalaiset, viranomaiset ja elinkeinoelämä. toimivat yhdessä, jotta kehittäminen ja innovaatiot vastaisivat yhteiskunnan arvoja ja odotuksia (Stahl, Eden, Jirotka & Coeckelbergh 2014). RRI on implementoitu osaksi Euroopan unionin Horizon 2020 -hanketta läpileikkaavana teemana ja tukee näin ollen vastuullista kehitystä[8]. RRI:n tuominen osaksi julkisen hallinnon kansallista toimintaa edistäisi vastuullista toimintaa kansallisella tasolla nojautuen jo laajemmassa käytössä olevaan – hyväksi koettuun – käytäntöön.

[8] Horizon 2020, the EU Framework Programme for Research and Innovation. https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation, accessed15.1..2017

Lähteet

Bakos, Y., Marotta-Wurgler, F. & Trossen, D. R. (2014). Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts. *The Journal of Legal Studies*, 43(1), 1–35. doi:10.1086/674424

Hern, A. (2015). I Read the small print on the Internet and it made me want to die. *The Guardiaa 15.6.2015.*

Kainu, V. & Koskinen, J. (2012). Between public and personal information - not prohibited, therefore permitted. Teoksessa Bottis, M. (toim.). *Privacy and Surveillance, Current aspects and future perspectives*. (45–59). Nomiki Bibliothiki.

Koskinen J. (2016). *Datenherrschaft – an Ethically Justified Solution to the Problem of Ownership of Patient Information.* Doctoral thesis, Turku School of Economics, Publications of Turku School of Economics, Series A.

Koskinen, J., Kainu V. & Kimppa K. (2016). The concept of Datenherrschaft of patient information from a Lockean perspective. *Journal of Information, Communication and Ethics in Society*, Vol 14(1), 70–86.

Lahtiranta J., Hyrynsalmi S. & Koskinen J. (2017). The False Prometheus – Customer Choice, Smart Devices and Trust. *SIGCAS Computers and Society*, Vol 47(3), 86-97.

Poikola A., Kuikkaniemi K. & Kuittinen O. (2014). *My Data – johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen.* Liikenne- ja viestintäministeriö. http://urn.fi/URN:ISBN:978-952-243-418-0

Stahl, B.C., Eden, G., Jirotka, M. & Coeckelbergh, M. (2014). From computer ethics to responsible research and innovation in ICT: The transition of reference discourses informing ethics-related research in information systems. *Information & Management*, 51(6), 810–818. doi:http://dx.doi.org/10.1016/j.im.2014.01.001

Tilastokeskus. (2016). *Väestön tieto- ja viestintätekniikan käyttötutkimus 2015*.

Waddell, T. F., Auriemma, J. R. & Sundar, S. S. (2016). *Make it Simple, or Force Users to Read?: Paraphrased Design Improves Comprehension of End User License Agreements.* Paper presented at the Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, Santa Clara, California, USA.

Watkins, R. D., Denegri-Knott, J. & Molesworth, M. (2016). The relationship between ownership and possession: observations from the context of digital virtual goods. *Journal of Marketing Management*, 32(1-2), 44–70. doi:10.1080/0267257X.2015.1089308

LUKU 2.

Tiedonsuojausominaisuuksien merkitys käyttäjäluottamuksen kannalta digitaalisissa palveluissa

Haukola Timo

Karhunen Joonas

Ahvenjärvi Samu

Palveluympäristöjen siirtyminen verkkoon on luonut organisaatioille uusia, ketteriä ja tehokkaita tapoja toimia. Digitalisaatio on toiminut merkittävänä muutosajurina toimintatapojen tehostamisessa ja kokonaan uusien palvelumuotojen kehittämisessä. Digitalisaatio tarjoaa mahdollisuuksia valinnanvapauden, saatavuuden ja tuottavuuden parantamiseen, säästää aikaa ja vähentää sekä asiakkaille että yhteiskunnalle aiheutuvia kustannuksia (eduskunnan sosiaali- ja terveysvaliokunta 2014).

Digitalisaatio on voimakkaasti esillä Sipilän hallituksen strategiassa ja mukana lähes jokaisessa sen toteuttamista tukevassa kärkihankkeessa. Kärkihankkeiden tavoitteina on mm. uudistaa julkiset palvelut ensisijaisesti sähköisiksi (kärkihanke: julkisten palveluiden digitalisaatio) ja edistää elinkeinoelämän digitalisaatiota (digitaalisen liiketoiminnan kasvuympäristön rakentaminen) (Valtioneuvoston kanslia 2015). Suomen kansallisessa tietoturvallisuusstrategiassa (liikenne- ja viestintäministeriö 2016) todetaan ja asetetaan tavoitteeksi, että tulevaisuudessa ‘’Maailman luotetuin digitaalinen liiketoiminta tulee Suomesta’’. Luottamus on yksi liiketoiminnan kulmakivistä digitaalisissa ympäristöissä, sillä ilman käyttäjien luottamusta digiympäristö ei voi kehittyä.

Luottamukselle ei ole vakiintunutta määritelmää, mutta sitä voidaan tarkastella esimerkiksi olettamuksien ja odotuksien näkökulmasta. Kaupankäynnissä luottamuksella tarkoitetaan asiakkaan odotuksia käyttämiään palveluita kohtaan. Luottamuksen puute voi heikentää kuluttajien halukkuutta toimia markkinoilla ostaen ja myyden palveluita ja tuotteita (Euroopan unioni 2016). Esimerkiksi asiakas odottaa luovuttamiensa ja itseään koskevien tietojen säilyttämistä järjestelmissä siten, että niiden luottamuksellisuus, eheys ja saatavuus toteutuvat kaikissa tilanteissa (Heino 2016).

Digitalisoiduissa palveluissa käsitellään usein pankkisalaisuuden piirissä olevaa tietoa tai arkaluonteista henkilötietoa, jolloin tietoturvallisuuden ja tietosuojan on kestettävä vertailu perinteisiin palvelumuotoihin käyttäjän luottamuksen saavuttamiseksi. Toisaalta on huomattava, että digitaalisen palveluntarjoajan mahdollisuudet vaikuttaa palvelun fyysiseen käyttöympäristöön ovat usein rajalliset, ja näin ollen myös loppukäyttäjä on enenevässä määrin vastuussa tietojen huolellisesta käsittelystä. Palveluntarjoajan on lähes mahdotonta varmistaa, että asiakas käyttää palvelua fyysisesti tietoturvallisessa ympäristössä, vaikka teknisiä tietoturva- ja tietosuojariskejä kyettäisiinkin hallitsemaan.

Käyttäjien luottamusta sähköisiin palveluihin on tutkittu pääasiassa verkkokaupan näkökulmasta ostopäätökseen vaikuttavana tekijänä. Erilaisten tiedonsuojausmenetelmien vaikuttavuus luottamuskokemukseen vaihtelee, sillä tätä kokemusta vahventavat tai heikentävät erilaiset tekijät, kuten käyttäjän tietotekninen osaamistaso, riskitietoisuus ja käsiteltävän tiedon sensitiivisyys. Tämän tutkimuksen tavoitteena on tarkastella tiedonsuojausominaisuuksien ja sertifiointien tarvetta ja niiden merkitystä rakennettaessa käyttäjien kokemaa luottamusta digitaalisia hyödykkeitä kohtaan.

Tässä luvussa käsitellään tiedonsuojausominaisuuksien ja käyttäjien palvelua kohtaan kokeman luottamuksen suhdetta kuvailevan kirjallisuuskatsauksen keinoin. Tutkimuksen orientaatio on narratiivinen, jonka keinoin on mahdollista tuottaa laaja kuva käsiteltävän aiheen kehityskulusta ja jäsenneltyä ajankohtaista tietoa hajanaisenkin tutkimuskentän tuloksista (Salminen 2011). Kirjallisuuskatsauksen avulla on laadittu lähtökohtaolettamuksia kyselytutkimuksen tueksi.

Luottamusta ja sen merkitystä sähköisissä palveluissa käsitellään tässä luvussa erityisesti sosiaali- ja terveydenhoitoalan kontekstissa. Toimiala ja sen sähköisten palveluiden kehitys tarjoavat tämän tutkimuksen kontekstissa arvokasta näkökulmaa siihen, miten perinteisesti vastaanotoilla käsiteltävää potilastietoa voidaan käsitellä tietoturvallisesti, sekä mahdollisuuden tunnistaa valitulta toimialalta yleistettäviä havaintoja. Tutkimuksen tietoperustaksi valittu aineisto koostuu korkeintaan 15 vuotta vanhoista julkaisuista, tutkimuksista ja selvityksistä, joissa käsitellään käyttäjien kokemaa luottamusta digitaalisia hyödykkeitä kohtaan.

2.1. Luottamus

Eurobarometri-tutkimuksen (Euroopan komissio 2015) mukaan suurin osa eurooppalaisista on sitä mieltä, että omien henkilökohtaisten tietojen jakaminen on osa nykyelämää digitaalisella aikakaudella. Toisaalta vain pieni osa tutkimukseen osallistuneista oli sitä mieltä, että omien tietojen jakaminen ei ole merkityksellistä heille, ja 63 % vastanneista ei luottanut digitaalisten palveluntarjoajien tapoihin hallinnoida henkilötietoja. Kyselytutkimuksen mukaan eurooppalaiset luottavat viranomaisiin ja rahoituslaitoksiin enemmän kuin yksityisen sektorin yrityksiin. Tampereen yliopiston tutkimushankkeen (Tampereen yliopisto 2015) tulokset ovat samansuuntaisia: tutkimuksen osallistujista 72 % luotti pankkien ja vakuutusyhtiöiden, 69 % terveydenhuollon palvelujen ja 59 % Suomen valtion salassapitokykyyn. Vain alle viidennes tutkimuksen vastaajista luotti Googleen tai Facebookiin

Kim, Song, Braynov ja Rao (2005) esittävät, että sähköisten palveluntarjoajien ja akateemisen tutkimuksen näkökulmat luottamuksen rakentumisesta poikkeavat toisistaan. Palveluntarjoajilla on taipumus keskittyä ensisijaisesti teknologia-alustoihin ja niiden rajoitteisiin, tuotteen ominaisuuksiin sekä luottamuksen rakentamisen teknisiin ratkaisuihin. Akateeminen tutkimus on puolestaan keskittynyt perustavanlaatuisen luottamuksen syntymekanismiin (engl. *fundamental trust-building mechanism)*, siihen, miten se vaikuttaa kuluttajan ostokäyttäytymiseen verkossa sekä sähköisen tiedon luotettavuuteen ja uskottavuuteen. Cazier, Shao ja Luis (2006) havaitsivat tutkimuksessaan arvoristiriitojen vähentävän luottamusta, ja he korostavat kuluttajan sekä palveluntarjoajan arvojen yhteneväisyyden merkitystä luottamuksen rakentumisessa.

Koehn (2003) on tutkinut luottamusta verkkopalveluissa luottamuskäsitteen ja parhaiden käytänteiden näkökulmasta. Tutkimus luokittelee luottamuksen neljään tyyppiin. Päämäärähakuinen luottamus (engl. *goal-based trust)* syntyy osapuolten yhteisestä päämäärästä tai yhteisistä tavoitteista. Luottamusosapuolet eivät ole kiinnostuneita toistensa identiteetistä tai tarpeista, paitsi siinä määrin kuin ne johtavat samaan päämäärään. Laskelmoiva luottamus (engl. *calculative trust*) perustuu luottamuksen luottamusosapuolen arvioon luottamussuhteen riskeistä ja hyödyistä. Luottamustyyppinä laskelmoiva luottamus on tavanomainen liiketoiminnallisissa

suhteissa, ja nojaa usein sopimuksiin, jolloin luottamusta vahvistaa myös juridinen sitovuus. Tunnettavuusperustainen luottamus (engl. *knowledge-based trust)* perustuu luottamusosapuolten myönteiseen kuvaan toisistaan, mutta etenkin verkkopalveluissa myös vertais- tai editoriarvioihin sivuston luotettavuudesta. Google on tutkinut tunnettavuusperustaisen luottamuksen mittaamisen metodiikkaa websivustojen luotettavuuden arvioinnissa ja faktatarkistuksessa. Tutkimus ehdottaa uuttaa menetelmää www-sivustojen laadulliseen tarkasteluun, ja tuloksia kuvataan lupaaviksi (Dong, Gabrilovich, Murphy, Dang, Horn, Lugaresi & Zhang 2015). Korkeimmaksi luottamuksen asteeksi Koehn (2003) katsoo kunnioitukseen perustuvan luottamuksen (engl. *respect-based trust*). Tällainen luottamussuhde syntyy ja vahvistuu, kun osapuolien välillä vaikuttavat samansuuntaiset kiinnostuksen kohteet ja halu käydä avointa keskustelua toistensa päämäärien ymmärtämiseksi. Osapuolet ovat avoimia kritiikille, eivätkä pyri hyötymään tai hyväksikäyttämään toisiaan. Esimerkkinä tällaisesta luottamussuhteesta Koehn (2003) käyttää ystävyyssuhdetta.

Beldadin, Jongin ja Steehouderin (2010) mukaan verkkoasioinnin yhteydessä tapahtuva online-luottamuksen solmiminen voidaan määritellä sidosryhmien riippuvuussuhteena palvelun-tarjoajaan. Luottamussuhteen rakentavia tekijöitä ovat ulkoiset piirteet, kuten yrityksen sähköiset tietovälineet (engl. *electronic medium*), relatiiviset bisnesaktiviteetit ja yrityksen verkkosivusto kokonaisuudessaan. Ruotsalainen, Blobel, Seppälä, Sorvari & Nykänen (2012) esittävät luottamuksen rakentamisen edistämiseksi neljää käytäntöä: kolmannen osapuolen sertifikaatit, brändäys, tietolähteen omistajan julkistaminen ja itsesäädeltävät käytännöt.

Koehn (2003) jakaa osin Kimin ym. (2005) näkemyksen verkkokaupan keskittymisestä teknisiin tiedonsuojausratkaisuihin, kuten sertifiointiin, mutta nostaa esiin myös brändiluottamuksen. Koehn korostaa, että vain vähän on tehty kunnioitukseen perustavan luottamuksen (engl. *respect-based trust)* edistämiseksi, jonka hän katsoo kaikkein pitkäkestoisimmaksi ja siten tärkeimmäksi luottamuksen muodoksi.

The Cue Utilization -teoriaa (Hu, Wu, Wu & Zhang 2010) soveltamalla tuote- tai palvelusivusto lähettää kuluttajalle alitajuisia impulsseja, joiden perusteella hän arvioi tuotteen laadun. Impulssit luokitellaan kohdistuvaksi ulkoisesti tai sisäisesti tuotteeseen. Ulkoiset impulssit (engl. *extrinsic cues*) ovat tuoteliitännäisiä ominaisuuksia, jotka voivat muuttua, kun taas sisäiset impulssit (engl. *intrinsic cues*) ovat itse tuotteen ominaisuuksia, jotka hallitsevat ulkoisia impulsseja. Jos sisäiset impulssit puuttuvat, kuluttaja huomioi ulkoiset impulssit ja arvioi tuotteen laadun niiden perusteella (Hu ym. 2010). Teoriaa voidaan soveltaa esimerkiksi tilanteeseen, jossa asiakas valitsee verkkopalvelun ja asioi siellä ensimmäistä kertaa. Kuluttajan näkökulmasta palvelua käytettäessä sisäiset impulssit rakentuvat pääosin sivustoilla olevien tuotteiden ja brändien perusteella, kun taas ulkoiset impulssit ovat riippuvaisia asiakasarvioinneista ja kolmannen osapuolen tarjoamista ulkoisista sertifikaateista. Peräkkäiset sisäiset ja ulkoiset impulssit vaikuttavat siihen, kuinka luotettavaksi kuluttaja asioinnin verkkopalvelussa kokee.

2.2. Tiedonsuojausominaisuudet ja -sertifikaatit

Tiedonsuojausominaisuudet

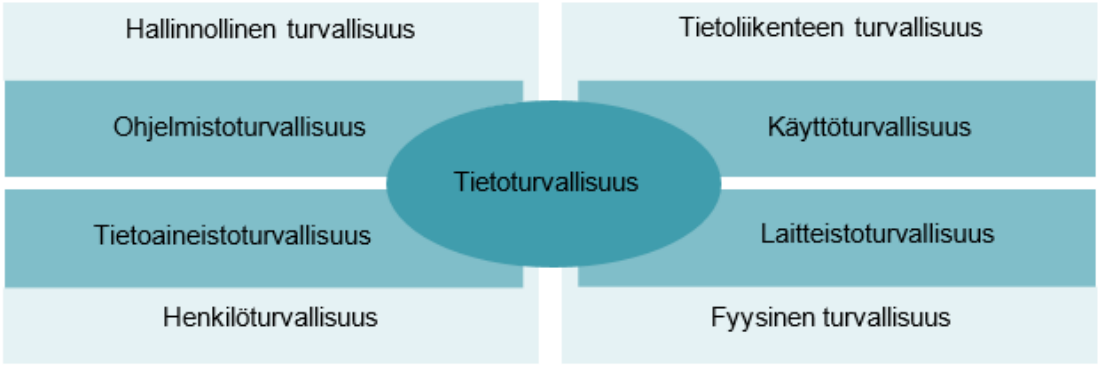
Tiedonsuojausominaisuuksia ja -menetelmiä on monenlaisia, ja niiden kehitystä ohjaavat muun muassa lainsäädäntö sekä alakohtaiset säädökset ja normit. Tässä kappaleessa tarkastellaan tarkemmin, mistä tietoturvallisuus ja tietosuoja muodostuvat.

Tiedonsuojausominaisuuksien avulla on voitava varmistaa säilytettävän tai käsiteltävän tiedon luottamuksellisuus, eheys ja saatavuus. Tietoturvan peruskäsitteiden mukaisesti suojattavaan tietoon saattaa kohdistua haavoittuvuuksia, joita hallitaan suojauskeinoilla uhkien pienentämiseksi tai haavoittuvuuksien paikkaamiseksi. (Holmström 2003.)

Tilastojen ja tutkimusten (mm. Marr 2015) mukaan sähköisten palvelujen käyttö ja etenkin eri tietokantojen käyttö lisääntyvät huomattavasti. Niiden sisältämät datamassat kasvavat räjähdysmäisesti vuosi vuodelta ja on arvioitu, että kahden viime vuoden aikana ihmiskunta on tuottanut enemmän dataa kuin aikaisemmin tähän asti on ollut olemassa. Tämä asettaa haasteita tiedon suojaamiselle, ja siksi tiedonsuojausominaisuuksia tarjoavien palveluntarjoajien tarve on jatkuvassa kasvussa. Aiemmin fyysisesti toimitettujen palveluiden digitalisoituessa ongelmaksi muodostuu se, kuinka luodaan luotettava vuorovaikutussuhde käyttäjän ja palveluntarjoajan välille. Viestintäviraston pääjohtaja (ent. Kyberturvallisuuskeskuksen johtaja) Kirsi Karlamaa (2015) on todennut, että kuluttajat ratkaisevat tällöin palvelun elinkelpoisuuden, ja tässä avaintekijänä on tietoturvallisuus.

Digitalisaatio mahdollistaa täysin uudenlaisia liiketoimintamuotoja, mutta se myös luo parempia ja luotettavampia palveluketjuja, sillä se vähentää joidenkin fyysisten ja manuaalisten työvaiheiden määrää (valtionvarainministeriö 2016a). Samalla kuitenkin huomioitavien tietoturvaseikkojen ja niihin liittyvien töiden määrä lisääntyy, sillä palvelumuotojen digitalisoituessa niiden käyttö on mahdollista missä ja milloin tahansa. Esimerkiksi loppukäyttäjän fyysisen tietoturvan merkitys korostuu etenkin terveydenhuoltopalveluiden sähköisissä palveluissa (Virtanen 2016).

Tietoturvallisuudesta puhuttaessa tarkoitetaan monen turvallisuuden osa-alueen ja käyttäjien summaa. Tietoturvallisuus jaetaan tyypillisesti ulkoiseen ja sisäiseen tietoturvallisuuteen: ulkoiseen osa-alueeseen kuuluvat hallinnollinen, tietoliikenne-, fyysinen ja henkilöturvallisuus ja sisäiseen osa-alueeseen lasketaan ohjelmisto-, laitteisto-, tietoaineisto- ja käyttöturvallisuus (kuva 2).



Kuva 2: Tietoturvallisuuden osa-alueet (Valtionhallinnon tietoturvallisuuden johtoryhmä 2008).

Tietoturvallisuuden kehittäminen edellyttää laaja-alaista näkökulmaa. Yksittäisen osa-alueen kehittäminen voi lisätä toisen haavoittuvuuksia. Esimerkiksi liiallinen keskittyminen tietoverkkoturvallisuuden kehittämiseen jättää hallinnollisen tietoturvan jälkeen. Tämän takia riskianalyyseja on hyvä tehdä myös hankkeiden toteuttamisen jälkeen, kun on kerätty tietoa toimintojen uusista vaikutuksista. Tämä koskee etenkin uusien järjestelmien käyttöönottoa (Jourdan, Rainer, Marshall & Ford 2010). Esimerkiksi Kelan etäkuntoutusselvitys tarkastelee sähköisten palveluiden tuottamiseen liittyviä haasteita ja mahdollisuuksia kuntoutuksen näkökulmasta, myös tietoturvaseikat huomioiden. Kuntoutuksen etätarjontaan sisältyvät omat erityispiirteensä, mutta selvitys osoittaa yleispätevästi kaikessa terveydenhuollon sähköisissä palveluissa huomioitavat salassapito- ja turvallisuusvelvoitteet (Salminen, Hiekkala & Stenberg 2016).

Tiedonsuojausominaisuudeksi voidaan katsoa teknisen tai fyysisen suojausominaisuuden lisäksi myös velvoittava lainsäädäntö. Sosiaali- ja terveydenhuoltoalalla tietosuojan ja tietoturvallisuuden merkitys korostuu, sillä käsiteltävä aineisto sisältää tyypillisesti arkaluontoista aineistoa, kuten potilas- tai henkilötietoja. Esimerkiksi asiakastietojen hallinnassa ja käsittelyssä sovelletaan terveydenhuollon laitteita ja tarvikkeita sekä niiden käytön turvallisuutta koskevan lain (629/2010) lisäksi muun muassa seuraavia lakeja (sosiaali- ja terveysministeriö 2016):

- Henkilötietolaki (523/1999)
- Laki potilaan asemasta ja oikeuksista (785/1992)
- Arkistolaki (831/1994)
- Potilasasiakirjoja koskeva asetus (298/2009)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (255/2015)
- Laki sähköisestä lääkemääräyksestä sekä terveydenhuoltolaki (61/2007).

Suomessa on vuonna 2009 tullut voimaan laki *vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista* (617/2009). Vahvassa sähköisessä tunnistamisessa on lain mukaan käytettävä vähintään kahta identiteetin todentamistekijää (laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista. 617/2009). Sosiaali- ja terveyspalveluissa hyödynnetään lähes poikkeuksetta vahvaa tunnistamista, ja tunnistamiseen käytetään henkilön tiedossa olevien todentamistekijöiden (esimerkiksi käyttäjätunnuksen ja salasanan yhdistelmän) lisäksi henkilön hallussa olevaa todentamistekijää (esimerkiksi verkkopankkitunnuksia). Tunnistamisessa yleisesti käytettyjä menetelmiä ovat muun muassa pankkien käyttämät verkkopankkitunnukset, Väestörekisterikeskuksen kansalaisvarmenne ja teleyritysten mobiilivarmenteet (Viestintävirasto, 2013).

Terveyspalveluiden ja digitaalisten hyödykkeiden osalta keskeisiä lakeja ovat laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) sekä laki sähköisestä lääkemääräyksestä (61/2007). Ensin mainitun tarkoituksena on edistää sosiaali- ja terveysalan asiakastietojen tietoturvallista sähköistä käsittelyä. Se sisältää muun muassa yleisiä vaatimuksia asiakastietojen sähköisestä käsittelystä, säännöksiä potilastietojen sähköisestä luovuttamisesta, säännöksiä asiakkaan tiedonsaantioikeudesta ja potilaan informoimisesta, vaatimuksia tietojärjestelmille sekä säännöksiä terveydenhuollon valtakunnallisista tietojärjestelmäpalveluista, omavalvonnasta ja vaatimustenmukaisuuden arvioinnista. Julkishallinnon sähköisten palveluiden osalta keskeistä lainsäädäntöä ovat lisäksi laki sähköisestä asioinnista viranomaistoiminnassa (13/2003) ja sähköisen viestinnän tietosuojalaki (516/2004). Rekisterinpitäjän ja tietosuojavastaavan aseman ja tehtävän osalta mainittu lainsäädäntö velvoittaa kuten tavanomaistenkin palveluiden kohdalla.

Sähköistä lääkemääräystä koskevan lain (61/2007) tarkoituksena on säännellä järjestelmää, jossa potilaiden lääkemääräykset voidaan tallentaa sähköisesti valtakunnalliseen reseptikeskukseen. Reseptikeskukseen tallennetut lääkemääräykset voidaan näin toimittaa potilaalle hänen valitsemaansa apteekkiin hänen haluamanaan ajankohtana. Lain tarkoituksena on myös parantaa potilas- ja lääketurvallisuutta. Sähköisellä lääkemääräyksellä tarkoitetaan tässä kontekstissa tietojenkäsittelylaitteella laadittua lääkemääräystä, joka siirretään tietoverkkoja käyttäen reseptikeskukseen.

Sosiaali- ja terveydenhuollon digitaaliseen toimintaan kohdistuu paljon vaatimuksia, ja näiden noudattamista myös valvotaan laajasti. Kela on vastuussa Kanta-palveluihin liittyvien järjestelmien testauksesta. Valvira valvoo ja edistää tietojärjestelmien käyttötarkoituksen mukaista käyttöä ja vaatimuksenmukaisuutta sekä ylläpitää julkista sosiaali- ja terveysalan tietojärjestel-

märekisteriä. Terveyden ja hyvinvoinnin laitos tuottaa ja ylläpitää vaatimuksiin ja omavalvontaan liittyviä määräyksiä ja ohjeita (Julkisen hallinnon tietohallinnon neuvottelukunta JUHTA 2012). Myös tietojärjestelmien valmistajien toimintaan liittyy Valviran taholta erilaisia vaatimuksia ja velvoitteita. Ensinnäkin järjestelmissä on otettava huomioon sosiaali- ja terveydenhuollon tietojärjestelmien vaatimukset, jotka liittyvät tietoturvaan, toiminnallisuuteen ja yhteentoimivuuteen. Kanta-palveluihin liittyvissä järjestelmissä osa vaatimuksista todennetaan sertifioinnin kautta. Toiseksi palveluntarjoajia koskee myös velvoite ilmoittaa Valviralle asiakas- ja potilastietojen käsittelyyn tarkoitetuista tietojärjestelmistä, jotka otetaan tuotantokäyttöön (Kanta 2016).

Sertifikaatit

Tietoturvan näkökulmasta verkkoasioinnissa painotetaan yksityisyyttä, turvallisuutta ja transaktioiden integriteettiä. Tietoturvasertifikaattien avulla pyritään todentamaan näistä aspekteista yksi tai useampia. Sertifikaatilla halutaan turvata paitsi käyttäjän, myös palveluntarjoajan integriteetti. Sertifikaatin symboli verkkoselaimen osoiterivillä takaa sen, että sivusto käyttää salausprotokollaa, esim. Transport Layer Security (TLS). Voimassaolevan sertifikaatin indikaattorina on vihreä lukko verkkosivun osoitteen vieressä (Hu ym. 2010). TLS-protokollaa voidaan hyödyntää muun muassa tiedonsiirron suojaamiseen käyttäjän ja palvelimen välillä HTTP-protokollaan yhdistettynä. HTTPS-alkuiset (Hypertext Transfer Protocol Secure) verkkosivut ovat varmennettuja ja akkreditoitu todentaja on myöntänyt niille sähköisen sertifikaatin.

Sähköistä luotettavuutta ja tietosuojakäytäntöjen soveltamista ilmentävät web-sertifikaatit, kuten TRUSTe, WebTrust, VeriSign ja BBBOnline, näkyvät websivustoilla symboleina, jotka viestivät sivuston käytänteiden olevan yhdenmukaisia ajantasaisen tietosuojalainsäädännön puitteissa ja riippumattoman kolmannen osapuolen katselmoimia. Näiden niin kutsuttujen WASS-sertifikaattien (Web Assurance Seal Service) vaikutusta kuluttajakäyttäytymiseen on tutkittu melko paljon 2000-luvun ensimmäisellä puoliskolla.

Hu ym. (2010) tarkastelivat WASS-sertifikaattien merkitystä vertailemalla tekaistujen ja aitojen sertifikaattien vaikutusten eroja. Tutkimuksen mukaan käyttäjät, jotka tuntevat verkkosivulla esitetyn sertifikaatin entuudestaan (esim. markkinoinnin kautta), osoittivat vertailuryhmää suurempaa luottamusta sivustoon. Edelleen Hun ym. (2010) mukaan tekaistukin sertifikaatti lisäsi ostopäätökseen päätymisen todennäköisyyttä. Mikään sertifikaateista ei osoittautunut merkittävästi muita enemmän luottamusta herättäväksi.

Kim ym. (2008) ovat tarkastelleet tiedotuksen merkitystä WASS-sertifikaattien tuottamassa luottamuskokemuksessa. Tutkimuksessa todettiin, että luottamuskokemuksen ja sertifikaatin ja sen suojausominaisuuksien tunnettuuden välillä on selkeä yhteys. Kuluttajat, joiden tietoisuutta tietoturva- ja tietosuojariskeistä sekä WASS-sertifikaateista kasvatettiin, kokivat sertifikaatit vertailuryhmää merkittävämmiksi. Tietoturva- ja tietosuojariskeistä vähemmän tietoisen kohderyhmän luottamusta voi olla mahdollista rakentaa brändiluottamuksen kautta, joka Chaudhurin ja Holbrookin (2001) mukaan vähentää verkkoympäristön aiheuttamaa epävarmuutta.

Eräänä esimerkkinä kolmannen osapuolen myöntämästä sertifikaatista toimii Kansallinen Terveysarkisto (Kanta), johon liittyviltä järjestelmiltä vaaditaan sertifiointi. Kanta-sertifiointi koskee sekä Kanta-palveluita että Kanta-välityspalveluita. Sertifioinnin avulla todennetaan tietojärjestelmään kohdistuvien, muun muassa tietoturvaan, toiminnallisuuteen ja yhteentoimivuuteen liittyvien vaatimusten täyttyminen. Osana sertifiointia suoritetaan yhteistestaus Kelan Kanta-palvelujen kanssa ja tietoturva-auditointi Viestintäviraston hyväksymän arviointilaitoksen kanssa.

Hyväksytyn sertifioinnin tuloksena tietojärjestelmä tai välityspalvelu saa asiakastietolain mukaisen todistuksen, joka on oltava jokaisella Kanta-palveluihin liitettävällä järjestelmällä. Sertifiointi on uusittava määräajoin, vaatimusten muuttuessa tai merkittävien järjestelmämuutosten yhteydessä. Vaatimuksiin linkittyy myös omavalvontasuunnitelma, joka kaikkien sähköisesti asiakas- ja potilastietoja käsittelevien sosiaali- ja terveyspalveluita tuottavien organisaatioiden on laadittava (Kanta 2016).

Sähköisten hyödykkeiden hankintaan ja käyttöön liittyy usein tunnistautumista tai muuta siihen verrattavaa suojattavan tiedon siirtoa. Esimerkiksi terveydenhuoltopalveluissa käsitellään käyttäjien henkilötietoja ja muita arkaluontoisia, salassa pidettäviä tietoja, minkä vuoksi tietosuoja korostuu toiminnassa erityisesti. Tämä on tärkeää myös käyttäjien luottamuksen säilymisen kannalta. Tietosuojavaatimusten osalta merkittävää on se, missä palvelussa edes väliaikaisesti tallennettava tieto fyysisesti sijaitsee. Mikäli tietoja siirretään EU:n tai ETA:n ulkopuolelle tai EU:n tai ETA:n alueella sijaitseviin tietoihin on pääsy EU:n tai ETA:n ulkopuolelta, tulee näille tiedonsiirroille hankkia riittävät siirtotakeet, esim. rekisteröityjen nimenomaisella suostumuksella, EU-komission hyväksymiä mallilausekkeita käyttämällä tai Privacy Shield -järjestelmän turvin (EUR-Lex 2016).

EU:n tietosuoja-asetuksen 42. artiklassa on erikseen kannustettu ottamaan käyttöön tietosuojaa koskevia sertifiointimekanismeja, tietosuojasinettejä ja merkkejä. Tarkoituksena on osoittaa, että rekisterinpitäjät ja henkilötietojen käsittelijät noudattavat EU:n yleistä tietosuoja-asetusta käsitellessään henkilötietoja. Sertifiointi takaa myös rekisterinpitäjien ja henkilötietojen käsittelijöiden ammattitaidon säilymisen, sillä se on uusittava vähintään kolmen vuoden välein. Sertifiointi on kuitenkin tietosuoja-asetuksen mukaan vapaaehtoista, ja sen on oltava saatavilla läpinäkyvän menettelyn perusteella. Sertifioinnin tarkoituksena ei ole vähentää rekisterinpitäjän tai henkilötietojen käsittelijän vastuuta henkilötietojen käsittelyyn liittyvän lainsäädännön noudattamisesta (EUR-Lex 2016).

Tällä hetkellä tietosuojaan liittyviä henkilösertifikaatteja myöntää International Association of Privacy Professionals (IAPP), joka on maailman suurin tietosuoja-ammattilaisten järjestö. IAPP:n kautta on mahdollista suorittaa CIPP-, CIPM- ja CIPT-sertifikaatti. CIPP-sertifiointi (Certified Information Privacy Professional) edellyttää suorittajaltaan tietosuojalainsäädännön sekä tietosuojaan liittyvien sääntöjen, käytänteiden ja standardien kokonaisvaltaista osaamista. CIPM-sertifiointi (Certified Information Privacy Manager) taas todistaa, että suorittaja kykenee tietosuojasääntöjen hallitsemisen lisäksi toteuttamaan niitä organisaatiossa. CIPT-sertifiointi (Certified Information Privacy Technologist) on laadittu teknologian ammattilaisille, jotka kehittävät tietosuojaa organisaatioissa aivan IT-tasolta lähtien (IAPP 2016).

2.3. Kirjallisuuskatsauksen yhteenveto ja lähtökohtaolettamat

Kirjallisuuskatsauksen perusteella sähköisiä palveluita kohtaan koettu luottamus vahvistui, mikäli palvelun tietoturva- ja tietosuojakäytänteet oli sertifioinut jokin kolmas osapuoli. Mielenkiintoista on huomata, että loppukäyttäjän kokema luottamus vahvistui riippumatta sertifioinnin aitoudesta tai siitä, kuka tämä kolmas osapuoli on.

Sertifiointeja enemmän koettua luottamusta vaikuttaisi parantavan palvelutarjoajan brändi, maine ja arvojen yhdenmukaisuus. Aktiivisesti tietosuojakäytännöistään tiedottavat ja TLS-salausta palveluissaan käyttävät Facebook ja Google olivat vähiten luotettuja tahoja (Tampereen yliopisto 2015). Sekä Eurobarometrin (European Commission 2015) että Tampereen yliopiston

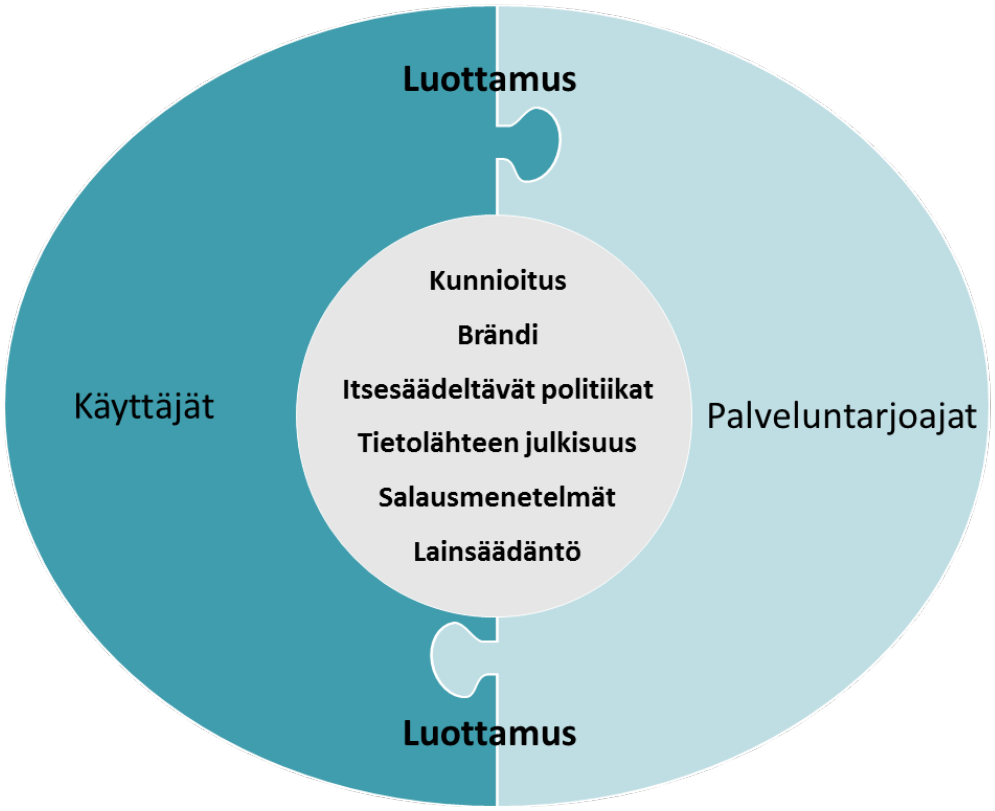
(2015) julkaisemien Yksityisyys-kyselytutkimustulosten mukaan eniten luotettuja tahoja sähköisien palvelujen tietoturvallisuuden suhteen olivat pankit, vakuutusyhtiöt ja valtionhallinto.

WASS-sertifikaattien merkitystä käyttäjäluottamuksen muodostumiseen on kirjallisuuskatsauksen perusteella tutkittu kattavasti, ja havaintojen perusteella koettu luottamus vahvistui sertifikaattipalveluiden tunnettuuden myötä. Luottamussuhteen syntymiseen riitti sertifiointileiman olemassaolo, eikä sen aitoudella ollut merkitystä ostopäätöksen syntymiseen. Epäselväksi jäi kuitenkin TLS -salausmenetelmien tunnettuus sekä se, ovatko käyttäjät tietoisia siitä, ettei salauksella suojatun yhteyden käyttö ole tavallista yhteyttä vaikeampaa.

Koehn (2003) määrittää kunnioitukseen perustuvan luottamuksen kaikkein korkeimmaksi ja kestävimmäksi luottamusmekanismiksi verkkopalveluissa. Kunnioitukseen perustuvan luottamuksen saavuttaminen vaatii palveluntarjoajalta avoimuutta ja moitteetonta mainetta sekä käyttäjälle mahdollisuutta vaikuttaa omien tietojensa käsittelyyn ja tehdä niitä koskevia päätöksiä. Ruotsalainen ym. (2015) esittävät itsesäädeltävät käytännöt merkityksellisenä ominaisuutena käyttäjäluottamuksen rakentamisessa, ja näkemystä tukevat Yksityisyys-kyselytutkimuksen (Tampereen yliopisto 2015) tulokset, joiden mukaan peräti 87 % vastaajista haluaisi itse määritellä, mihin tarkoitukseen henkilötietoja käytetään.

Lainsäädännöllinen pohja tunnistettiin tutkimuksessa paitsi luottamustekijäksi, myös varsin ajankohtaiseksi aiheeksi Euroopan unionin uudistuneen tietosuoja-asetuksen myötä. Tietosuojalainsäädännön tunnettuus kuluttajien keskuudessa ei ollut kirjallisuuskatsauksessa osoitettavissa, mutta sen arveltiin olevan etenkin sosiaali- ja terveyspalveluiden viitekehyksessä merkityksellinen.

Keskeiset luottamusta rakentavat elementit käyttäjien ja palveluntarjoajien suhteessa on kuvattu kuvassa 3.



Kuva 3: Käyttäjien ja palveluntarjoajien välinen luottamussuhde.

Kirjallisuuskatsauksessa muodostuneen näkemyksen perusteella laadittiin seuraavat lähtökohtaolettamat kyselytutkimuksen tueksi:

1. olettama: Palvelun tarjoajan maine ja brändi ovat sertifikaatteja merkityksellisempiä luottamustekijöitä kuluttajapalveluissa.

2. olettama: Palveluiden tarjoajan tunnettuus vaikuttaa positiivisesti luottamuksen syntymiseen.

3. olettama: Käyttäjien kyky vaikuttaa palveluihin tallentamansa tiedon määrään, laatuun ja käyttöön vaikuttaa positiivisesti luottamuksen syntymiseen.

2.4. Kyselytutkimuksen tulokset

Enemmistö vastaajista totesi tunnistavansa salausta käyttävän web-sivuston (väittämä 1).

Väittämä 1. Tunnistan salausta käyttävän web-sivuston.

	1	2	3	4	5		Yhteensä	Keskiarvo
Täysin eri mieltä	5	5	15	48	79	**Täysin samaa mieltä**	152	4,26
	3,29 %	3,29 %	9,87 %	31,58 %	51,97 %			

Neljännes vastaajista ei osannut sanoa, luottavatko he verkkosivustoon, vaikka se käyttäisikin salausta, ja lähes kymmenesosa vastaajista ei kokenut salausta käyttävää sivustoa lainkaan luotettavana (väittämä 2).

Väittämä 2. Koen salausta käyttävällä web-sivustolla asioinnin luotettavaksi.

	1	2	3	4	5		Yhteensä	Keskiarvo
Täysin eri mieltä	6	6	36	82	22	**Täysin samaa mieltä**	152	3,7
	3,95 %	3,95 %	23,68 %	53,95 %	14,47 %			

Kyselyn kysymykset kolme, neljä ja viisi käsittelivät vastaajan kykyä ja halua hallinnoida itseään koskevia tietoja verkkopalveluissa. Suurin osa vastaajista (yli 75 %) ei kokenut voivansa riittävästi vaikuttaa siihen, kuinka palveluntarjoaja käyttää palveluun tallennettuja tietoja (väittämä 3). Hieman yli puolet vastaajista (50,7 %) ei tiennyt, kuinka ja mistä he voivat pyytää omien tietojensa poistamista tai tarkistamista sähköisistä palveluista (väittämä 4). Yli 50 % vastaajista halusi itse määritellä, miten heistä kerättyjä ja heidän ilmoittamiaan tietoja tulisi käsitellä (väittämä 5).

Väittämä 3. Koen voivani riittävissä määrin vaikuttaa siihen, kuinka palveluntarjoaja käyttää palveluun tallentamiani tietoja.

	1	2	3	4	5		Yhteensä	Keskiarvo
Täysin eri mieltä	49	69	25	8	1	**Täysin samaa mieltä**	152	1,97
	32,24 %	45,39 %	16,45 %	5,26 %	0,66 %			

Väittämä 4. Tiedän, kuinka ja mistä pyytää omien tietojeni poistamista tai tarkistamista sähköisestä palvelusta.

	1	2	3	4	5		Yhteensä	Keskiarvo
Täysin eri mieltä	19	58	42	24	9	**Täysin samaa mieltä**	152	2,64
	12,5 %	38,16 %	27,63 %	15,79 %	5,92 %			

Väittämä 5. Haluan itse määritellä, mihin tarkoitukseen henkilötietojani käytetään.

	1	2	3	4	5		Yhteensä	Keskiarvo
Täysin eri mieltä	0	4	17	34	97	**Täysin samaa mieltä**	152	4,47
	0 %	2,63 %	11,18 %	22,37 %	63,82 %			

Yli puolet vastaajista ei kokenut, että palvelut ilmoittaisivat selkeästi käyttämistään tietosuojakäytänteistä (väittämä 6).

Väittämä 6. Koen, että sähköisissä palveluissa ilmaistaan selkeästi, millaisia tietosuojakäytänteitä palvelu soveltaa.

	1	2	3	4	5		Yhteensä	Keskiarvo
Täysin eri mieltä	27	69	39	15	2	**Täysin samaa mieltä**	152	2,32
	17,76 %	45,39 %	25,66 %	9,87 %	1,32 %			

Kysyttäessä digitaalisten terveyspalvelujen käytön luotettavuutta, noin 20 prosenttia vastaajista ei kokenut näitä luotettavana (väittämä 7).

Väittämä 7. Koen digitaalisten terveyspalveluiden käytön luotettavaksi.

	1	2	3	4	5		Yhteensä	Keskiarvo
Täysin eri mieltä	8	22	34	70	18	**Täysin samaa mieltä**	152	3,45
	5,26 %	14,47 %	22,37 %	46,05 %	11,84 %			

Yli puolet vastanneista ilmoitti, että heille sähköisten palveluiden käytössä merkityksellistä on, kuka palveluita tarjoaa ja kuinka tunnettu palveluntarjoaja on (väittämä 9). Vastaajien näkemykset tukevat KPMG:n teettämää kansainvälistä tutkimusta, jossa tutkittiin kuluttajakäyttäytymistä sähköisessä kaupankäynnissä. Tutkimuksen mukaan tärkein kriteeri hinnan jälkeen oli palveluntarjoajan tunnettuus. (KPMG 2017). Sähköisten terveyspalveluiden käytön luotettavuuteen liittyvässä kysymyksessä vastaajista viidennes ilmoitti suhtautuvansa siihen epäillen, eikä luottamussuhdetta palveluun ollut. Yli puolella vastaajista sen sijaan oli luottamussuhde sähköisiin terveyspalveluihin.

Palveluntarjoajan identiteetti ja tunnettuus osoittautuivat merkityksellisiksi (väittämät 8 ja 9). Vastaajista 76 % koki palveluntarjoajan identiteetin merkitykselliseksi. Vastaajista 73 % koki merkitykselliseksi sen, että palveluntarjoaja on tunnettu toimija (jokseenkin samaa mieltä tai täysin samaa mieltä).

Väittämä 8. Minulle on merkityksellistä, kuka on palveluntarjoaja.

	1	2	3	4	5		Yhteensä	Keskiarvo
Täysin eri mieltä	0	11	25	53	63	**Täysin samaa mieltä**	152	4,11
	0 %	7,24 %	16,45 %	34,87 %	41,45 %			

Väittämä 9. Minulle on tärkeää, että palveluntarjoaja on tunnettu toimija.

	1	2	3	4	5		Yhteensä	Keskiarvo
Täysin eri mieltä	1	14	25	67	45	**Täysin samaa mieltä**	152	3,93
	0,66 %	9,21 %	16,45 %	44,08 %	29,61 %			

Vastaajien keskuudessa tietous tietosuojalainsäädännön vaikutuksista tietojen käsittelyyn jakaantui tasaisesti (väittämä 10). Alle kymmenen prosenttia (9,87 %) vastaajista arvioi, ettei tunne tietosuojalainsäädäntöä lainkaan, ja vastaavasti noin kymmenen prosenttia (9,21 %) vastaajista ilmoitti tuntevansa tietosuojalainsäädäntöä erittäin hyvin. Suurin osa vastaajista (36,84 %) ilmoitti tuntevansa tietosuojalainsäädäntöä kohtalaisesti.

Väittämä 10. Tunnen tietosuojalainsäädännön vaikutuksen tietojeni käsittelyyn.

	1	2	3	4	5		Yhteensä	Keskiarvo
Täysin eri mieltä	15	56	32	35	14	**Täysin samaa mieltä**	152	2,85
	9,87 %	36,84 %	21,05 %	23,03 %	9,21 %			

2.5. Yhteenveto

Neljännes kyselytutkimuksen vastaajista ei osannut sanoa, luottavatko he verkkosivustoon, vaikka se käyttäisikin salausta. Tutkimuksessa ei oteta kantaa siihen, miksi käyttäjät eivät luota (tai eivät osaa sanoa luottavatko he) salausta käyttävään sivustoon. Vaikka suuri osa vastanneista koki tunnistavansa salausta käyttävän sivuston, yksi syy epävarmuuteen ja luottamuksen puutteeseen voi olla mahdollisuus salauksen kiertämiseen esimerkiksi väärennetyn sertifikaatin avulla.

Sertifikaattien koettiin lisäävän kuluttajien luottamusta, mutta lähtökohtaolettaman 1 mukaisesti palveluntarjoajan maine ja brändi osoittautuivat käyttäjille merkityksellisemmäksi tekijäksi luottamuksen rakentumisessa. Tutkimustulokset myös vahvistavat lähtökohtaolettaman 2, jonka mukaan palveluiden tarjoajan tunnettuus vaikuttaa positiivisesti luottamuksen syntymiseen.

Kyselytutkimuksen perusteella käyttäjien kokemus mahdollisuuksistaan vaikuttaa palveluihin jättämäänsä tietoon ja sen käsittelyyn oli vähäinen, ja kolmas lähtökohtaolettama osoittautui virheelliseksi. Loppukäyttäjän vaikutusmahdollisuudet ja niistä tiedottaminen esimerkiksi itsesäädeltävien käytäntöjen muodossa saattavat olla merkittäviä luottamuksen vahvistamisessa, mutta kuten Googlen ja Facebookin osalta osoitettiin (Tampereen yliopisto 2015), eivät ne yksinään kykene rakentamaan käyttäjäluottamusta.

Tietoturvallisuus ja tietosuoja ovat tänä päivänä niin tärkeitä asioita, että lähes jokaisen organisaation, toimialasta riippumatta, tulisi jollain tavalla ottaa ne huomioon omassa toiminnassaan. Molemmat tulisi ottaa osaksi organisaation toimintaprosesseja, joita tarkkaillaan ja kehitetään jatkuvasti. Prosessinomaisella ajattelulla ja toimintatavoilla voidaan näyttää tarvittaessa toteen, että organisaatiossa todella työskennellään asioiden kehittämisen eteen. Toteen näyttäminen on tärkeätä muun muassa voimaan tulleen EU:n tietosuoja-asetuksen (EUR-Lex 2016) vuoksi, minkä takia organisaatiolle voidaan määrätä maksettavaksi sakkoja, mikäli tietoturvallisuudesta tai tietosuoja-asioista ei ole huolehdittu vaaditulla tavalla.

Kuluttajaluottamuksen näkökulmasta ongelmallista on se, että fyysisen palvelun tai tuotteen toimittamisen mahdollistamiseksi on usein luovutettava henkilö- tai osoitetietoja. Vuonna 2016 valmistuneessa KPMG:n tietosuojaan ja yksityisyyteen liittyvässä tutkimuksessa selvisi, että suomalaiset luottavat omia henkilökohtaisia tietojaan organisaatioille helpommin kuin esimerkiksi tanskalaiset ja ruotsalaiset (KPMG 2016). Eurobarometrin kyselytutkimus (European Commission 2015) ilmentää varsin korkeaa luottamusta niin terveyspalvelujen kuin julkishallinnonkin tiedonsuojauskykyä kohtaan etenkin Pohjoismaissa, kun taas Etelä- ja Itä-Euroopassa vastaava luottamus on huomattavasti heikompaa. Suurten erojen syyt jäävät kuitenkin selittämättä, ja niiden taustalla saattaa myös olla merkittäviä rakenne-eroja julkisten palveluiden toteutuksessa.

Pohjoismaiden verrattain yhtenevä toimintaympäristö ja samankaltaiset terveydenhuoltojärjestelmät tukevat kuitenkin johtopäätöstä, jonka mukaan terveydenhoitoalan voidaan katsoa soveltuvan erityisen hyvin digitalisaation muutosajuriksi sen nauttiman korkean luottamuksen vuoksi. Huomioitavaa kuitenkin on, että tässä tutkimuksessa noin viidennes vastaajista ei kokenut digitaalisten terveyspalveluiden käyttöä luotettavana. Eräs ratkaisu tähän ristiriitaan saattaisi olla esimerkiksi KAPA-arkkitehtuurin (Kansallinen Palveluarkkitehtuuri) tiedonvälityskerroksen ja tunnistusratkaisuiden (valtionvarainministeriö 2016) luomat mahdollisuudet luottamuksen parantamiseksi digitaalisessa liiketoiminnassa.

Käyttäjän ja palveluntarjoajan arvopohjan yhdenmukaisuus sekä arvoristiriitojen välttäminen ovat merkittäviä tekijöitä luottamuksen rakentamisessa, ja niitä voidaan hyödyntää kilpailutekijänä (Cazier ym. 2006). Julkishallinnon tasoista luottamusta nauttivan välitysratkaisun hyödyt luottamuksen rakentamisessa saattavat olla merkittäviä. Jatkotutkimuksessa voisikin olla hedelmällistä selvittää KAPA:n kaltaisen julkishallinnon palvelun hyödyntämistä luottamustekijänä digitalisaatiossa.

Lähteet

Beldad, A., De Jong, M. & Steehouder, M. (2010). How shall I trust the faceless and the intagible - A literature review the antecendents of online trust. *Computers in Human Behavior*, 26(5), 857–869. doi:10.1016/j.chb.2010.03.013

Cazier, J.A., Shao, B.B. & St. Louis, R.D. (2006). E-business differentiation through value-based trust. *Information & Management*, 43(6), 718–727. doi:10.1016/j.im.2006.03.006

Chaudhuri, A., & Holbrook, M.B. (2001). The Chain of Effects from Brand Trust and Brand Affect to Brand Performance: The Role of Brand Loyalty. *Journal of Marketing*, 65(2), 81-93. doi:10.1509/jmkg.65.2.81.18255

Dong, X.L., Gabrilovich, E., Murphy, K., Dang, V., Horn, V., Lugaresi, C. & Zhang, W. (2015). Knowledge-Based Trust: Estimating the Trustworhiness of Web Sources. *Proceedings of the VLDB Endowment*, 8, 938–949. doi:10.14778/2777598.2777603

EUR-Lex. (2016). Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). Haettu 22.8.2016 osoitteesta http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FIN

European Commission. (2015). *Data Protection Report Special Eurobarometer 431*. Haettu 22.8.2016 osoitteesta http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf

European Union. (2016). *Consumer Markets Scoreboard*. Luxembourg: Publications Office of the European Union. doi:10.2838/32

Heino, I. (2016). *Yksityisyyden suoja ja luottamus sähköisissä palveluissa*. VTT Technology 256, 97. Espoo, Suomi: Teknologian tutkimuskeskus VTT Oy. Haettu 20.8.2017 osoitteesta http://www.vtt.fi/inf/pdf/technology/2016/T256.pdf

Holmström, U. (2003). *Tietoturvaan liittyviä peruskäsitteitä*. Haettu 12.9.2016 osoitteesta http://www.tml.tkk.fi/Opinnot/T-110.250/2003/titujohdanto.html

Hu, X., Wu, G., Wu, Y. & Zhang, H. (2010). The Effects of Web assurance seals on consumers initial trust in an online ventor. A functional perspective. *Decision Support Systems*, 48(2), 210, 408–410. doi:10.1016/j.dss.2009.10.004

IAPP. (2016). *IAPP Certification Programs*. Haettu 22.8.2016 osoitteesta https://iapp.org/certify/programs/

Jourdan, Z., Rainer, K., Marshall, T. & Ford, N. (2010). Investigation Of Organizational Information Security Risk Analysis. *Journal of Service Science*, 3(2), 34–36. doi:10.19030/jss.v3i2.368

JUHTA – Julkisen hallinnon tietohallinnon neuvottelukunta. (2012). Videoneuvottelun käyttö julkisessa hallinnossa. Haettu 29.9.2016 osoitteesta http://docs.jhs-suositukset.fi/jhs-suositukset/JHS168/JHS168.pdf

Kanta. (2016). Sertifiointi. Haettu 22.8.2016 osoitteesta Sertifiointi, olennaiset vaatimukset ja omavalvonta: http://www.kanta.fi/web/ammattilaisille/sertifiointi

Karlamaa, K. (2015). Tietosuoja-lehti. Haettu 28.9.2016 osoitteesta Digitaalinen turvallisuus: https://www.tietosuoja-lehti.fi/index.php?mid=2&pid=32&aid=3553

Kim, D. J., Song, Y. I., Braynov, S. B. & Rao, H. R. (2005). A multidimensional trust formation model in B-to-C e-commerce: a conceptual framework and content analyses of adademia/practitioners perspectives. *Decision Support Systems*, 40(2), 149–150. doi:10.1016/j.dss.2004.01.006

Kim, D. J., Steinfield, C. & Ying-Ju, L. (2008). Revisiting the role of web assurance seals in business-to-consumer. *Decision Support Systems*, 44(4), 1000–1015. doi:10.1016/j.dss.2007.11.007

Koehn, D. (2003). The Nature of and Conditions for Online Trust. *Journal of Business Ethics*, 43(1), 3–19. doi:10.1023/A:1022950813386

KPMG Global. (2016). *Companies that fail to see privacy as a business priority risk crossing the 'creepy line'*. Haettu 15.9.2016 osoitteesta KPMG: https://home.kpmg.com/sg/en/home/media/press-releases/2016/11/companies-that-fail-to-see-privacy-as-a-business-priority-risk-crossing-the-creepy-line.html

KPMG Global. (2017). *Insights: The truth about online consumers*. Haettu 15.9.2016 osoitteesta The truth about online consumers: https://home.kpmg.com/xx/en/home/insights/2017/01/the-truth-about-online-consumers.html

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista. 617/2009. (2009). Haettu 20.9.2016 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/2009/20090617

Liikenne- ja viestintäministeriö. (2016). *Maailman luotetuinta digitaalista liiketoimintaa. Työryhmän ehdotus Suomen tietoturvallisuusstrategiaksi*. Haettu 22.8.2016 osoitteesta Julkaisuja 4/2016: http://www.lvm.fi/documents/20181/877203/Julkaisuja+4-2016/795a8541-7ef5-4690-967d-a1861f1a8a48

Marr, B. (2015). *Big Data: 20 Mind-Boggling Facts Everyone Must Read*. (Forbes) Haettu 28. 11 2016 osoitteesta http://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#3e5dc0496c1d

Ruotsalainen, P. S., Blobel, B. G., Seppälä, A. V., Sorvari, H. O. & Nykänen, P.A. (2012). A Conceptual Framework and Principles for Trusted Pervasive Health. *Journal of Medical Internet Research*, 14(2), e52. doi:10.2196/jmir.1972

Salminen, A. (2011). Mikä kirjallisuuskatsaus? *Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin*. Opetusjulkaisuja 62. Vaasa: Vaasan yliopiston julkaisuja.

Salminen, A.-L.;Hiekkala, S. & Stenberg, J.-H. (2016). *Etäkuntoutus*. Helsinki: KELA. Haettu 26. 9. 2016 osoitteesta http://www.kela.fi/documents/10180/0/Et%C3%A4kuntoutus/4a50ddb8-560c-47b4-94ed-09561f6981df

Shankar, V., Urban, G.L. & Sultan, F. (2002). Online trust: a stakeholder perspective, concepts, implications and future directions. *Journal of Strategic Information Systems*, 11(3), 143–165.

Sirkkunen, E. (2015). *Raportti yksityisyys-kyselytutkimuksen tuloksista*. Tampereen yliopisto, Journalismin, viestinnän ja median tutkimuskeskus COMET. Haettu 12. 9. 2016 osoitteesta http://www.uta.fi/cmt/tutkimus/comet/tutkimus/Yksityisyys-ja-anonymiteetti-verkkoviestinnassa/index/prianokyselyraportti.pdf

Sosiaali- ja terveysministeriö. (2016). Sosiaali- ja terveysministeriö. Haettu 22.8.2016 osoitteesta Lainsäädäntö ohjaa asiakas- ja potilastietojen hallintaa: http://stm.fi/asiakas-potilastietojen-hallinta

Sosiaali- ja terveysvaliokunta. (2014). Sosiaali- ja terveysvaliokunnan lausunto 1/2014 vp. Haettu 25.8.2016 osoitteesta Sosiaali- ja terveysvaliokunnan lausunto 1/2014 vp.: https://www.eduskunta.fi/FI/vaski/sivut/trip.aspx?triptype=ValtiopaivaAsiakirjat&docid=stvl+1/2014+vp

Tampereen yliopisto. (2015). *Raportti yksityisyys-kyselytutkimuksen tuloksista*. Haettu 12.9.2016 osoitteesta http://tampub.uta.fi/bitstream/handle/10024/98537/report_on_the_result_2015.pdf?sequence=1

The Department of Health. (2016). NHS Choises Home Page. (NHS Digital) Haettu 6.9.2016 osoitteesta http://www.nhs.uk/pages/home.aspx

Valtionhallinnon tietoturvallisuuden johtoryhmä. (2008). Hankkeen tietoturvaohje, VAHTI 9/2008. Haettu 27.4.2016 osoitteesta https://www.vahtiohje.fi

Valtioneuvoston kanslia. (2015). *Ratkaisujen Suomi - Pääministeri Juha Sipilän hallituksen strateginen ohjelma* 29.5.2015, Haettu 20.9.2017 osoitteesta: http://valtioneuvosto.fi/sipilan-hallitus/hallitusohjelma

Valtionvarainministeriö. (2016a). *Digitalisaatio*. Haettu 12.9.2016 osoitteesta http://vm.fi/digitalisaatio

Valtionvarainministeriö. (2016b). *Kansallinen palveluarkkitehtuuri*. Haettu 29.9.2016 osoitteesta http://vm.fi/palveluarkkitehtuuri

Valvira. (2015). *Potilaille annettavat terveydenhuollon etäpalvelut*. Haettu 25.8.2016 osoitteesta http://www.valvira.fi/terveydenhuolto/yksityisen_terveydenhuollon_luvat/potilaille-annettavat-terveydenhuollon-etapalvelut

Viestintävirasto. (2013). *Vahva sähköinen tunnistaminen, sähköinen allekirjoitus ja varmenne*. Haettu 25.8.2016 osoitteesta https://www.viestintavirasto.fi/kyberturvallisuus/sahkoinentunnistaminen-jaallekirjoitus.html

Virtanen, T. (2016). *Tietoturva etäkuntoutuksessa*. [YouTube] KELA. Haettu 14.9.2016 osoitteesta https://www.youtube.com/watch?v=k-08CYd0U7w

LUKU 3.

Sertifiointien merkitys digitaalisten hyödykkeiden markkinoilla – luottamuksen lisääminen

Haukola Timo

Wallgren Wanda

Andersson Jenna

Kilpailu- ja kuluttajaviraston kuluttajapoliittisen katsauksen (Kilpailu- ja kuluttajavirasto 2015) mukaan markkinat monimutkaistuvat ja muutosten ennakointi muuttuu vaikeammaksi. Pitkän aikavälin muutoksia, jotka vaikuttavat sekä globaaleihin että kansallisiin markkinoihin, ovat kuluttajapoliittisen katsauksen mukaan seuraavat:

1. **Digitalisaatio** – Muuttaa muun muassa toiminnan tapoja, tavaroiden ja palveluiden perinteinen raja hämärtyy sekä jakelukanavat muuttuvat.

2. **Globalisaatio** – Tavaroita ja palveluita voidaan hankkia mistä tahansa ja hyödykkeiden alkuperä jää hämäräksi. Innovaatiot leviävät nopeasti.

3. **Fragmentaatio** – Pirstaloituminen näkyy markkinoilla asiakkaiden käyttäytymisen eriytymisenä.

4. **Kaupallistuminen ja markkinaehtoistuminen** – Muuttavat muun muassa toimijoiden perinteistä työnjakoa ja aiheuttavat näin yhteiskunnan perustoimintojen murrosta.

5. **Jakamistalous** – Tavaroiden ja palveluiden yhteiskäyttö, vaihtaminen, vuokraaminen, myyminen tai muu vastaava toiminta muuttavat käsitteitä koskien hyödykkeiden tuottamista, kuluttamista ja omistamista.

6. **Ilmastonmuutos** – Pakottaa muuttamaan totuttuja toimintatapoja, mutta tarjoaa myös mahdollisuuden uudenlaiselle liiketoiminnalle.

Kuluttajapoliittisessa katsauksessa todetaan, että em. muutoksista huolimatta suomalaisilla on vahva luottamus markkinoiden olosuhteisiin ja toimintaympäristöön. Tätä tukee myös EU:n tulostauluaineisto (European Commission 2016), jonka mukaan suomalaisten kuluttajien luottamus markkinoihin on keskimäärin vahvistunut viime vuosina. Tosin muihin Euroopan unionin maihin verrattuna suomalaiskuluttajien luottamus on heikentynyt viime vuosina televisio-, puhelin- ja Internetpalveluiden sekä ICT-laitteiden markkinoilla. Yleistyvät huijaukset heikentävät kuluttajien luottamusta markkinoiden toimivuuteen, ja elinkeinoelämässä huijaukset vääristävät kilpailua markkinoilla (Kilpailu- ja kuluttajavirasto 2015).

Luottamuksella on merkittävä rooli etenkin digitaalisten palvelumuotojen toimivuudessa; osapuolten välillä vallitseva luottamus edesauttaa tietojen jakamista ja ostospäätöksen tai inves-

toinnin tekoa ja on perusedellytys sähköiselle kaupankäynnille. Luottamus poistaa ennakkoluuloja ja turvattomuuden tunnetta palveluita käytettäessä ja on näin ollen kriittinen tekijä markkinoiden toimivuuden kannalta (McKnight;Choudhury & Kacmar 2002).

Käyttäjien luottamusta digitaalisiin hyödykkeisiin vahvistetaan pääasiassa erilaisten standardisointien ja sertifiointien myötä (Tilastokeskus 2016). Digitaalisia hyödykkeitä voivat olla esimerkiksi tallenteet, datavirta tai digitaaliset palvelut (Shapiro & Varian 1999). Standardi tarkoittaa toistuvaa toimintaa koskevaa yhteistä menettelytapaa (Suomen Standardisoimisliitto SFS ry 2016a). Sertifiointi tarkoittaa standardin mukaisten vaatimusten noudattamisen osoittamista sertifikaatein, todistuksin tai tunnuksin (Stakes 2008).

Tässä tutkimuksessa keskitytään sertifiointien ja standardointien vaikutukseen markkinoiden osapuolten välillä vallitsevaan luottamukseen. Raportin tavoitteena on kartoittaa parhaita käytäntöjä, joilla voidaan lisätä luottamusta markkinoilla osapuolten välillä, sekä kartoittaa, mikä on luotettujen hyödykkeiden taustalla vaikuttavien sertifiointi- ja standardisointielimien merkitys ICT-alan laite- ja palveluntuottajille sekä niiden asiakkaille.

Luvussa esitellään ensin tutkimustavoite ja -menetelmät, jonka jälkeen käsitellään luottamuksen rakentumista. Tämän jälkeen esitellään kirjallisuuskatsauksen keinoin löydetyt parhaat käytännöt luottamuksen lisäämiseksi terveydenhuoltoalalla. Seuraavana luvussa käsitellään edellä mainitun kirjallisuuskatsauksen yhteenveto ja tehdyn kyselytutkimuksen yhteenveto. Näiden pohjalta esitellään lopuksi yhteenveto.

3.1. Tutkimustavoitteet

Tässä luvussa esitellyn tutkimuksen tavoitteena on vastata kahteen tutkimuskysymykseen:

1) Mitä parhaita käytäntöjä voitaisiin hyödyntää luottamuksen lisäämiseen markkinoilla osapuolten välillä?

2) Mikä on luotettujen hyödykkeiden taustalla vaikuttavien sertifikaattien ja standardien merkitys ICT-alan laite- ja palveluntuottajille sekä niiden asiakkaille?

Koska markkinoilla vallitseva luottamus on aihealueena laaja, ja koska eri standardisointi- ja sertifiointimahdollisuuksia on useita, tutkimuksen näkökulmaksi on valittu terveydenhoitoala. Tästä syystä tutkimus on rajattu eri standardisointi- ja sertifiointitapojen suhteen koskemaan vain terveydenhoitoalan standardisointeja sekä sertifiointeja. Tutkimuksessa käsitellyt hyödykkeet on myös rajattu koskemaan ainoastaan digitaalisia hyödykkeitä. Näin ollen asiakkailla tarkoitetaan tässä raportissa niin terveydenhoitoalalla terveyspalveluita tarjoavia yrityksiä kuin palveluita käyttäviä asiakkaita, eli loppukäyttäjiä. Palveluntarjoajalla viitataan ICT-alan laite- ja palveluntuottajiin.

Ensimmäisen tutkimuskysymyksen osalta kartoitettiin terveydenhoitoalalla olevia parhaita käytäntöjä luottamuksen lisäämiseksi. Eri käytännöissä keskityttiin erityisesti standardisointiin ja sertifiointiin. Toisen tutkimuskysymyksen analysoimiseksi toteutettiin kyselytutkimus, jonka kysymysten teemana oli kyselyyn vastanneiden tietoturva-, tietosuoja- ja sertifiointivalveutuneisuus sekä luottamus sertifiointeja ja yrityksen verkkosivuja kohtaan.

Tutkimuksen toteutusvaiheessa on etsitty laajasti tietoa eri lähteistä. Käytettyjä hakusanoja ovat esimerkiksi ’’terveysala standardisointi’’, ’’terveysala sertifiointi’’, ’’KanTa-auditointi’’, ’’KanTa-sertifiointi’’, ”Web page security”, ”Trust certificates”, ”Consumer and digitalization of

health care” sekä ’’terveyspalvelut ja luottamus’’. Lähdetietoa on kerätty kaupallisten ja ei-kaupallisten tietokantojen lisäksi muun muassa Stakesin, Suomen Standardisoimisliiton, Kanta.fi-sivuston, sosiaali- ja terveysministeriön, Terveyden ja hyvinvoinnin laitoksen sekä liikenne- ja viestintäministeriön julkaisuista.

3.2. Luottamuksen rakentuminen

Luottamuksen rakentumista on tutkittu monesta eri näkökulmasta ja sitä voidaan kategorisoida eri tavoin (McKnight, Choudhury, & Kacmar 2002). McKnight ym. (2002) määrittelevät luottamuksen rakentumisen tarkoitettavan tilannetta, jossa henkilö muodostaa riippuvuuden kohteeseen ja/tai kohteen toimiin. He erottavat luottamuksen rakentumisessa kaksi tekijää: henkilön uskon ihmisyyteen (engl. *faith in humanity*) ja henkilön luottavaisen asenteen (engl. *trusting stance)* (McKnight ym. 2002; McKnight, Larry & Chervany 1998). Uskolla ihmisyyteen viitataan yksilön olettamuksiin siitä, että muut toimijat ovat hyväntahtoisia ja luotettavia. Luottavaisella asenteella tarkoitetaan tilannetta, jossa yksilö hyväksyy riippuvuutensa toisiin tahoihin, kunnes yksilön odotus hyväntahtoisuudesta ja reiluudesta todistetaan vääräksi. Toisin sanoen yksilö luottaa toiseen osapuoleen, kunnes hänen luottamuksensa petetään (McKnight ym. 2002).

Pennanen, Tuomaala ja Luomala (2007) esittävät, että palveluiden käyttäjien henkilökohtaiset arvot vaikuttavat siihen, miten luottamus rakentuu. Tätä tukee Cazierin, Shaon ja St. Louisin (2006) tutkimus, jossa arvoristiriitojen todetaan vähentävän luottamusta, ja he korostavat kuluttajan sekä palveluntarjoajan arvojen yhteneväisyyden merkitystä luottamuksen rakentumissa. Pennanen ym. (2007) tunnistivat kaksi luottamuksen rakentumiseen vaikuttavaa muuttujaa: ulkoiset tekijät (esim. käytetty teknologia, muut palvelun käyttäjät) ja käytösmallit (esim. ystävien kokemukset). He esittivät, että palvelujen käyttäjät arvioivat palveluiden luottamuksellisuutta ja luovat olettamuksia palvelua kohtaan muiden käyttäjien kokemusten perusteella.

Luottamusta saattavat toisinaan lisätä myös huomaamattomat tekijät, joihin emme välttämättä kiinnitä tietoisesti huomiota. Yrityksen kotisivuilla esiintyvät sertifiointi- ja standardisointimerkinnät eivät tule välttämättä aina tietoisesti huomioiduiksi, mutta saattavat silti lisätä luottamusta. Esimerkiksi nettisivujen ulkonäkö vaikuttaa suuresti luottamuksen tasoon, sillä ensivaikutelma on tärkeä (Demers 2014). Ammattimaisen näköiset ja käyttäjäystävälliset sivut lisäävät luottamusta ja saavat kävijät viihtymään pidempään sivuilla. Luottamuksen lisäämiseksi kotisivuilla on hyvä kertoa taustatietoja yrityksestä ja liiketoiminnasta. Yhteystiedot on myös tärkeä mainita. Muita luottamusta lisääviä keinoja ovat muun muassa sijoittuminen hakukoneissa mahdollisimman ylös, vaihto- ja palautusoikeudet sekä muiden asiakkaiden suositukset (Demers 2014).

3.3. Parhaita käytäntöjä luottamuksen lisäämiseen terveydenhoitoalalla

Terveyden ja hyvinvoinnin laitoksen raportissa (2016b), jossa seurataan strategian toteutumista, on huomioitu, että vain 20 prosenttia lääkäreistä piti tietojärjestelmien tuottamaa seurantatietoa luotettavana ja virheettömänä. Maaliskuussa 2016 tehdyssä Terveyden ja hyvinvoinnin laitoksen kyselytutkimuksessa keskityttiin lääkäreiden sijasta terveydenhoitoalan palveluita käyttävään väestöön. Kyselytutkimuksen mukaan enemmistö väestöstä luottaa terveydenhoitoalan palveluiden toimivuuteen (Terveyden ja hyvinvoinnin laitos 2016b).

Terveydenhoitoalan tietojärjestelmäkokonaisuuksilta vaaditaan paljon. Luottamuksen muodostamisen ja sen ylläpitämisen edellytyksenä on, että terveydenhoitoalan tietojärjestelmät ovat tietoturvallisia ja laadukkaita ja edistävät potilasturvallisuutta poikkeuksellisen tarkasti lailla säädellyllä toimialalla. Tietojen verkottunut käsittely edellyttää, että kaikki osapuolet potilaista

ammattihenkilöstöön voivat luottaa heidän käyttämäänsä tietojärjestelmäkokonaisuuden lainmukaisuuteen ja tietoturvallisuuteen (Stakes 2008).

Sosiaali- ja terveysministeriön sekä Kuntaliiton *Sote-tieto hyötykäyttöön 2020* -strategiassa linjataan sosiaali- ja terveydenhuollon digitaalisia kehityslinjoja vuoteen 2020 saakka. Vaikka sosiaalihuollon tiedonhallintaa on aktiivisesti standardoitu sisällöllisesti ja teknisesti jo pitkään, strategiassa esitetään toimenpiteenä edelleen avointen ja standardipohjaisten rajapintojen systemaattista käyttöä.

Standardisointi

Terveydenhuollossa standardien merkitys korostuu, kun halutaan varmistaa asiakkaiden tietojen yksityisyys ja säilyminen ulkoisten uhkien ulottumattomissa. Standardien käytöllä pyritään varmistamaan potilaiden turvallisuus ja terveydenhuoltoa säätelevien direktiivien vaatimusten täyttyminen sekä minimoimaan tuotekehitysriskit (Suomen Standardoimisliitto SFS ry 2016b).

Standardisointi edesauttaa toimintatapojen tehostamista, kustannusten pienentämistä ja laadun lisäämistä. Terveydenhoitoalan tietojärjestelmästandardeja tarvitaan esimerkiksi tietoturvaan liittyviin seikkoihin – esim. tietojärjestelmän käytettävyys ja luotettavuus, sähköisen allekirjoituksen käyttöpotilastietojen siirtoon, terveydenhoitoalalla käytettävien laitteiden turvalliseen yhdistämiseen, älykkäiden tietojärjestelmien luomiseen sekä järjestelmien yhteen toimivuuden ylläpitämiseen (Klein 2002).

Asiakkaita koskevat terveystiedot ovat lain mukaan salassa pidettäviä. Digitaalisten terveyspalveluiden ansiosta terveystietoja käsitellään eri järjestelmissä ja eri järjestelmien välillä. Tietojenkäsittelyn edellytyksinä eri järjestelmien välillä ovat järjestelmien tietosisältöjen ja rajapintojen standardointi, jolloin sisällöt ja rajapinnat ovat yhtenäiset ja näin ollen mahdollistavat järjestelmien välisen tiedonvaihdon (Suomen Standardisoimisliitto SFS ry 2016c). Koska terveystiedot ovat salassa pidettäviä tietoja, myös tietotekniikan standardisoinnissa on kiinnitettävä erityishuomiota tietoturva-asioihin. Potilasturvallisuutta lisäävät esimerkiksi samojen asteikkojen ja symbolien käyttäminen eri valmistajien laitteissa (Suomen Standardisoimisliitto SFS ry 2016c).

Turvallisuutta ja palvelujen vaivattomuutta lisää myös terveydenhoitoalan sanastojen ja koodien standardisointi, jonka tavoitteena on maailmanlaajuisesti yhtenäinen terveydenhoitoalan palveluiden termistö. ISO, CEN ja HL7 koordinoivat terveydenhoitoalan tietotekniikan standardisointia (Suomen Standardisoimisliitto SFS ry 2016c). Maailmanlaajuisella tasolla terveydenhoitoalan standardisointia tekee ISO/TC 215 Health Informatics -komitea, jonka standardisointikohteina ovat muun muassa laitteistot, sähköinen resepti, sanastot, potilaskertomus ja järjestelmien yhteensopivuus. Euroopan laajuisella tasolla terveydenhoitoalan standardisointia taas toteuttaa CEN/TC 251 Health Informatics -komitea, jonka kohteina ovat tietoturva, tietosisällöt, järjestelmien välinen tiedonvälitys ja yhteentoimivuus sekä sanastot. Kansainvälinen HL7-yhdistys on tehnyt sanomakuvauksien standardisointia, ja monet sen standardit on vahvistettu kansainvälisiksi ISO-standardeiksi (Suomen Standardisoimisliitto SFS ry 2016c).

Terveydenhoitoala on luonteeltaan yhteistyötä vaativaa, ja nykyisellääänkin alan eri ammattilaisten välillä sattuu kulttuurillisia yhteentörmäyksiä (Kaplan & Harris-Salamone 2009). Tähän lisättynä terveydenhuollon tietojärjestelmien standardointia vaikeuttaa järjestelmätoimittajien ja käyttäjien laaja kirjo. Eri toimittajat, tilaajat ja käyttäjät saattavat käyttää erilaisia toimintatapoja ja standardeja, mikä voi monimutkaistaa kokonaisuuden saattamista yhtenäisen standardin piiriin (Greenhalgh, Stramer, Bratan, Byrne, Russell & Potts 2010).

Sertifiointi

Sertifiointi on yksi tärkeimmistä menetelmistä, jonka avulla eri osapuolet, kuten hankkijat, käyttäjät ja kansalaiset, voidaan vakuuttaa ohjelmiston tai tietojärjestelmän lain- ja määritystenmukaisuudesta. Sertifiointi jaetaan usein henkilö-, tuote-, palvelu- ja järjestelmäsertifiointeihin (Stakes 2008).

Voittoa tavoittelematon The Health on the Net -säätiö (HON) tarjoaa sertifiointeja keskittyen terveyteen liittyvää sisältöä tarjoaviin verkkosivuihin ja verkkopalveluihin. Verkkosivuston tai palvelun HON-sertifikaatti osoittaa, että sen sisältö on luotettavaa ja terveydenhoitoalan ammattilaisten hyväksymää (Health On the Net Foundation, 2014). Terveydenhoitoalan palveluita koskeva tietojärjestelmäsertifiointi koskee muun muassa KanTa-palveluihin liittyviä tietojärjestelmiä ja KanTa-välityspalveluita. Hyväksytyn sertifioinnin osoituksena on todistus, joka osoittaa vaatimustenmukaisuuden ja joka on oltava kaikilla KanTa-palveluihin liitettävillä järjestelmillä (Kansallinen Terveysarkisto 2016).

Terveydenhoitoalalla on myös tuotesertifikaatteja, kuten esimerkiksi ISO 13485. Sertifikaatin tarkoituksena on, että laitteiden valmistajat ja käyttäjät voivat varmistua siitä, että lainsäädännön turvallisuusvaatimukset sekä asiakasvaatimukset täyttyvät laitteen koko elinkaaren ajalta (International Organization for Standardization 2016).

Palvelusertifikaatilla todennetaan palveluiden vaadittu taso. Esimerkiksi ISO 9001:2015 on globaali sertifikaatti, joka on käytössä myös terveydenhoitoalalla. Kyseinen sertifikaatti keskittyy laadunhallintaan ja laadunhallintajärjestelmiin ja huomioi myös palveluiden tuottajat (International Organization for Standardization 2015). Edellä mainittu ISO 13485 on osa ISO 9000 -sertifikaattikokonaisuutta (International Organization for Standardization 2016). Tietojärjestelmiä koskevat vaatimukset liittyvät tietoturvaan, toiminnallisuuteen ja yhteentoimivuuteen. Yhtenäisyyttä lisää myös terveydenhoitoalan vaatimus omavalvontasuunnitelmasta, mikä koskee kaikkia sähköisesti asiakas- ja potilastietoja käsitteleviä sosiaali- ja terveyspalveluita. Myös asiakas- ja potilastietojen käsittelyyn valmistettavien tietojärjestelmien valmistajia koskee velvollisuus ilmoittaa tuotantokäyttöön otettavasta tietojärjestelmästä Valviralle (Kansallinen Terveysarkisto 2016).

Yritysten välisessä verkkokaupankäynnissä yrityskumppaniin kohdistuva suora luottamus on merkittävämmässä asemassa kuin järjestelmien vakuuttaminen sertifikaateilla (Mauldin;Nicolaou;& Kovar 2006). Niin yritysten kuin yritysten ja kuluttajien välisissä suhteissa kaikki kuluttajat eivät koe verkossa tapahtuvaa rahaliikennettä verkossa tarpeeksi turvatuksi. Tässä tapauksessa sertifikaattien rooli turvallisuuden takaajina korostuu (Runyan, Smith & Smith 2008).

Merkittävässä roolissa ovat turvallisuussertifikaatteja tarjoavat organisaatiot, jotka määrittelevät ne kriteerit, jonka mukaan yritykselle myönnetään sertifikaatti (Edelman 2010). Edelman huomauttaa tutkimuksessaan, että verkkosivustojen luottamussertifikaattien myöntäjät pyrkivät joissain tapauksissa tavoittelemaan omia etujaan, jolloin on mahdollista, että myös heikkolaatuisemmat sivustot saavat käyttöönsä luottamussertifikaatteja. Kuluttajien näkökulmasta tämä kyseenalaistaa verkkosivustojen luottamussertifikaattien todellisen merkityksen. Tutkimus, jossa tarkasteltiin hotelliketjujen verkkosivustojen sertifiointien ja yleisen ulkoasun vaikutusta kuluttajaluottamukseen, vahvistaa lähtökohtaolettamaa, jonka mukaan verkkosivuston laadukkaalla ulkoasulla on merkittävä vaikutus kuluttajaluottamuksen rakentumiseen (Wang, Law, Guillet, Hung & Fong 2015). Tutkimusten perusteella voidaan olettaa, että luottamuksen rakentumista tarkasteltaessa nimenomaan verkkosivustojen huoliteltu ulkonäkö on luottamussertifikaattia merkittävämmässä asemassa.

Muut hyvät käytännöt luottamuksen lisääjinä

Auditoinnin ja arvioinnin tarkoituksina on tunnistaa, onko kohteelle asetetut määräykset ja tavoitteet saavutettu ja missä laajuudessa. Auditoinnin voi tehdä joko organisaatio itse tai ulkoinen toimija. Terveydenhoitoalalla KanTa-auditointi on välttämätön ehto organisaation liittymiselle KanTa-palveluihin, ja se jakautuu sekä järjestelmien auditointiin että organisaatioiden auditointiin (sosiaali- ja terveysministeriö 2012).

Sertifikaattien lisäksi kuluttaja voi uudella terveydenhoitoalan palveluita tarjoavalla verkkosivustolla vieraillessaan tarkastaa, käyttääkö sivusto salausprotokollaa. Suurin osa eri alojen kuluttajaluottamukseen panostavista yrityksistä käyttää SSL/TLS-protokollaa (Manik Las Das 2014). Osa luottamussertifikaateista takaa SSL-suojatun yhteyden, kuten esimerkiksi VeriSign (Runyan ym. 2008).

Verkkosivuston luotettavuuden takaa aikaisemmin käytetty SSL (Secured Sockets Layer), joka on nykyisin TLS:llä (Transport Layer Security) korvattava protokolla. Protokollat on kehitetty etenkin asiakkaan ja palvelimen välisen verkkoliikenteen salaamiseen. (Viestintävirasto 2003.) Yritys voi turvata sivustonsa myös omatoimisesti ilman kolmannen osapuolen sertifiointia (self-signed certificate) (Kappenberger 2012). On kuitenkin todettu, että omatoimisesti luodut sertifikaatit eivät ole kaikissa tapauksissa täysin turvallisia esimerkiksi niissä tapauksissa, joissa SSL/TSL-protokollat ovat joutuneet ulkopuolisen hyökkääjän kohteeksi

3.4. Kirjallisuuskatsauksen yhteenveto ja lähtökohtaolettamat

Digitalisaatio luo terveydenhoitoalalle paljon mahdollisuuksia, mutta myös uusia haasteita ja uhkakuvia. Potilastietoja kerätään useisiin eri järjestelmiin, ja tiedot saattavat kulkea jopa eri maihin. Lisäksi markkinoilla on jatkuvasti kehitteillä uusia laitteita ja apuvälineitä, jotka auttavat terveysammattilaisten työtä sekä keräävät samalla potilaista tietoa. Kaikki potilastiedot ovat luottamuksellisia, jolloin tietoturvan ja palveluiden yhtenäistämisen tarve korostuu entisestään.

Terveydenhoitoalalla käyttäjien luottamusta digitaalisiin hyödykkeisiin voidaan mahdollisesti lisätä standardisointien ja sertifiointien myötä. Standardisoinnin avulla tehostetaan toimintatapoja, pienennetään kustannuksia ja lisätään laatua. Yhtenäisten menettelytapojen, tietotekniikan ja sanastojen myötä lisätään myös turvallisuutta ja palveluiden vaivattomuutta, mikä edesauttaa käyttäjäluottamuksen syntymistä palveluita, järjestelmiä ja tuotteita kohtaan. Sertifioinnilla tarkoitetaan standardinmukaisten vaatimusten noudattamisen osoittamista, mikä voi olla myös yksi tekijä luottamuksen syntymisessä.

Kuluttajien ja loppukäyttäjien näkökulmasta luottamuksen tunne ei kuitenkaan synny yksinomaan standardisoinnin ja sertifioinnin seurauksena. Loppukäyttäjien kohdalla luottamuksen syntymiseen vaikuttavat monet muutkin asiat, kuten esimerkiksi sivustojen ulkoasu ja helppokäyttöisyys. On myös todettu, että yrityksen julkisuuskuvalla ja positiivisen brändin luoneilla yhteistyökumppaneilla on vaikutusta kuluttajaluottamuksen syntymiseen.

Kirjallisuuskatsauksen pohjalta esitimme kyselytutkimusta varten seuraavat lähtökohtaolettamat:

1) Kuluttajat kiinnittävät huomiota tietosuojaan ja tietoturvaan silloin, kun he tunnistautuvat digitaaliseen palveluun verkkopankin kautta (esim. asioidessaan rahaliikennettä

käsittelevillä sivustoilla tai terveydenhoitopalveluita käyttäessään). Näin ei ole esimerkiksi sosiaalisen median kohdalla, jolloin tietosuoja ja tietoturva jäävät toissijaisiksi.

2) Aikaisempien tutkimusten mukaan nuorien kuluttajien luottamus sertifikaatteihin on vahvahko, sillä he ovat vanhempia kuluttajia perehtyneempiä sertifikaattien arvoon. Nuorten kuluttajien luottamuksen rakentumiseen vaikuttaa valveutuneisuus.

3) Kuluttajat ovat tietoisia siitä, että standardit ja sertifikaatit todentavat yhteisesti määriteltyjen tietoturva- ja lakivaatimusten täyttymisen.

3.5. Kyselytutkimuksen tulokset

Suurin osa vastaajista (53 %) vastasi kiinnittävänsä erittäin usein huomiota tietoturvaan ja tietosuojaan käyttäessään digitaalisen palvelun maksuominaisuuksia tai tunnistautuessaan verkkopankkitunnuksilla (kysymys 1). Yksikään vastaajista ei ilmoittanut täysin laiminlyövänsä tietoturvaa ja tietosuojaa käyttäessään maksu- ja luottokorttitunnistautumiseen liitettyjä digitaalisia palveluita.

Kysymys 1. Kuinka paljon kiinnität huomiota tietoturvaan ja tietosuojaan silloin, kun käytät digitaalisen palvelun maksuominaisuuksia tai tunnistaudut verkkopankin kautta Internetissä?

	1	2	3	4	5		Yhteensä	Keskiarvo
En koskaan	0	9	19	44	80	**Erittäin usein**	152	4,28
	0 %	5,92 %	12,5 %	28,95 %	52,63 %			

Sosiaalisen median palveluita käytettäessä vastaajat kiinnittivät tietoturvaan ja tietosuojaan huomattavasti vähemmän huomiota. Vastaajista vain 17 % vastasi kiinnittävänsä huomiota tietoturvaan erittäin usein luovuttaessaan tietoja sosiaalisen median sivustoille (kysymys 2).

Kysymys 2. Kuinka paljon kiinnität huomiota tietoturvaan ja tietosuojaan silloin, kun luovutat tietojasi verkkosivustoille tai sosiaalisen median sivustoille, joiden kautta ei kulje maksuliikennettä?

	1	2	3	4	5		Yhteensä	Keskiarvo
En koskaan	3	35	41	47	26	**Erittäin usein**	152	3,38
	1,97 %	23,03 %	26,97 %	30,92 %	17,11 %			

Vastaajat kiinnittivät vähäisesti huomioita siihen, onko ulkopuolinen taho arvioinut digitaalisia hyödykkeitä tai niitä tarjoavan organisaation (kysymys 3). Vastaajista kolmannes ei koskaan kiinnitä huomiota sertifiointeihin.

Kysymys 3. Kiinnitätkö huomiota siihen, onko ulkopuolinen taho arvioinut digitaalisia hyödykkeitä tai niitä tarjoavia organisaatioita (arviointilaitoksen myöntämä sertifikaatti koskien hyödykkeen tai organisaation turvallisuutta, esim. ISO 27001)?

	1	2	3	4	5		Yhteensä	Keskiarvo
En koskaan	46	45	34	22	5	**Erittäin usein**	152	2,31
	30,26 %	29,61 %	22,37 %	14,47 %	3,29 %			

Kuitenkin lähes puolet vastaajista koki sertifiointien lisäävän heidän luottamustaan palveluita kohtaan (kysymys 4).

Kysymys 4. Kuinka paljon edellä mainittu ulkopuolisen tahon tekemä arviointi hyödykkeen tai organisaation turvallisuudesta (sertifiointi) vaikuttaa kokemaasi luottamukseen palvelua kohtaan?

	1	2	3	4	5		Yhteensä	Keskiarvo
Ei lainkaan	15	25	38	49	25	**Erittäin paljon**	152	3,29
	9,87 %	16,45 %	25 %	32,24 %	16,45 %			

Vastaajien tietämys arviointien tai sertifiointien arviointikriteeristöihin vaikuttavasta lainsäädännöstä on välttävä. Yhteensä noin 65 % vastaajista vastasi tietävänsä vaikuttavasta lainsäädännöstä erittäin vähän tai ei lainkaan. Vain noin kymmenesosa vastaajista ilmoitti tietävänsä arviointien ja sertifiointien arviointikriteeristöt erittäin hyvin.

Kysymys 5. Kuinka tietoinen olet edellä mainittujen arviointien tai sertifiointien arviointikriteeristöistä ja niihin vaikuttavasta lainsäädännöstä?

	1	2	3	4	5		Yhteensä	Keskiarvo
En ollenkaan tietoinen	54	44	24	15	15	**Erittäin tietoinen**	152	2,3
	35,53 %	28,95 %	15,79 %	9,87 %	9,87 %			

3.6. Yhteenveto

Kyselytutkimuksen tulokset vahvistivat ja tukivat osittain tutkimukselle asetettuja lähtökohtaolettamia. Kyselytutkimus vahvisti ensimmäisen lähtökohtaolettaman, jonka mukaan kuluttajat kiinnittävät enemmän huomiota tietoturvaan ja tietosuojaan verkkopankkitunnuksia käyttäessään (esim. digitaalisissa maksupalveluissa tai terveydenhoitopalveluissa) kuin sosiaalisessa mediassa. KPMG:n vuonna 2016 laatiman tutkimuksen mukaan vain 14 % suomalaisista tutustuu palvelun tietosuojakäytäntöön perustaessaan uutta sosiaalisen median profiilia (KPMG Global 2016).

Kyselytutkimukseen vastanneet kokivat sertifiointien lisäävän luottamusta, mutta suurin osa vastaajista ei kiinnittänyt tai kiinnitti erittäin vähän huomiota digitaalisten hyödykkeiden tai organisaatioiden sertifiointeihin. Vastaukset eivät tämän havainnon kohdalla riippuneet vastaajien iästä. Näin ollen voidaan todeta, että nuoret kuluttajat eivät ole vanhempia enemmän valveutuneita sertifikaattien suhteen, mikä taas ei vastaa toista lähtökohtaolettamaa.

Kyselytutkimuksen perusteella kuluttajien tietämys sertifiointien taustalla olevasta lainsäädännöstä on erittäin huono. Tulos kumoaa kolmannen lähtökohtaolettaman, jonka mukana kuluttajat ovat tietoisia siitä, että standardit ja sertifikaatit todentavat yhteisesti määriteltyjen tietoturva- ja lakivaatimusten täyttymisen.

Kyselytutkimuksesta voidaan tehdä johtopäätös, että kaikki digitaalisia hyödykkeitä käyttävät osapuolet eivät välttämättä ole tietoisia sertifikaattien arvosta tai niiden sisällöstä. On kuitenkin monia muita tekijöitä, jotka lisäävät merkittävästi digitaalisten hyödykkeiden käyttäjien luottamusta, kuten esimerkiksi yrityksen julkisuuskuva, brändi, sivustojen helppokäyttöisyys ja miellyttävä ulkoasu. Kirjallisuuskatsauksen perusteella voidaan todeta, että laitteiden ja palveluiden toimittajien kannalta sertifiointi sekä standardisointimenetelmien noudattaminen ovat hyödyllisiä, sillä ne osoittavat karkeasti tuotteiden ja palveluiden korkealaatuisuuden ja luotettavuuden.

Tulevaisuudessa kuluttajien sertifiointitietämys ja -tietoisuus saattavat kasvaa tekniikan ja lainsäädännön kehittyessä. Tämän tapahtuessa nähtäväksi jää, riittääkö enää yksi sertifikaatti, vai pitääkö laitteiden ja järjestelmien kehittäjien sekä palveluiden tarjoajien hankkia kaikki mahdolliset tietoturvaa tukevat sertifikaatit laadun osoittamiseksi. Yksi tämän hetken ongelmista yleisellä tasolla on verkkopalveluiden sertifikaattien runsaslukuisuus. Todennäköisesti ”perinteikkäät” luottamuksen lisääjät (yrityksen julkisuuskuva, brändi, sivustojen helppokäyttöisyys ja miellyttävä ulkoasu) ovat tulevaisuudessakin merkittäviä luottamuksen lisääjiä.

Lähteet

Cazier, J. A., Shao, B. B. & St. Louis, R. D. (2006). E-business differentiation through value-based trust. *Information & Management*, 43(6), 718–727.

Demers, J. (2014). *11 Simple Techniques for Gaining Customers' Trust Online*. Haettu 31.10.2016 osoitteesta Inc: http://www.inc.com/jayson-demers/11-simple-tactics-to-increase-trust-online.html

Edelman, B. (2010). Adverse selection in online "trust" certifications and search results. *Electronic Commerce Research and Applications*, 10, 17–18. doi:10.1016/j.elerap.2010.06.001

European Commission. (2016). *2016 Edition Consumer Markets Scoreboard, Making markets work for consumers*. Luxembourg: Publications Office of the European Union. doi:10.2838/32

European Union. (2016). *Consumer Markets Scoreboard*. Luxembourg: Publications Office of the European Union. doi:10.2838/32

Greenhalgh, T., Stramer, K., Bratan, T., Byrne, E., Russell, J. & Potts, H. (2010). Adoption and non-adoption of a shared electronic summary record in England: a mixed-method case study. *BMJ* (Clinical research ed.), 340(7761), c3111. doi:10.1136/bmj.c3111

Hakanen, M. & Häkkinen, M. (2015). Management possibilities for interpersonal trust in a business network. *Nordic Journal of Business*, 64(4), 249–265.

Health On the Net Foundation. (2014). HONcode certification. Haettu 25.8.2016 osoitteesta http://www.hon.ch/HONcode/Patients/

International Organization for Standardization. (5. 2015). ISO 9000:2015 Quality management systems - Fundamentals and vocabulary. Haettu 5.5.2017 osoitteesta https://www.iso.org/standard/45481.html

International Organization for Standardization. (2016, 3.). ISO 13485:2016. Haettu 5.4.2017 osoitteesta https://www.iso.org/standard/59752.html

Kansallinen Terveysarkisto. (2016). *Sertifiointi, olennaiset vaatimukset ja omavalvonta*. Haettu 25.8.2016 osoitteesta http://www.kanta.fi/web/ammattilaisille/sertifiointi

Kaplan, B. & Harris-Salamone, K. D. (2009). Health IT success and failure: recommendations from literature and an AMIA workshop. *Journal of the American Medical Informatics Association*, 16(3), 291–229. doi:10.1197/jamia.M2997

Kappenberger, R. (2012). The True cost of self-signed SSLcertificates. *Computer Fraud & Security*, 2012(9), 14–16. doi:10.1016/S1361-3723(12)70092-1

Kilpailu- ja kuluttajavirasto. (2015). *Kuluttajapoliittinen katsaus 2015*. A. Raijas (toim.). Kilpailu- ja kuluttajaviraston selvityksiä (2), 33. Haettu 5.9.2016 osoitteesta http://www.kkv.fi/globalassets/kkv-suomi/julkaisut/selvitykset/2015/kkv-selvityksia-2-2015-kuluttajapoliittinen-katsaus-2015.pdf

Klein, G. O. (2002). *Standardization of Health Informatics - Results and Challenges*. Methods Archive, 41(4), 261–270. Haettu 5.9 osoitteesta https://methods.schattauer.de/en/contents/archivepremium/issue/special/manuscript/225.html

KPMG Global. (2016). *Companies that fail to see privacy as a business priority risk crossing the 'creepy line*'. Haettu 15.9.2016 osoitteesta KPMG: https://home.kpmg.com/sg/en/home/media/press-releases/2016/11/companies-that-fail-to-see-privacy-as-a-business-priority-risk-crossing-the-creepy-line.html

Lazarte, M. (2015). *Security toolbox protects organizations from cyber-attacks*. (International Organization for Standardization) Haettu 4.9.2016 osoitteesta ISO: http://www.iso.org/iso/home/news_index/news_archive/news.htm?Refid=Ref2032

Liikenne- ja viestintäministeriö. (2016). *Maailman luotetuinta digitaalista liiketoimintaa*. Suomen turvallisuusstrategia. Haettu 22.8.2016 osoitteesta http://www.lvm.fi/documents/20181/877203/Julkaisuja+4-2016/795a8541-7ef5-4690-967d-a1861f1a8a48

Manik Las Das, N. S. (2014). On the Security of SSL/TLS- enabled applications. *Applied computing and informatics*, 10(1-2), 68–72. doi:10.1016/j.aci.2014.02.001

Mauldin, E. G., Nicolaou, A. L. & Kovar, S. E. (2006). The influence of scope and timing of reliability assurance in B2B e-commerce. *International Journal of Accounting Information Systems*, 7(2), 115-129. doi:10.1016/j.accinf.2005.09.002

McKnight, D. H., Choudhury, V. & Kacmar, C. (2002).). Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research*, 13(3), 334–359.

McKnight, D. H., Larry, L. C. & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management review*, 23(3), 473–490. doi: 10.5465/AMR.1998.926622

Pennanen, K., Tiainen, T. & Luomala, H. T. (2007). A qualitative exploration of a consumer's value-based e-trust building process: A framework development. *Qualitative Market Research: An International Journal*, 10(1), 28–47. doi: 10.1108/13522750710720387

Runyan, B.;Smith, K. & Smith, L. M. (2008). Implications of Web assurance *Services on e-commerce. Accounting Forum*, 32(1), 46–61. doi:10.1016/j.accfor.2007.10.002

Shapiro, C. & Varian, H. R. (1999). The Art of Standards Wars. *California Management Review*, 41(2), 8–32. doi:10.2307/41165984

Sosiaali- ja terveysministeriö. (2012). KanTa-palveluihin liittyvän auditoinnin menettelyt. Haettu 30.8.2016 osoitteesta http://www.kanta.fi/documents/12105/3983179/Auditointiohje_kanta-palveluihin+liittyv%C3%A4n+auditoinnin+menettelyt+v1.1.pdf/01eca7d9-e057-4745-9128-36910de27a83

Stakes. (2008). *Menetelmä sosiaali- ja terveydenhuollon tietojärjestelmien sertifiointivaatimusten tuottamiselle*. M. J. Ruotsalainen P. (toim.) Haettu 25.8.2016 osoitteesta Stakesin raportteja 41/2008: https://julkari.fi/bitstream/handle/10024/75431/R41-2008-VERKKO.pdf?sequence=1

Suomen Standardisoimisliitto SFS ry. (2016a). Usein kysyttyä. Haettu 26.8.2016 osoitteesta http://www.sfs.fi/usein_kysyttya

Suomen Standardisoimisliitto SFS ry. (2016c). Terveydenhuollon tietotekniikka. Haettu 26.8.2016 osoitteesta https://www.sfs.fi/it/sr301

Suomen Standardoimisliitto SFS ry. (2016b). Terveydenhuolto. Haettu 26.8.2016 osoitteesta https://www.sfs.fi/aihealueet/terveydenhuolto

Terveyden ja hyvinvoinnin laitos. (2016a). Sosiaali- ja terveydenhuollon digitalisaatio. Haettu 30.8.2016 osoitteesta Seurantamittarit ja tuloksia Sote-tieto hyötykäyttöön - strategian näkökulmasta: https://www.julkari.fi/bitstream/handle/10024/130610/URN_ISBN_978-952-302-667-4.pdf?sequence=1

Terveyden ja hyvinvoinnin laitos. (2016b). Mitä väestö ajattelee sosiaali- ja terveyspalveluiden uudistamisesta? Haettu 24.8.2016 osoitteesta Tutkimuksesta tiiviisti 4: http://www.julkari.fi/bitstream/handle/10024/130233/TUTI2016_4_Mit%C3%A4%20v%C3%A4est%C3%B6%20ajattelee_WEB.pdf?sequence=1

Tilastokeskus. (2016). Käsitteet ja määritelmät - Hyödyke. Haettu 30.8.2016 osoitteesta http://www.stat.fi/meta/kas/hyodyke.html

Wang, L., Law, R., Guillet, B., Hung, K. & Fong, D. (2015). Impact of hotel website quality on online booking intentions: eTrust as a mediator. *International Journal of Hospitality Management*, 47, 108–115. doi:10.1016/j.ijhm.2015.03.012

Vanhala, M. & Ahteela, R. (2011). The effect of HRM practices on impersonal organizational trust. *Management Research Review*, 34(8), 869–888. doi:10.1108/01409171111152493

Viestintävirasto. (2003). *Haavoittuvuuksia TLS ja SSL protokollatestauksissa*. Haettu 5.9.2016 osoitteesta Viestintäviraston virallinen verkkosivu: https://www.viestintavirasto.fi/kyberturvallisuus/haavoittuvuudet/2003/varoitus-2003-63.html

LUKU 4.

Nykyaikaisten viestintäsovellusten ja pilvipalveluiden parhaat tietosuojakäytännöt – käyttäjien mahdollisuudet hallita tietojaan ja vaihtaa palveluntarjoajaa

Hartikainen Pauliina

Verkottuneiden järjestelmien ja Internetin laajan käytön myötä yksityisyyden ymmärtäminen ja sen suojaaminen on yhä merkittävämpää tietojärjestelmiä suunniteltaessa, rakennettaessa ja tarjottaessa. Nykyaikaisten, alati kehittyvien teknologioiden avulla eri sovellusten ja palveluiden käyttäjistä on mahdollista kerätä suuria määriä henkilötietoja, joita voidaan käyttää niitä eri tarkoituksiin. Henkilötietojen kerääminen, käsittely tai käyttö saattaa johtaa henkilöiden yksityisyyden loukkaamiseen, mikäli tietosuojaa ei huomioida koko henkilötietojen elinkaaren ajan (Kirmani & Rao 2000, 66–79.).

Viimeaikaisten tutkimusten mukaan kuluttajien tietoisuus digitaalisten palveluiden tietosuojariskeistä on kasvamaan päin. Näin ollen he ovat alkaneet suojata yksityisyyttään verkossa ja etsiä osoituksia digitaalisten palveluntarjoajien luotettavuudesta. KPMG:n (2016, 29) tekemän maailmanlaajuisen kyselytutkimuksen mukaan 56 % kuluttajista on joko huolissaan tai erittäin huolissaan siitä, miten yritykset käsittelevät ja käyttävät heidän tietojaan. Lisäksi 84 % vastaajista koki, että heillä ei ole riittäviä mahdollisuuksia hallita tietojaan digitaalisissa palveluissa (KPMG International 2016, 13.). Mikäli yritykset ja organisaatiot eivät käsittele asiakkaidensa tietoja asianmukaisesti, yksityisyydestään huolestuneet käyttäjät saattavat pidättäytyä käyttämästä yrityksen tarjoamia tuotteita tai palveluita. Tietosuojaa eli ”yksilön kykyä kontrolloida henkilökohtaisesti tietoja itsestään” onkin pidetty yhtenä tärkeimmistä informaatioaikakauden eettisistä kysymyksistä (Smith, Milberg & Burke 1996, 167.).

Digitalisaatio nähdään IT-kehityksen kolmantena aikakautena, jota edelsivät IT-käsityöläisyyden ja IT-teollisuuden aikakaudet (Tuominen 2014). ETLA:n (2015, 18) mukaan digitalisaatio tarkoittaa ”digitaaliteknologian integrointia jokapäiväiseen elämään digitoimalla kuvaa, ääntä, dokumenttia tai signaalia biteiksi ja tavuiksi kuvaamaan asioita ja tietosisältöä”. Digitaalitalouden (engl. *digital economy*) tehokkaan toimimisen yhtenä edellytyksenä on toimiva ja luotettava IT-infrastruktuuri. Liiketoiminnan digitalisoitumisen nähdään mahdollistavan uudenlaisten toimintatapojen ja liiketoimintamallien kasvun. Samalla se kuitenkin asettaa valtavia haasteita kansalaisten yksityisyydensuojan turvaamiselle. Uudenlaisten teknologioiden ja palvelumallien tietosuojariskit on huomioitava sekä tietojärjestelmiä suunniteltaessa että tietojenkäsittelyä koskevan sääntelyn kehitystyössä. Yhtäältä se laittaa tietojen käsittelijät huomioimaan tietosuoja-asiat entistä tarkemmin ja toisaalta se koettelee tietosuojalainsäädännön rajoja ja luo uudenlaisia paineita kehittää sitä (liikenne- ja viestintäministeriö 2016, 7.). Euroopan unioni on vastannut tarpeeseen tietosuojauudistuksella, jonka tavoitteena on päivittää tietosuojasääntely digiaikakaudelle. Uusia sääntelyinstrumentteja ovat yleinen tietosuoja-asetus ((EU) 2016/679) ja direktiivi lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta ((EU) 2016/680) (Euroopan unionin neuvosto 2016). Lisäksi keskeinen valmisteilla oleva sääntelyinstrumentti on sähköisen viestinnän tietosuoja-asetus (COM/2017/010 final). Tietosuoja-asetuksen tavoitteena on huomioida uusien teknologioiden ja tiedonkeruumenetelmien riskit sekä velvoittaa

organisaatiot suhteuttamaan suojausmekanismit tietojenkäsittelyyn liittyvään riskiin (valtiovarainministeriö 2016, 6). Asetus on jäsenmaita suoraan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa 25. toukokuuta 2018 alkaen ((EU) 2016/679, 99 artikla).

Tässä raportissa tarkastellaan digitaalisten hyödykkeiden, nykyaikaisten viestintäsovellusten ja pilvipalveluiden parhaita tietosuojakäytäntöjä sekä käyttäjien mahdollisuuksia hallita tietojaan ja vaihtaa palveluntarjoajaa. Digitaalinen hyödyke on tuote tai palvelu, joka toimitetaan sähköisessä muodossa tietoliikenneverkon välityksellä myyjältä asiakkaalle (Salste 2000, 9–11; (EU) 2015/1535, 1 artikla 1 kohta b alakohta). Digitaalisia palveluita ovat esimerkiksi verkossa toimiva markkinapaikka, verkossa toimiva hakukone ja pilvipalvelu ((EU) 2016/1148, liite III). Yksi digitaalisen aikakauden mielenkiintoisista teknologioista onkin ”pilvilaskenta”, joka perustuu moniin eri konsepteihin, kuten palvelukeskeiseen arkkitehtuuriin, hajautettuun tietojenkäsittelyyn ja virtualisointiin. Pilvipalvelut ovat herättäneet mielenkiintoa viime vuosien aikana niiden valtavan potentiaalin myötä: teknologia mahdollistaa tietojenkäsittelyresurssien kustannustehokkaan hyödyntämisen ja asiakaslähtöisten palvelujen tarjoamisen. Pilvipalvelu on tietojenkäsittelymalli, jossa palveluntarjoaja toimittaa palvelun asiakkaalle tietoliikenneverkkojen välityksellä. Perinteisiin tietojenkäsittelymalleihin verrattuna pilvipalveluiden etuja ovat esimerkiksi niiden laajennettavuus, joustavuus, saatavuus ja kustannustehokkuus (Youseff, Butrico & Da Silva 2008, 1.). Digitaalisiin hyödykkeisiin lukeutuvat myös viestintäsovellukset, jotka voidaan toimittaa pilvipalveluna. Suomen virallisen tilaston (2015) mukaan suurin osa suomalaisista (69 %) käyttää mobiililaitteita, joita hyödynnetään eniten viestintään ja asioiden hoitoon. Nykyaikaiset viestintäsovellukset ovatkin usein mobiilisovelluksia, joita käytetään älypuhelimilla tai tableteilla. Viestintäsovellukset eivät kuitenkaan rajoitu pelkästään älypuhelinsovelluksiin; laajemmin määriteltynä viestintäsovellus on ohjelmisto, jonka toiminnot mahdollistavat viestien lähettämisen ja vastaanottamisen kahden tai useamman osapuolen välillä (ITIL 2001, 5; Duncan 2014.).

Nykyaikaisiin viestintäsovelluksiin ja pilvipalveluihin liittyy merkittäviä haasteita yksityisyydensuojan kannalta. Kuluttajien tullessa yhä tietoisemmiksi yksityisyyteensä liittyvistä asioista yritykset kohtaavat jatkuvasti uudenlaisia haasteita, kun kuluttajille valkenee, missä laajuudessa heidän tietojaan käytetään liiketoiminnallisiin tarkoituksiin ja minkä verran yritykset tekevät rahaa heidän tiedoillaan. (KPMG International 2016, 16.) OECD (2013, 5) on esimerkiksi arvioinut, että Facebookille yksittäiseen eurooppalaiseen kuluttajaan liittyvien tietojen arvo on alle 5 dollaria vuodessa, ja yhdysvaltalaisen tietojen arvo on lähempänä 10 dollaria. Näin ollen on tärkeää, että palveluntarjoajien tietojenkäsittely- ja suojaustoimet ovat läpinäkyviä (Aïmeur, Lawani & Dalkir 2016, 368). Avoimuuden ja läpinäkyvyyden takaamiseksi lainsäädäntö velvoittaa yrityksiä kertomaan tietojenkäsittelytoimistaan. Tietosuoja-asetuksen ((EU) 2016/679, 30 artikla) nojalla henkilötietoja käsittelevien tahojen tulisi laatia seloste käsittelytoimista. Tämä voi esimerkiksi olla sähköisesti saatavilla oleva tietosuojakäytäntö. Tietosuojakäytäntö kertoo käyttäjälle, miten tietty teknologia, tuote tai palvelu käsittelee hänen henkilötietojaan (Aïmeur ym. 2016, 368.). Mikäli palveluntarjoaja ilmoittaa tietojenkeräys- ja käsittelytoimistaan läpinäkyvästi ja avoimesti, se tutkitusti parantaa palvelun luotettavuutta (Earp, Antón, Aiman-Smith & Stufflebeam 2005, 235). Tavoitteiden toteutumisen kannalta on kuitenkin haastavaa, etteivät käyttäjät usein lue tietosuojakäytäntöä ja käyttöehtoja ennen palvelun käyttöönottoa. Näin ollen he saattavat hyväksyä sellaisia ehtoja tai menettelytapoja, jotka ovat ristiriidassa heidän yksityisyyteen liittyvän tahtotilansa kanssa. Lisäksi palveluiden käyttöehtojen ja henkilötietojen käsittelystä kertovien selosteiden pituus ja monimutkaisuus heikentävät tietojenkäsittelytoimien läpinäkyvyyttä. (Aïmeur ym. 2016, 368; KPMG International 2016; Capistrano & Chen 2015, 24; Michota & Katsikas 2015, 139; Geng, Liu & Bryant. 2010, 58, 26.)

4.1. Tutkimuskysymykset ja -menetelmät

Raportti on tiivistelmä Turun yliopiston tietojärjestelmätieteen pro gradu -tutkielmasta, joka tehtiin toimeksiantona KPMG Oy:lle 2016–2017. Työn tavoitteena oli tutkia nykyaikaisten viestintäsovellusten ja pilvipalveluiden parhaita tietosuojakäytäntöjä sekä käyttäjien mahdollisuuksia hallita tietojaan ja vaihtaa palveluntarjoajaa. Ensimmäinen tutkimuskysymys rakennettiin työn tavoitteiden mukaisesti:

- Mitkä ovat nykyaikaisten viestintäsovellusten ja pilvipalveluiden parhaita tietosuojakäytäntöjä?

Tutkimuskysymystä lähestytään luotettavuuden näkökulmasta, jonka osateemoiksi määriteltiin ”kansalaisten hyväksymä ja luottama” ja ”lain velvoitteet täyttävä”. Näin ollen tarkastelutapa on kuluttajalähtöinen; minkälaiset tietosuojakäytännöt lisäävät kuluttajien luottamusta digitaalisiin hyödykkeisiin. Kuluttajat arvioivat hyödykkeen luotettavuutta osana liiketoimipäätöksiään usein siihen kohdistuvien riskien, kustannusten ja hyötyjen perusteella (Aljukhadar, Senecal &Ouellette 2010, 103–126). He muodostavat käsityksensä näistä organisaation antamien ”signaalien” pohjalta. Tällaisena signaalina toimii esimerkiksi tietosuojakäytäntö (Kirmani & Rao 2000, 66–79.). Näin ollen tutkimuksessa on tarkoituksena selvittää viestintäsovelluksiin ja pilvipalveluihin kohdistuvia tietosuojariskejä ja muodostaa niiden pohjalta kokonaiskuva parhaista tietosuojakäytännöistä, jotka auttavat organisaatiota täyttämään lainsäädännölliset velvoitteensa kansalaisten luottamusta lisäävällä tavalla. Päätutkimuskysymyksen tueksi laadittiin kaksi alatutkimuskysymystä:

- Mitkä ovat nykyaikaisten viestintäsovellusten ja pilvipalveluiden merkittävimmät tietosuojariskit?
- Minkälainen on tehokas tietosuojakäytäntö?

Tutkimuksen toisena päätavoitteena oli tutkia käyttäjien mahdollisuuksia hallita tietojensa käyttöä tai vaihtaa palveluntarjoajaa. Työssä tarkastellaan tutkimusongelmaa kahdesta näkökulmasta: minkälaisia lainsäädännöllisiä oikeuksia käyttäjillä on ja miten viestintäsovelluksia tai pilvipalveluita tarjoavien organisaatioiden tulisi toteuttaa näitä. Tutkielman toinen päätutkimuskysymys on:

- Mitä mahdollisuuksia käyttäjillä on hallita tietojaan tai vaihtaa palveluntarjoajaa?

Tutkimusongelmaa lähestytään seuraavien alatutkimuskysymysten avulla:

- Minkälaisia lainsäädännöllisiä oikeuksia rekisteröidyllä on?
- Miten kaupallisten viestintäsovellusten ja pilvipalveluiden tietosuojakäytännöt vastaavat niille asetettuja vaatimuksia?

Tutkimusote on toiminta-analyyttinen, jonka tausta on anti-positivistinen eli subjektiivinen. Tutkimus koostuu teoreettisesta ja empiirisestä osiosta, jotka keskustelevat keskenään ja muodostavat yhdessä yhtenäisen ja johdonmukaisen kokonaisuuden. Aiheen tuoreuden, monimuotoisuuden ja jatkuvan muutoksen vuoksi tutkimusmetodologiaksi valittiin laadullinen tutkimus. Toiminta-analyyttisen tutkimusotteen mukaiset laadulliset menetelmät sopivat tähän tilanteeseen, sillä sen avulla pyritään kuvaamaan ilmiöitä ja ymmärtämään tiettyä toimintaa. (Hirsjärvi, Remes & Sajavaara 2004, 212.) Lähestymistavan luonteeseen kuuluu empiirinen aineisto, joka kerätään harvoilta kohdeyksilöiltä. Toiminta-analyyttisessä tutkimuksessa empiria ja teoria kulkevat rinnakkain, eikä tutkimusvaiheiden välillä ole selkeää eroa (Neilimo & Näsi

1980, 35). Laadullisessa lähestymistavassa tutkittavien näkökulma on keskeinen. Kvalitatiiviset tutkimusmenetelmät sopivat tähän tutkimukseen parhaiten, sillä aiheen kannalta on tärkeää muodostaa kokonaisnäkemys, joka perustuu tutkimuksessa haastateltujen henkilöiden henkilökohtaisten kokemusten ja ajatusten ymmärtämiseen ja tulkitsemiseen (Eskola & Suoranta 1998).

Laadullisina tutkimusmetodeina olivat haastattelut ja dokumentaation läpikäynti. Haastatteluiden lähestymistapa oli puolistrukturoitu eli teemahaastattelu. Teemahaastattelut sisältävät käytännössä katsoen useita tarinoita, ja näin ollen narratiivinen analyysi mahdollistaa aineiston tutkimisen. Puolistrukturoidun haastattelun avoimuutta hyödynnettiin tässä tutkimuksessa kahdella tapaa: testattavia hypoteeseja ei laadittu etukäteen, ja haastateltavia kannustettiin puhumaan avoimesti. Haastateltaville ei annettu ennalta määritettyjä tarkkoja kysymyksiä vastattavaksi, vaan heidän annettiin puhua tutkimuksen teemoista omin sanoin ja omasta näkökulmastaan (Eriksson & Kovalainen 2008).

Tutkimukseen haastateltiin kuutta asiantuntijaa. Teemahaastattelu sallii haastateltavalle vapauksia; haastateltava voi vastata tutkijan määräämiin kysymyksiin omin sanoin, poiketa kysymysten järjestyksestä ja joskus jopa ehdottaa uusia kysymyksiä (Koskinen, Alasuutari & Peltonen 2005, 105). Tätä mukaillen haastattelut etenivät tutkijan laatiman haastattelurungon mukaisesti, kuitenkin ilman tiukkaa kontrollia tai järjestyksenmukaisuutta. Haastattelujen toteuttamiseen käytettiin kahta vaihtoehtoista tapaa, osa pidettiin kasvotusten ja osa tehtiin puhelimitse. Kaikki keskustelut äänitettiin. Analyysivaiheessa äänitteet litteroitiin auki, mikä helpotti haastatteluaineiston käsittelyä ja analysointia. Taulukko 2 havainnollistaa tutkimuksen teema-alueita, jotka muodostettiin tutkimusongelmien ja osaongelmien mukaan.

Taulukko 2: Tutkimuksen teema-alueet.

Tutkimusongelma	Osaongelma	Teoriatausta	Teema-alue
Mitkä ovat nykyaikaisten viestintäsovellusten sekä pilvipalveluiden parhaita tietosuojakäytäntöjä?	Mitkä ovat nykyaikaisten viestintäsovellusten ja pilvipalveluiden merkittävimmät tietosuojariskit?	Esim. Svantesson ym. (2008); Bashir ym. (2011); Duncan (2014); Ricker ym. (2015); Rizvi ym. (2016); Chandramohan ym. (2016)	Pilvipalveluiden ja viestintäsovellusten tietosuojariskit
	Minkälainen on tehokas tietosuojakäytäntö?	Esim. Kirmani ym. (2000); Earp ym. (2005); Capistrano ym. (2015); Aïmeur ym. (2016)	Hyvä tietosuojakäytäntö
Mitä mahdollisuuksia käyttäjillä on hallita tietojensa käyttöä tai vaihtaa palveluntarjoajaa?	Minkälaisia lainsäädännöllisiä oikeuksia rekisteröidyllä on?	Henkilötietolaki (1999/523, 6 luku); yleinen tietosuoja-asetus ((EU) 2016/679)	Käyttäjien oikeudet hallita tietojaan
	Miten kaupallisten viestintäsovellusten ja pilvipalveluiden tietosuojakäytännöt vastaavat niille asetettuja vaatimuksia?	Kaupalliset palveluntarjoajat: Google, WhatsApp, Dropbox	Tietosuojalainsäädäntö

4.2. Yksityisyydensuoja verkossa

Yksityisyydensuoja verkossa (engl. *Internet privacy*) on konsepti, jolle ei ole olemassa yksiselitteistä määritelmää, mutta siitä on useita tulkintoja kirjallisuudessa. Yksityisyydensuoja eli tietosuoja (engl. *privacy*) tarkoittaa henkilöstä itsestään ja hänen toiminnastaan kerättävien tietojen suojaamista siten, ettei niitä käytetä luvattomasti tai henkilön omaa etua vaarantaen (Paananen 2005, 415.). Toisin sanoen tietosuoja tarkoittaa yksityisyyden suojaamista henkilötietoja käsiteltäessä (valtiovarainministeriö 2016, 12). Tietosuoja voidaan nähdä myös yksilön mahdollisuutena hallita henkilötietojensa käyttöä (Smith ym. 1996, 167; Wolf 2012; Pentina, Zhang, Bata & Chen 2016, 410).

Yksityisyys rinnastetaan usein anonyymiyteen, salassapitoon tai läheisyyteen, jotka ovat vastaavanlaisia konsepteja. Nämä on kuitenkin syytä erottaa yksityisyyden määritelmästä: yksityisyys tarkoittaa sitä, että yksilöllä on oikeus päättää itseensä liittyvistä asioista, omista teoistaan ja tiedoistaan. Kansalaisen yksityisyyden ei esimerkiksi katsota tulleen loukatuksi, mikäli valtio pääsee selville hänen tekemisistään tai liikkeistään. Kyseessä on enemmänkin ajatus siitä, että yksilö saa tehdä mitä haluaa omalla ajallaan (De George 2003, 43). Yksityisyydensuoja verkossa -konsepti voidaan jakaa kolmeen rinnakkaiseen lähestymistapaan: yksityisyydensuoja oikeutena tietoihin pääsyä rajoittamiseen, yksityisyydensuoja oikeutena tietojen hallintaan ja yksityisyydensuoja yhteiskuntasopimuksena (Martin 2016, 552).

Martinin (2016, 552) esittämää jaottelua mukaillen taulukossa 3 havainnollistetaan yksityisyydensuojan eri lähestymistapoja ja niiden eettisiä näkökulmia. Ensimmäisen lähestymistavan mukaan yksityisyys merkitsee yksilön oikeutta olla rauhassa. Määritelmä on kehittynyt ajasta, jolloin oikeudellista suojaa annettiin pelkästään yksilön elämälle ja fyysiselle omaisuudelle. Sittemmin käsitteen ”omaisuus” on nähty käsittävän kaikenlainen omistus: niin aineeton kuin aineellinen omaisuus. (Warren & Brandeis 1890; Martin 2016, 552.) Toinen lähestymistapa keskittyy kontrolliin, jonka mukaan yksityisyys tarkoittaa sitä, että yksilöllä on mahdollisuus hallita tietoja itsestään. Peruselementtinä on nimenomaan tietojen hallinta; kyse ei ole tietojen salaamisesta muilta vaan siitä, että yksilö saa itse päättää, mitä tietoja luovuttaa ulkopuolisille. Yksilön mahdollisuudet hallita henkilötietojaan on nähty keskeisenä tekijänä myös luottamussuhteen rakentamisessa. Palveluntarjoajan ja käyttäjän välisen luottamuksen kannalta on keskeistä, että käyttäjä voi itse valita, kuka hänen tietojaan näkee ja mitä hänestä tiedetään. (Schoeman 1984, 213; Pollach 2005, 222.) Viimeisimmän tarkastelutavan mukaan yksityisyydensuojanormit voidaan nähdä molempia osapuolia hyödyttävänä ja kestävänä yhteisön sisällä tehtävänä sopimuksena (Martin 2012) tai kontekstista riippuvaisina sääntöinä (Nissenbaum 2011).

Taulukko 3: Yksityisyydensuoja eettisistä näkökulmista (mukaillen Martin 2016, 552).

Lähestymistapa	Aiempi tutkimus	Yksityisyydensuojan määritelmä	Eettinen näkökulma
Pääsy tietoihin (engl. *access view*)	Bonner (2007), Manning (1997), Miller & Weckert (2000), Persson & Hansson (2003)	”oikeus olla rauhassa” Warren & Brandeis (1890); Prosser (1960, 389); Peslak (2005, 329)	Henkilön yksityisyyteen puuttuminen on oikeutettua, jos yksilölle annetaan riittävät perustelut puuttumisen syistä ja nämä syyt ylittävät yksilön vaatimukset yksityisyydensuojalle (Persson & Hansson 2003, 65).
Tietojen hallinta (engl. *control*)	Hsu & Kuo (2003), Angst (2009), Alder ym. (2007)	”vaatimus siitä, että yksilöt, ryhmät tai instituutiot saavat päättää itse milloin, miten ja missä määrin heihin liittyvää tietoa jaetaan muille” Westin (1969); Pollach (2005, 222)	Yksilöiden katsotaan voivan hallita tietojaan antamalla tietoisen suostumuksen tietojen keräämiselle (Martin 2016, 552). Suostumuksen edellytyksistä säädetään esimerkiksi EU:n tietosuoja-asetuksessa ((EU) 2916/679, 7 artikla).
Kontekstiriippuvaiset normit (engl. *context-dependent norms*)	Brown (1996), Martin (2012), Cranford (1998)	“tietyssä yhteisössä tai tilanteessa [kontekstissa] sovitut menettelytavat” Nissenbaum (2011); Martin (2012, 520)	Lähestymistavan eettisiin kysymyksiin kuulu esim. se, miten yksilöt kokevat yksityisyyden. (Kuo ym. 2007; Martin 2016, 552).

Haastattelututkimuksen tulokset vahvistavat taulukossa 3 esitettyä näkemystä kyberyksityisyydensuojan keskeisimmistä ulottuvuuksista; yksilön on saatava pääsy häneen liittyviin tietoihin ja pystyttävä hallitsemaan niitä. Yksilölle on annettava riittävät perustelut yksityisyyteen puuttumiselle. Tämä tarkoittaa käytännössä sitä, että tietojen käsittelijöiden on informoitava käyttäjiä heistä kerättävien tietojen keräys- ja käsittelyperusteista. Haastatteluissa korostui tarve antaa yksilöille mahdollisuuksia hallita tietojaan. Käyttäjän antama suostumus nähdään keskeisenä keinona hallita, mitä tietoa hänestä voidaan kerätä. Suostumukseen liittyy kuitenkin tulkintahaasteita; esimerkiksi sen vapaaehtoisuus ja peruutettavuus eivät aina ole yksiselitteisiä. Käyttäjien mahdollisuuksia hallita tietoja ja vaihtaa palveluntarjoajaa käsitellään jäljempänä tässä luvussa.

Yksityisyydensuoja perusoikeutena

Tietosuoja on teemana hyvin moniulotteinen, ja sen tarkasteluun on kehittynyt viime vuosikymmenten aikana eri lähestymistapoja. Suomessa yksityisyydensuojalla on perustuslaillinen lähtökohta: perustuslain 10 §:n mukaan jokaisen henkilön yksityiselämä, kunnia ja kotirauha on turvattu. Pykälän mukaan myös ”kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton”. Pykälän toisen momentin sisältö on kuitenkin lähtökohta, johon voidaan säätää rajoituksia lailla. Näin ollen viestin salaisuuden loukkaamattomuus ei merkitse ehdotonta suojaa viestinnälle (Laaksonen ym. 2006, 28–29).

Euroopan unionissa uskotaan vakaasti sääntelyn voimaan, jolla pyritään turvaamaan yksilöiden perustuslailliset oikeudet. Yhdysvallat on pyrkinyt liberaalimpaan lähestymistapaan it-

sesääntelyllä, jonka taustalla vallitsee ajatus yksilön vapaudesta. Euroopan unionin perustuslaillinen lähestymistapa painottaa tehokkaan suojauksen tärkeyttä ja tarvetta ennaltaehkäistä oikeudenloukkauksia (Simitis 2010, 1993). Euroopassa tietosuojalainsäädännöllä on näin ollen merkittävä rooli, ja sitä pyritään kehittämään kansalaisten perusoikeuksien turvaamiseksi entistä tehokkaammin. Sääntelyn haasteena on kuitenkin se, että sen voimaansaattamisessa menee keskimäärin 10 vuotta, kun taas informaatio- ja viestintähyödykkeiden elinkaari on keskimäärin alle vuoden (3–7 kuukautta). Sääntelyriskit ovat näin ollen lähes poikkeuksetta käyttöönotettua teknologiaa jäljessä. Euroopan unionin lähestymistavan suurena haasteena onkin ollut kautta linjan se, miten lainsäädäntö saadaan sopimaan nykyaikaisiin liiketoimintamalleihin ja niiden tarpeisiin sekä miten sen toteutumista pystytään valvomaan tehokkaasti (Spiekermann ym. 2001, 38).

Teknologian kehittymisen ja uudenlaisen, digitaalisen, toimintaympäristön myötä Euroopan unioni on tunnistanut tarpeen uudistaa tietosuojasääntelyä entistä riskilähtöisemmäksi ja teknologiariippumattomammaksi. Tietosuojauudistuksen on tarkoitus vastata edellä mainittuun sääntelyhaasteeseen: se pyrkii huomioimaan uusien teknologioiden ja tiedonkeruumenetelmien riskit sekä velvoittaa suhteuttamaan suojausmekanismit tietojenkäsittelyyn liittyvään riskiin (valtiovarainministeriö 2016, 6). EU:n yleisen tietosuoja-asetuksen tavoitteena on vahvistaa yksilön oikeuksia ja vapauksia sekä parantaa luottamusta Internet-palveluihin (Euroopan unionin neuvosto 2016). Haastattelujen perusteella voidaan todeta, että asetus on tietosuojalainsäädännön merkittävä kehitysaskel.

Yksityisyydensuojaparadoksi

Kuluttajat ovat huolissaan yksityisyydestään käyttäessään digitaalisia palveluita, mutta jakavat siitä huolimatta vapaaehtoisesti tietoja itsestään esimerkiksi sosiaalisen median sivustoilla. Tätä epäjohdonmukaisuutta yksilön suhtautumisen ja tosiasiallisen käyttäytymisen välillä kutsutaan yksityisyydensuojaparadoksiksi (engl. *privacy paradox*) (Kokolakis 2017, 122). Ilmiö kuvastaa ihmisten epäloogista käyttäytymistä; yhtäältä he ovat valmiita paljastamaan tietoja itsestään ja toisaalta he ovat huolissaan siitä, että yritykset käyttävät näitä tietoja vastoin heidän suostumustaan. Toisin sanoen, yksilöiden halu suojata yksityisyyttään on paradoksaalisessa suhteessa sen kanssa, että he ovat valmiita luovuttamaan tietoja itsestään saadakseen esimerkiksi taloudellisia etuja tai parempia palveluita (Nissenbaum 2011; Kuo, Lin & Hsu, 2007, 148).

Yksityisyydensuojaparadoksin kaksi päätekijää ovat käyttäjän tosiasiallinen käyttäytyminen ja aikomukset. Tutkimuksissa on usein keskitytty jälkimmäisen tutkimiseen, kun on pyritty selvittämään yksilöiden suhdetta yksityisyyteen. Tällöin on usein jäänyt huomioimatta se tosiasia, että yksilön aikomukset eivät aina johda yksityisyyttä suojaavaan käyttäytymiseen. On osoitettu, että ihmiset ovat valmiita vastaanottamaan taloudellisia hyötyjä yksityisyytensä kustannuksella (Kokolakis 2017, 123). Brown (2001) tutki verkko-ostosten suosiota ja asiakkaiden verkkokauppojen tietosuojaan ja tietoturvaan liittyviä huolenaiheita. Tutkimukseen haastatellut verkkokaupan asiakkaat olivat valmiita luovuttamaan itsestään enemmän tietoja, mikäli he saivat sen myötä esimerkiksi hinta-alennuksia. Haastatellut henkilöt olivat huolissaan yksityisyytensä loukkaamisesta, eivätkä näin ollen tunteneet oloaan mukavaksi luovuttaessaan tietojaan verkkokaupalle. Tietojen antamisen myötä saadut taloudelliset edut koettiin kuitenkin merkittävämmiksi kuin yksityisyyden suojaaminen (Brown 2001, 17–18).

KPMG:n tekemän kansainvälisen kyselytutkimuksen tulokset osoittavat, että ihmiset suhtautuvat yksityisyyteensä eri tavoin. Nykyisin henkilökohtaisten tietojen luovuttaminen on usein välttämätöntä digitaalisten hyödykkeiden, kuten viestintäsovellusten tai pilviteknologiaan perustu-

vien palveluiden käyttämiseksi. Käyttäjät ovatkin usein valmiita antamaan tietoja itsestään saadakseen sellaisia tuotteita tai palveluita, jotka tekevät elämästä helpompaa, parempaa tai toisinaan edullisempaa. Kuluttajat ovat yhä enenevässä määrin tietoisia siitä, että heistä kerättyjä tietoja saatetaan käyttää ja myydä eteenpäin esimerkiksi markkinointitarkoituksiin. Yritysten on kuitenkin tunnistettava raja, joka menee tietojenkeruun hyödyllisyyden ja tunkeilevuuden välillä. Se, mikä on yhden mielestä vastenmielistä ja tunkeilevaa (”creepy”) on jonkin toisen mielestä harmitonta ja hyödyllistä (”cool”). (KPMG International 2016, 4.) Kuluttajien epäjohdonmukaista käyttäytymistä voidaan perustella käyttäytymistieteiden avulla. Lyons (2016) jakaa syyt neljään ryhmään (KPMG International 2016, 20):

1. nykytilaharha (engl. *status quo bias*)
2. asetteluharha (engl. *framing bias*)
3. yli-itsevarmuus (engl. *overconfidence*)
4. nykyhetkiharha (engl. *present bias*).

Harha nykytilasta tarkoittaa sitä, että ihmisillä on tapana pitää kiinni siitä mitä heillä on, eivätkä he kyseenalaista asioiden nykytilaa. Yritykset käyttävät tätä hyväkseen asettamalla verkkopalvelun oletusasetukset tyypillisesti sellaisiksi, että käyttäjä jakaa tietoja itsestään mahdollisimman paljon. Asetteluharha viittaa yritysten tapaan esitellä ja viestiä asioista: he korostavat tietojen jakamisesta saatavia hyötyjä, kun taas siitä koituvat haittapuolet (kuten yksityisyyden menettäminen) piilotetaan. Näin ollen kuluttajat yleensä hyväksyvät ehdot, vaikka eivät tuntisi oloaan mukavaksi. Ihmisten on lisäksi todettu olevan yli-itsevarmoja toimiessaan verkossa. Usein luotetaan siihen, että itse ei jakaisi sellaista tietoa, jonka julkaisemista katuisi myöhemmin (KPMG International 2016, 20). Käytäntö kuitenkin kertoo toista: Suomestakin löytyy tapauksia, joissa yksityishenkilöiden Twitter-julkaisut ovat johtaneet työsuhteen irtisanomiseen (ks. esim. Helsingin Sanomat 2016). Neljäs syy eli nykyhetkiharha tarkoittaa sitä, että ihmisillä on tapana saada välitöntä mielihyvää ”tykkäyksistä” ja tietojen jakamisesta sosiaalisessa mediassa, mutta he eivät usein osaa arvioida tietojen jakamisen kauaskantoisia seurauksia (KPMG International 2016, 20).

Yksityisyydensuoja nähdään usein kontekstisidonnaisena, jonka mukaan yksilön halu paljastaa itsestään tietoja riippuu kontekstista (Hirschprung ym. 2016, 443). Nissenbaumin teorian (engl. *theory of contextual integrity*) mukaan ei ole olemassa universaaleja tietosuojanormeja, vaan ne ovat kussakin tilanteessa erillisiä. Teorian mukaan yksityisyydensuoja ei ole staattinen vaan dynaaminen käsite, joka määrittyy asiayhteyden ja siten myös kulttuurin mukaan. Joissain kulttuureissa esimerkiksi vuosipalkka koetaan yksityiseksi asiaksi, kun taas toisissa kulttuureissa on normaalia jakaa tämä tieto muiden kanssa. (Nissenbaum 2011; Kowalewski, Ziefle, Ziegeldorf & Wehrle 2015, 816.) Yksityisyydensuoja ei näin ollen tarkoita anonyymiyttä tai salassapitoa, kun puhutaan yksityisten viestinnällisten ja taloudellisten tietojen suojaamisesta (Chandramohan, Vengattaraman, Rajaguru. & Dhavachelvan 2016, 38). Yksilöillä on erilaisia tarpeita yksityisyytensä turvaamiseen ja henkilötietojensa suojaamiseen. Yksilöt voidaan jakaa tarpeidensa mukaan kolmeen ryhmään (Nissenbaum 2011; Earp, Antón, Aiman-Smith & Stufflebeam 2005):

- tietosuojafundamentalistit, jotka ovat äärimmäisen huolestuneita yksityisyydestään
- Internet-käyttäjien pragmaattinen enemmistö, joka on huolestunut yksityisyydestään, mutta jonka huolia voidaan vähentää kertomalla tietojenkäsittelystä avoimesti ja läpinäkyvästi
- yksityisyydestään vähiten huolestuneet yksilöt, jotka ovat valmiita luovuttamaan tietoja itsestään palvelun ehdoista riippumatta.

Yksilöiden oikeutta yksityisyydensuojaan voidaan toteuttaa esimerkiksi antamalla käyttöön keinoja heidän omien tietojensa hallitsemiseen. Oikeuksien tehokkuuden varmistamiseksi on ensinnäkin selvitettävä, kohdistuvatko käyttäjien huolet yksityisyydestään palveluntarjoajaa vai muita käyttäjiä kohtaan. Mikäli käyttäjät eivät luota palveluntarjoajaan ja siihen, miten tämä käsittelee henkilötietoja, tarvitaan toimenpiteitä tietosuojakäytäntötasolla. Lisäksi on huomioitava, että käyttäjät eroavat toisistaan merkittävästi taidoiltaan, tietämykseltään ja riskikäyttäytymiseltään, ja näin ollen heidän yksityisyydensuojaa koskevat huolensa ovat erilaisia (Kowalewski ym. 2015, 816). Tehokkaan tietosuojakäytännön ominaisuuksia ja käyttäjän oikeuksia tietojensa hallintaan käsitellään seuraavissa luvuissa.

4.3. Viestintäsovellusten ja pilvipalveluiden parhaat tietosuojakäytännöt

Digitaaliset hyödykkeet ja tietosuoja

Digitaalinen hyödyke on tuote tai palvelu, joka toimitetaan tietoliikenneverkon välityksellä aineettomasti myyjältä asiakkaalle. Erään jaottelun mukaan digitaaliset tuotteet voidaan jakaa kolmeen ryhmään: tallenteet, datavirta ja digitaaliset palvelut. Tallenteet ovat eräänlaisia tavaroita, jotka toimitetaan tietoverkon kautta asiakkaalle. Datavirta on yksisuuntaista joukkoviestintää tietoverkossa, kuten esimerkiksi radio- tai televisiolähetys. Digitaaliset palvelut ovat yksinkertaisimmin määriteltyinä tietoliikenneverkon välityksellä toimitettavia palveluita (Salste 2000, 9–11). Lainsäädännössä digitaalisen palvelun määritelmä sisältää kolme ominaisuutta: digitaalinen palvelu on tietoyhteiskunnan palvelu, joka toimitetaan etäpalveluna sähköisessä muodossa palvelun vastaanottajan henkilökohtaisesta pyynnöstä ((EU) 2015/1535, 1 artikla 1 kohta b alakohta). Digitaalisia palveluita ovat edelleen esimerkiksi verkossa toimiva markkinapaikka, verkossa toimiva hakukone ja pilvipalvelu ((EU) 2016/1148, liite III).

Viestintäsovellus

Viestintäteknologian sovelluksilla, *viestintäsovelluksilla*, tarkoitetaan esimerkiksi älypuhelin- (mobiili-) ja videoneuvottelusovelluksia. Viestintäsovellukselle ei löydy kirjallisuudesta yksiselitteistä määritelmää, mutta sen määritelmä voidaan johtaa viestinnän ja sovelluksen määritelmistä. *Viestintä* on yksinkertaisimmillaan sanoman siirtoa ja vaihdantaa (Kunelius 1998, 10). Toisin sanoen viestien lähettäminen ja vastaanottaminen ovat viestintää. ITIL:n (2001, 5) määritelmän mukaan *sovellus* on ohjelmisto, joka tarjoaa Internet-palvelun tarvitsemat toiminnot. Sovellus toimii yhdessä tai useassa palvelimessa tai työasemassa, ja voi olla osa yhtä tai useampaa IT-palvelua. Viestintäsovellus on siis ohjelmisto, joka tarjoaa toiminnot sanoman siirtoon ja vaihdantaan, eli viestien lähettämiseen ja vastaanottamiseen.

Viestintäsovelluksen ja viestintäpalvelun väliset käsitteelliset erot on syytä huomioida. Viestintäpalvelu on palvelu, joka muodostuu kokonaan tai pääosin viestien siirtämisestä viestintäverkossa. Sekä viestintäpalveluissa että viestintäsovelluksissa viestien välittämiseksi käsitellään välitystietoja, jotka ovat joissain tapauksissa yhdistettävissä oikeus- tai luonnolliseen henkilöön siten, että tämä on tunnistettavissa niistä (TYK 3§). Käytännössä käsitteitä käytetään kuitenkin usein rinnakkain: esimerkiksi WhatsApp[9] määrittelee sovelluksen ”nopeasti ja luotettavasti toimivaksi viestintäpalveluksi” (WhatsApp 2015b). Henkilötiedon ja välitystiedon ero ei ole aina

[9] WhatsApp on viestintäsovellus, jota käyttää yli miljardi ihmistä 180 eri maassa. Sovellus on alun perin kehitetty vaihtoehdoksi perinteisille tekstiviesteille ja se on nykyään kasvanut monipuoliseksi viestintäsovellukseksi: sen avulla on mahdollista lähettää ja vastaanottaa erilaisia medioita, kuten tekstiä, kuvia, videoita, tiedostoja tai sijaintitietoja. <https://www.whatsapp.com/about/>, haettu 28.12.2016.

selvä: asiantuntijoiden mukaan toisinaan on vaikea määritellä, onko jokin tieto henkilö- vai välitystietoa. Tiedon luonne on tunnistettava, sillä niiden lainsäädännölliset käsittelyperusteet eroavat toisistaan. Henkilötietojen käsittelyperusteet löytyvät henkilötietolaista ja tulevaisuudessa yleisestä tietosuoja-asetuksesta, kun taas välitystietojen käsittelyperusteista säädetään kansallisessa tietoyhteiskuntakaaressa. Huomionarvoista on kuitenkin se, että välitystiedot ovat aina myös henkilötietoja, eivätkä käsitteet näin ollen ole toisensa poissulkevia.

Mobiililaitteet, ja niiden myötä myös niihin ladattavat sovellukset, ovat yleistyneet Suomessa viime vuosina nopeasti. Suomalaisista suurin osa (69 % vuonna 2015) käyttää mobiililaitteita, ja eniten niitä käytetään viestintään ja asioiden hoitoon (Suomen virallinen tilasto 2015). Monet sovellukset tarvitsevat tietoja käyttäjästä toimiakseen; osassa käyttäjä syöttää tietonsa itse ja toisissa sovellus pyytää lupaa päästä käsiksi joihinkin käyttäjän laitteella jo olemassa oleviin tietoihin. Joissain tapauksissa sovellukseen kirjaudutaan jonkun toisen palvelun tunnuksilla, jolloin ainakin osa käyttäjän tiedoista luultavimmin siirtyy palvelusta toiseen. Käyttäjän voi olla välillä vaikea muistaa, mitä tietoja hän jakaa mihinkin palveluun ja mihin näitä tietoja käytetään (Duncan 2014).

Pilvipalvelu

Pilvipalveluille (engl. *cloud services*) ei ole olemassa standardisoitua, yhtenäistä määritelmää, mutta yksinkertaisimmin ne ovat verkkoyhteyden välityksellä tarjottavia tietojenkäsittely- ja tallennuspalveluita sekä tietoliikennepalveluita (Kyberturvallisuuskeskus 2014, 5). Nämä palvelut ovat skaalautuvia eli helposti tarpeen mukaan säädettäviä, usean käyttäjän kesken jaettuja resursseja (Baun ym. 2011, 2–3). Heinäkuussa 2016 Euroopan unionin virallisessa lehdessä julkaistu verkko- ja tietoturvadirektiivi (NIS-direktiivi) käsittää pilvipalveluiksi palvelut, jotka ”mahdollistavat pääsyn skaalautuvaan ja mukautuvaan joukkoon jaettavissa olevia tietoteknisiä resursseja”. Nämä tietotekniset resurssit ovat verkkojen, palvelinten tai muun infrastruktuurin, sovellusten ja palvelujen, kaltaisia resursseja. Termillä ”skaalautuva” tarkoitetaan tietoteknisiä resursseja, joita pilvipalvelujen tarjoaja pystyy jakamaan joustavasti kysynnän vaihtelun mukaan resurssien maantieteellisestä sijainnista riippumatta. Termi ”mukautuva joukko” viittaa tietoteknisiin resursseihin, joita voidaan lisätä tai vähentää kysynnästä ja tarpeesta riippuen. Termi ”jaettavissa oleva” kuvaa niitä tietoteknisiä resursseja, joita tarjotaan useille käyttäjille palveluun, johon heillä on yhteinen pääsy, mutta jossa käsittely tapahtuu kuitenkin erikseen kunkin käyttäjän osalta ((EU) 2016/1148, johdanto-osan kappale 17; 4 artikla 19 kohta).

Yhdysvaltain standardointi- ja teknologiavirasto (NIST) määrittelee pilvipalveluiden viideksi pääominaisuudeksi seuraavat (Mell & Grance 2011, 2):

1. *Itsepalvelullisuus*: Kuluttaja voi käyttää resursseja tarpeensa mukaan automaattisesti ja itsenäisesti, ilman kahdensuuntaista vuorovaikutusta palveluntarjoajan kanssa.

2. *Pääteriippumattomuus*: Palvelut ovat saatavilla verkkoyhteyden välityksellä ja niihin pääsee kirjautumaan eri laitteilta, kuten mobiilipuhelimelta, tabletilta ja työasemalta.

3. *Resurssien yhteiskäyttö*: Palveluntarjoajan tietojenkäsittelyresurssit on jaettu siten, että niitä voidaan tarjota useille kuluttajille käyttäen erilaisia fyysisiä ja virtuaaliresursseja, kuluttajien kysynnästä riippuen. Käytännössä asiakkaalla on hyvin vähän tai ei lainkaan tietoa tarjottujen resurssien tarkasta sijainnista. Palveluntarjoajien on kuitenkin mahdollista määritellä sijainti yleisemmällä tasolla (esim. maa, kaupunki tai palvelinkeskus).

4. *Nopea joustavuus*: Resursseja voidaan tarjota ja vapauttaa joustavasti (joissain tapauksissa automaattisesti) siten, että resurssien määrä vastaa kysyntää.

5. *Käytön tarkka mittaaminen*: Resurssien käyttöä voidaan seurata ja hallita, mikä lisää läpinäkyvyyttä sekä palvelun käyttäjän että palveluntarjoajan kannalta.

Pilvipalvelut voidaan jaotella esimerkiksi sen mukaan, miten muotoiltua palvelua (palvelumallit) tarjotaan ja miten palvelun hankinta on järjestetty (hankintamallit). Pilvipalvelu ohjelmistoresurssina (engl. *Software as a Service, SaaS*) on yksinkertaisin malli ottaa käyttöön, mutta toisaalta käyttäjällä ei ole paljoa mahdollisuuksia vaikuttaa palvelun tekniseen tietoturvallisuuteen tai toteutukseen. Ohjelmistoresurssipalveluita ovat esimerkiksi verkkoselaimella käytettävät toimisto-ohjelmat ja tallennussovellukset. Alustapalvelumallissa (engl. *Platform as a Service*) palveluntarjoaja tuottaa valitsemaansa apuohjelmien ja sovelluskehitysympäristön kokonaisuuden. Palvelun käyttäjällä on mahdollisuus toteuttaa alustan päälle omat ohjelmistonsa ja niiden tietoturvaratkaisut. Käyttäjät eivät voi kuitenkaan vaikuttaa palvelun fyysisten tai virtuaalisten tietojärjestelmien käyttöjärjestelmiin. Infrastruktuuriresurssipalvelu (engl. *Infrastructure as a Service, IaaS*) tarjoaa käyttäjälle tietokoneiden laskentatehoa, tallennustilaa ja verkkoyhteyksiä. Tässä palvelumallissa asiakas saa itse valita tai toteuttaa ohjelmistot ja loogiset yhteydet (Kyberturvallisuuskeskus 2014, 5).

Palvelumallien lisäksi pilvipalvelut voidaan jakaa käyttöönottomallien mukaan: yksityinen, julkinen, yhteisö ja hybridi (Ramachandran & Chang 2016, 618). Yhdysvaltain standardointi- ja teknologiavirasto (NIST) määrittelee pilvipalveluiden käyttöönottomallit seuraavasti (Mell & Grance 2011, 3):

- *Yksityinen pilvi* (engl. *private cloud*): Pilviarkkitehtuuri tarjotaan yksinomaiseen käyttöön yhdelle organisaatiolle, joka sisältää useita käyttäjiä (esim. liiketoimintayksiköitä). Sen voi omistaa ja sitä voi hallita ja käyttää organisaatio itse, kolmas osapuoli tai näiden yhdistelmä.
- *Julkinen pilvi* (engl. *public cloud*): Pilviarkkitehtuuri tarjotaan julkisen yleisön avoimeen käyttöön. Sen voi omistaa ja sitä voi hallita ja pyörittää liike-, akateeminen tai valtionhallinnollinen organisaatio, tai joku näiden yhdistelmistä.
- *Yhteisöpilvi* (engl. *community cloud*): Pilviarkkitehtuuri jaetaan tietyn kuluttajayhteisön yksinomaiseen käyttöön. Yhteisö koostuu organisaatioista, joilla on yhteiset intressit (esim. tietoturvavaatimukset ja vaatimusmäärittelyt).
- *Hybridipilvi* (engl. *hybrid cloud*): Pilviarkkitehtuuri on kahden tai useamman arkkitehtuurin (yksityinen, julkinen tai yhteisö) yhdistelmä. Kukin arkkitehtuuri säilyy itsenäisenä kokonaisuutena, mutta ne on sidottu toisiinsa teknologialla, joka mahdollistaa datan ja sovellusten siirrettävyyden.

Viestintäsovellusten ja pilvipalveluiden tietosuojariskit

Tutkimuksen tulokset osoittavat, että viestintäsovelluksiin ja pilvipalveluihin liittyviä tietosuojariskejä ovat yhtäältä organisaation avoimuuden puute ja toisaalta kuluttajien heikko ymmärrys henkilötietojen käsittelytoimista. Tulosten analysoinnissa keskeisimmäksi riskitekijäksi nousivat informaation puute ja tietosuojakäytäntöjen epäselvyys. Käyttäjän on usein vaikea arvioida sovelluksen luotettavuutta saamiensa tietojen pohjalta niiden niukkuuden tai monimutkaisuuden takia. Signaaliteoriaa hyödyntäen voidaan todeta, että tietosuojakäytännöllä on merkittävä rooli hyödykkeen luotettavuuden osoittamisessa (Kirmani ym. 2000, 66–79). Informaation asymmetria muodostuu esimerkiksi silloin, kun organisaatiolla on asiakasta enemmän tietoa henkilötietojen käsittelytavoista (Spence 2002; Connelly, Certo, Ireland & Reutzel, 2011, 42). Tällöin asiakas saattaa tehdä päätöksensä käyttää palvelua puutteellisin tiedoin, ja sen myötä luovuttaa tietojaan enemmän kuin tosiasiassa haluaisi. Joissain tapauksissa tietosuojakäytännön puuttumisen tai puutteellisuuden nähdään johtavan jopa siihen, että kyseistä palvelua ei haluta ottaa käyttöön tai sen käyttöä ei haluta jatkaa.

Ricker, Schuurman ja Kessler (2015, 647) esittivät käyttäjien usein ymmärtävän, että heidän käyttämiinsä sovelluksiin liittyy tietosuojariskejä. Kuluttajien on osoitettu olevan yhä tietoisempia siitä, että heidän tietojaan saatetaan käyttää muihin tarkoituksiin kuin mihin ne alun perin kerätään (KPMG International 2016). Tämän tutkimuksen tulokset ovat osittain päinvastaisia: käyttäjät ovat kiinnostuneita yksityisyydensuojastaan periaatteellisella tasolla, mutta käytännössä he eivät ymmärrä viestintäsovelluksiin tai pilvipalveluihin liittyviä tietosuojariskejä. Lähes kaikissa asiantuntijahaastatteluissa merkittävimmäksi riskiksi nostettiin käyttäjien ymmärryksen puute. Käyttäjät eivät usein käsitä, mitä tietoja he antavat itsestään, mihin kerättyjä tietoja käytetään ja minkälaiset ehdot he hyväksyvät ottaessaan sovelluksen käyttöönsä.

Taulukkoon 4 on koottu tutkimuksessa löydetyt merkittävimmät tietosuojariskit, joita nykyaikaisiin viestintäsovelluksiin ja pilvipalveluihin liittyy. Lähestymistapa on kuluttajalähtöinen; miten palveluntarjoajan toimi vaikuttaa käyttäjän yksityisyydensuojaan ja minkälaisia mahdollisia seurauksia sillä on yksilölle. Suurin osa riskeistä toistuu sekä viestintäsovelluksissa että pilvipalveluissa ja lisäksi hyödykkeillä on omia erityispiirteitä. Erityispiirteiden jaottelu ei ole kuitenkaan tarkkarajainen. Toisin sanoen pilvipalveluiden riskit liittyvät tyypillisesti myös viestintäsovelluksiin, ja päinvastoin. Lisäksi on syytä muistaa, että moni viestintäsovellus toimitetaan pilvipalveluna, ja näin ollen myös pilvipalveluiden tietosuojariskit on otettava huomioon.

Taulukko 4: Viestintäsovellusten ja pilvipalveluiden tietosuojariskit.

Riski	Organisaatio	Kuluttaja
Avoimuuden puute	Organisaatiot eivät välttämättä tiedota tai kerro avoimesti siitä, minkälaista tietojenkäsittelyä viestintäsovellus ja/tai pilvipalvelu tekee.	Kuluttaja voi arvioida palvelun luotettavuutta pelkästään sen informaation perusteella, jonka palveluntarjoaja toimittaa (esim.i tietosuojakäytännössä).
Tietosuojakäytäntöjen tai sopimusehtojen epäselvyys	Organisaatio saattaa määritellä käytännöissään tai sopimusehdoissaan kohtia, joita käyttäjän on vaikea ymmärtää.	Kuluttaja ei välttämättä ymmärrä, mihin hän antaa suostumuksensa hyväksyessään palveluntarjoajan ehdot.
Puutteellinen informaatio tietojenkäsittelytoimista	Organisaatio ei välttämättä informoi käyttäjää tarpeeksi selkeästi tietojenkäsittelyprosesseista.	Yksittäisen kuluttajan on vaikea selvittää palveluntarjoajan tietojenkäsittelyprosesseja muualta kuin organisaation antamasta informaatiosta.
Riittämätön tai tulkinnanvarainen suostumus	Tietojen käsittelyyn ei välttämättä pyydetä riittävää hyväksyntää tai se voi olla liian ylimalkainen.	Palvelun käyttäjä saattaa antaa vahingossa tai ”pakon edessä” suostumuksensa sellaiseen tietojenkeräykseen tai -käsittelyyn, joka loukkaa hänen yksityisyyttään.
Liiallinen tietojenkeruu	Sovellukset saattavat pyytää pääsyä sellaisiin tietoihin (esim. käyttäjän kuviin), joita ne eivät tarvitse toimiakseen.	Käyttäjä ei aina ymmärrä, mitä kaikkea tietoa hänestä kerätään.
Tietojen käyttäminen muihin tarkoituksiin kuin palvelun toteuttamiseen	Palveluntarjoajat käyttävät asiakkaidensa tietoja usein myös muihin tarkoituksiin (esim. markkinointitarkoituksiin) kuin pelkkään palvelun tarjoamiseen.	Käyttäjälle ei välttämättä ole aina selvää se, että hänen tiedoillaan on markkina-arvoa, ja niitä myydään usein eteenpäin liiketoiminnallisin perustein.
Kolmansien osapuolten puutteellinen tietoturva ja tietosuoja	Kolmansien osapuolten tietoturva- ja tietosuoja-asioista ei välttämättä huolehdita, jolloin ei voida varmistua niiden riittävyydestä.	Käyttäjälle saattaa olla epäselvää, ketkä ovat kolmansia osapuolia ja minkälainen rooli heillä on viestinvälityksessä tai palvelun tarjoamisessa.
Tietojen siirto Suomen tai EU:n ulkopuolelle	Kun tietoja siirretään muihin maihin, muiden maiden lainsäädännöllisiä eroja ei välttämättä huomioida.	Kuluttajan on vaikea saada tietoa siitä, missä tietojenkäsittely tosiasiassa tapahtuu ja mihin maihin tietoja siirretään.
Tietojen poistaminen	Tietoja ei välttämättä poisteta tarvittavan ajan kuluessa kaikkialta, mihin niitä on tallennettu.	Käyttäjän poistaessa tietojaan sovelluksesta hän ei voi varmistua siitä, että tiedot tosiasiassa poistuvat kaikkialta.
Puutteellinen tietoturva	Henkilötietoja ei ole välttämättä turvattu riittävällä tasolla.	Mikäli viestintäsovellusten tietoturvassa on puutteita, käyttäjien tiedot saattavat joutua tietomurtojen kohteeksi.
Viestintäsovellusten erityispiirteet		
Viestinvälityksen varrella eri toimijoita	Viestinvälityksen varrella voi olla useita toimijoita, joiden tietosuoja- ja tietoturvakäytännöissä on hajanaisuutta.	Käyttäjän on usein vaikea hahmottaa, mitä eri toimijoita viestinvälityksen varrella on.
Salaamaton viestiliikenne	Mikäli viestiliikennettä ei salata päästä päähän, palveluntarjoaja tai kolmas osapuoli saattaa päästä käsiksi viestien sisältöihin.	Viestiliikenteen salaamattomuus heikentää käyttäjän luottamusta sovellusta kohtaan ja ei-toivotuilla osapuolilla saattaa olla pääsy käyttäjän viesteihin.

Pilvipalveluiden erityispiirteet		
Pilvipalveluiden kansainvälisyys	Pilvipalvelut tarjotaan hajautetusti ympäri maailmaa, jolloin palveluntarjoajan tulee huomioida alueiden väliset (esim. lainsäädännölliset) erot.	Kuluttajan on vaikea tai jopa mahdoton tietää, missä tietojenkäsittely tosiasiassa tapahtuu.
Kolmansien osapuolten pääsy tietoihin	Pilvipalvelut ovat eriasteisia, ja osapuolten vastuut vaihtelevat tasoittain. Kyseessä on kuitenkin palvelu, jossa on aina kolmas osapuoli mukana.	Kuluttaja tai käyttäjä ei välttämättä ymmärrä sitä, kenellä tai keillä on pääsy hänen tietoihinsa.
Tukihenkilöiden tai muiden ulkomaisten osapuolten pääsy tietoihin	Organisaatiot saattavat tarjota palvelua takaamalla, että palvelut pysyvät esimerkiksi ETA-alueella. Heillä saattaa kuitenkin olla muualla tukihenkilöitä, joilla on pääsy tietoihin.	Käyttäjän saattaa usein olla lähes mahdoton varmistua kaikista osapuolista, joilla on jonkinlainen pääsy häntä koskeviin tietoihin.
Tietojen turvaamiskäytännöt	Pilvipalveluiden kaikkien osapuolten tietoturvakäytännöt eivät aina ole riittävällä tasolla, jolloin tietomurron riski kasvaa.	Käyttäjän on vaikea varmistua siitä, että palveluntarjoaja ja eri osapuolet ovat toteuttaneet riittävät tekniset toimenpiteet turvatakseen ja suojatakseen käyttäjän tiedot.

Kuten taulukko 4 osoittaa, sovellukset tai palvelut pyytävät usein tietoja, joita ne eivät tarvitse toimiakseen. Sovelluksilla saattaa näin ollen olla pääsy sellaisiin tietoihin, joita käyttäjä ei haluaisi jakaa itsestään. Viestintäsovellukset pyytävät tyypillisesti pääsyä esimerkiksi laitteen yhteystietoihin, puhelutietoihin, kalenteritietoihin, sijaintitietoihin tai laitteen yksilöityyn id-tunnisteeseen. Kuluttajan kannalta haasteena on se, että hänen mahdollisuutensa suostumuksen antamiselle tai antamatta jättämiselle ovat usein rajalliset. Mikäli sovellusta haluaa käyttää, sille on annettava oikeudet päästä käsiksi niihin tietoihin, joita se pyytää. KPMG:n tekemän tutkimuksen vastaajista suurin osa (84 %) piti liian tunkeilevina sellaisia viestintäsovelluksia, joilla on pääsy käyttäjän yhteystietoihin, kuviin ja selaushistoriaan (KPMG International 2016, 14).

Viestintäsovellusten erityispiirteenä on, että viestinvälityksen varrella on usein eri toimijoita, joista osalla saattaa olla pääsy jopa viestien sisältöön. Viestinvälitykseen voi osallistua palveluntarjoajan ja asiakkaan lisäksi esimerkiksi operaattoreita, viestintäyrityksiä tai tiedonkäsittelijöitä. Käyttäjän on usein vaikea hahmottaa eri toimijoita ja näiden rooleja; usein ajatellaan, että viestinnän osapuolina ovat pelkästään viestin lähettäjä ja vastaanottaja. Viestinnän tietosuojaa voidaan parantaa esimerkiksi viestiliikenteen salauksella. Duncanin (2014) mukaan yksi riskialttiimmista asioista, jonka mobiilisovellus voi tehdä, on tallentaa käyttäjästä kerättyjä henkilötietoja salaamattomana. Kaupallisista viestintäsovelluksista esimerkiksi WhatsApp tarjoaa asiakkaidensa viestinnälle suojaa salaamalla viestien sisällöt päästä päähän. Päästä päähän -salaus (engl. *end-to-end encryption*) tarkoittaa sitä, että viestit suojataan salaamalla, eivätkä palveluntarjoaja tai kolmannet osapuolet näin ollen voi lukea viestien sisältöä (WhatsApp 2016a). Tutkimukseen haastateltujen asiantuntijoiden mukaan viestinnän salaaminen on erittäin tärkeää viestintäsovelluksen luotettavuuden kannalta. Heidän mukaansa viestiliikenteen salaamattomuus on merkittävä riski käyttäjän yksityisyydensuojalle. Mikäli ei-toivotut osapuolet pääsevät käsiksi viestien sisältöön, käyttäjien luottamus palvelua kohtaan heikkenee.

Palveluihin liittyvien tietosuoja- ja tietoturvariskien tunnistaminen ja niistä ilmoittaminen on tärkeää, jotta asiakas voi niiden pohjalta harkita, kokeeko hän palvelun riittävän turvalliseksi ja haluaako hän käyttää palvelua (Svantesson & Clarke 2010, 3). Riskilähtöisen ajattelun kannalta on olennaista jakaa pilvimallit kahteen (Svantesson ym. 2010, 4):

- kotimaiset pilvipalvelut
- kansainväliset pilvipalvelut.

Mikäli palvelu sijaitsee fyysisesti vain yhden ja saman hallintoalueen sisällä, voidaan puhua kotimaisesta pilvipalvelusta. Tietosuojariskejä liittyy sekä kotimaisiin että kansainvälisiin pilvipalveluihin, joista jälkimmäisiin kohdistuu erityisiä haasteita. Kaikki haastateltavat nimesivät pilvipalveluiden kansainvälisyyden merkittäväksi tietosuojariskiksi. Kuluttajan on usein mahdotonta tietää, missä tietojenkäsittely tosiasiassa tapahtuu. Näin ollen hänellä on erittäin rajalliset mahdollisuudet arvioida tietojenkäsittelytoimien luotettavuutta ja vaatimustenmukaisuutta. Alueiden väliset lainsäädännölliset erot ovat riski kuluttajan yksityisyydensuojalle myös siksi, että keskivertokuluttaja ei tyypillisesti tunne eri maiden sääntelyä.

Alueellisen ulottuvuuden lisäksi pilvipalvelumalli vaikuttaa tietosuojariskeihin ja -vastuisiin. Palveluntarjoajan tekemät ratkaisut ja soveltamat käytännöt vaikuttavat vähiten, kun pilvipalvelu ostetaan infrastruktuuritasolla. Tällöin voidaan puhua käytännössä tallennuskapasiteetista, ja palvelun ostajalle jää suurin vastuu tietosuoja- ja tietoturvatoimenpiteiden toteutuksesta. Myös alustapalvelumallissa palveluntarjoajalle jää vähemmän vastuuta. Sovellustasolla tietosuojavastuu taas on lähes täysin palveluntarjoajalla. Kuluttajapalveluissa tämä tarkoittaa sitä, että käyttäjä on riippuvainen palveluntarjoajan ratkaisuista. Se merkitsee myös sitä, että käyttäjä voi arvioida pilvipalvelun luotettavuutta pelkästään palveluntarjoajalta saamansa tiedon perusteella. Pilvipalvelumallista riippumatta kyseessä on palvelu, jossa on aina mukana kolmas osapuoli. Osa haastateltavista korosti kolmansien osapuolten merkitystä palvelun sijainnin kannalta: tietojen käsittelijä saattaa luvata tietojen sijaitsevan tietyllä alueella, mutta sen tukihenkilöillä tai muilla ulkopuolisilla saattaa olla pääsy tietoihin muualta. Palveluntarjoajat saattavat taata palvelun pysyvän ETA-alueella. Lupaus ei kuitenkaan toteudu täysin, mikäli tukihenkilöt sijaitsevat esimerkiksi Aasiassa. Näin ollen tietoihin on pääsy myös ETA-alueen ulkopuolelta, vaikka tiedot sijaitsisivat fyysisesti Euroopassa. Kolmansiin osapuoliin liittyväksi haasteeksi nimettiin myös tiedonsuojaus- ja turvaamistoimien riittävyydestä varmistuminen. Kuluttaja-asiakkaan on miltei mahdoton selvittää ja arvioida eri osapuolten luotettavuutta.

Hyvä tietosuojakäytäntö

Tietosuojakäytäntö (engl. *privacy policy*) on menettelytapa, määritelmä tai selvitys, jossa yritys tai palveluntarjoaja määrittelee tavat, joilla se kerää ja käsittelee asiakkaidensa henkilötietoja. Toisin sanoen tietosuojakäytäntö on asiakirja, joka kertoo sen lukijoille, miten tietty teknologia, tuote tai palvelu käsittelee käyttäjän henkilötietoja. Sen tulisi kattaa koko se tiedonmäärän kirjo, jota palveluntarjoaja saa käyttäjästä. Tietosuojakäytäntö voi olla esillä esimerkiksi sähköisesti palveluntarjoajan Internetsivuilla (Aïmeur ym. 2016, 368). Haastatteluiden perusteella tietosuojakäytännöt voidaan nähdä joko konkreettisina toimenpiteinä, joita yritys tai organisaatio toteuttaa tietosuojan varmistamiseksi tai asiakirjana, jossa kerrotaan näistä henkilötietojen käsittelyyn liittyvistä toimista. Näin ollen tietosuojakäytäntö on käsitteenä laaja: sitä voidaan käyttää nimityksenä niin käytännön toiminnasta kuin myös juridisesti sitovasta sopimuksesta tai suositushenkisestä asiakirjasta.

Tietosuojakäytäntö sisältää tyypillisesti seuraavat kappaleet (Crowe ym. 2013, 27):

- *Johdanto* – kerrotaan käyttäjälle palveluntarjoajayrityksestä tai organisaatiosta

- *Tiedot, jotka käyttäjästä kerätään* – kuvaillaan käyttäjälle, mitä tietoa hänestä kerätään, vaikka se saattaisi olla itsestään selvää (esim. pyydettäessä käyttäjää täyttämään lomake henkilötiedoillaan)
- *Tiedonkeräystavat* – tarkennetaan tavat, joilla käyttäjästä kerätään tietoa (esim. automaatio, käyttäjän täyttämät lomakkeet tai epäsuorat tavat kerätä tietoa käyttäjistä)
- *Tietojen tallentaminen* – kerrotaan, miten ja mihin tiedot tallennetaan. Tämän osion tulee myös vahvistaa ja osoittaa käyttäjän oikeudet heistä tallennettujen tietojen suojaukseen ja turvallisuuteen.

Tietosuojakäytäntöä määriteltäessä on hyvä huomioida siihen rinnastettavat käsitteet: rekisteriseloste ja tietosuojaseloste. Nykyisen henkilötietolain mukaan rekisterinpitäjän on laadittava rekisteriseloste, josta käyvät ilmi muun muassa rekisterinpitäjän yhteystiedot, henkilötietojen käsittelyn tarkoitus ja se, mihin tietoja säännönmukaisesti luovutetaan ja siirretäänkö niitä Euroopan unionin ulkopuolelle (HetiL 10 §.). Henkilötietolaissa määritelty informointivelvollisuus koskee kaikkia rekisterinpitäjiä, ja sitä voi toteuttaa laatimalla tietosuojaseloste. Tietosuojaseloste on samantyylinen asiakirja kuin rekisteriseloste, mutta siinä informoidaan lisäksi rekisteröityjen oikeuksista (Tietosuojavaltuutetun toimisto 2014). Tietosuoja-asetuksen ((EU) 2016/679) artiklan 30 mukaan jokaisen rekisterinpitäjän on ylläpidettävä selostetta vastuullaan olevista tietojenkäsittelytoimista. Tietosuojaseloste ja tietosuojakäytäntö voivat olla käytännössä sama asiakirja, mutta ne on mahdollista pitää myös toisistaan erillisinä. Rekisterinpitäjä voi julkaista esimerkiksi verkkosivuillaan tietosuojakäytännön, jossa kerrotaan yleisemmällä tasolla tietojenkäsittelytavoista. Tietosuojaselosteen taas on täytettävä rekisterinpitäjän laajemmat velvollisuudet toimittaa rekisteröidylle tietoa. Mikäli tietosuojakäytäntö ja tietosuojaseloste halutaan julkaista erillisinä asiakirjoina, tietosuojaseloste kuitenkin todennäköisesti pitkälti ohjaa tietosuojakäytäntöjen laatimista.

Tietosuojakäytännön tavoitteena on kertoa läpinäkyvästi tietojen käsittelystä. Siinä tulisi välttää kapulakieltä ja kuvata asiat loppukäyttäjälle helposti ymmärrettävällä tavalla (Aïmeur ym. 2016, 368). Tutkimustulokset vahvistavat aiempia osoituksia siitä, että käyttäjät jättävät tietosuojakäytännöt usein lukematta (Aïmeur ym. 2016, 368; Capistrano ym. 2015, 24; Michota ym. 2015, 139; Geng ym. 2010, 58). Syitä löytyy sekä organisaatioista että käyttäjistä itsestään. Yhtäältä palveluiden tietosuojakäytännöt ja käyttöehdot ovat epäselviä tai vaikeasti ymmärrettäviä, ja toisaalta käyttäjä ei aina ymmärrä tai edes yritä ymmärtää niitä. Tutkimusten mukaan tehokas tietosuojakäytäntö on selkokielinen, helppolukuinen, ymmärrettävä ja täsmällinen (Capistrano ym. 2015, 29; Earp ym. 2005, 229). EU:n tietosuoja-asetus vaatii, että rekisteröidystä kerätyt tiedot toimitetaan ((EU) 2016/679 artikla 12, kohta 1)

- tiiviisti esitetyssä muodossa
- läpinäkyvässä muodossa
- helposti ymmärrettävässä ja helposti saatavilla olevassa muodossa
- selkeällä ja yksinkertaisella kielellä
- kirjallisesti tai muulla tavoin
- tapauksen mukaan sähköisessä muodossa.

Tietosuojakäytäntöjen vaikutus palveluntarjoajan luotettavuuteen

Luottamusta konseptina on tutkittu monella eri tieteenalalla, mutta yksiselitteistä määritelmää sille ei ole löydetty. Perusajatus kaikissa tieteissä tuntuu kuitenkin olevan selvä: luottamus tarkoittaa luottajan uskoa siihen, ettei luottamuksen kohde petä (Tiainen, Luomala, Kurki & Mäkelä 2004, 11). Tietojärjestelmätieteessä luottamusta on tutkittu lähinnä organisaatioiden välisen vuorovaikutuksen kautta (Gefen,Karahanna & Straub 2003, 53–55), kun taas esimerkiksi filosofiassa luottamus käsitetään ihmisen haluna uskoa toisista

hyvää (Tiainen ym. 2004, 12). Luottamus voidaan määritellä myös vakuuttuneisuudeksi siitä, että toisen osapuolen käytös vastaa luottajan odotuksia ja yhteistä hyväntahtoisuutta (Lacity, Khan, Yan & Willcocks 2010, 409). Digitaalisten palvelujen luotettavuus tulee olemaan entistä suuremmassa roolissa lähitulevaisuudessa (valtiovarainministeriö 2016, 14). Tutkimukset osoittavat, että kuluttajan luottamusta digitaalisia palveluita tarjoavia organisaatioita kohtaan voidaan lisätä esimerkiksi läpinäkyvän informoinnin avulla. Tietosuojakäytäntöjen on nähty toimivan organisaation luotettavuuden signaalina (Earp ym. 2005, 235.).

Aljukhadar, Senecal ja Oullette (2010, 103–126) esittävät, että kuluttajien halukkuus paljastaa itsestään tietoja perustuu heidän arvioonsa tietojen luovuttamisen kustannuksista, riskeistä ja hyödyistä. Näin ollen he etsivät osoituksia näistä. Kuluttajat voivat arvioida yrityksen luotettavuutta esimerkiksi tietosuojakäytännön pohjalta. Käyttäjä kokee palvelun käytön turvallisemmaksi ja olonsa mukavammaksi, mikäli hänelle kerrotaan selkeästi, miten hänen henkilötietojaan käsitellään (Aljukhadar ym. 2010; Geng ym. 2010, 58). Yksilöiden päätöksentekoprosesseihin vaikuttaa tieto; he tekevät päätöksiä saatavillaan olevien tietojen pohjalta. Informaation asymmetria (engl. *information asymmetry*) syntyy, kun ’eri ihmiset tietävät eri asioita’. Toisin sanoen, informaation asymmetria vaikuttaa yksilön päätöksentekoon esimerkiksi siten, että hänen arvionsa palvelun luotettavuudesta saattaa perustua puutteelliseen informaatioon (Connelly ym. 2011, 42). Signaaliteorian pohjimmaisena tarkoituksena on vähentää osapuolten välillä epätasaisesti jakautuvaa informaatiota eli informaatioasymmetriaa. Signaaliteorian mukaan ”tietoinen” osapuoli välittää toiselle osapuolelle signaaleja, joiden avulla tämä voi tehdä parempia tietoon perustuvia valintoja (Spence, 2002).

Tehokkailla signaaleilla on kaksi pääluonteenpiirrettä: signaalin havaittavuus (engl. *signal observability*) ja signaalin kustannus (engl. *signal cost*). Signaalin havaittavuus viittaa siihen, kuinka hyvin vastaanottajat eli ulkopuoliset pystyvät havaitsemaan signaalin (Connelly ym. 2011, 45). Kuten edellä esitettiin, tietosuojakäytännön laittaminen julkisesti saataville ei yksinään riitä ollakseen tehokas. Organisaatioiden tulisi varmistaa, että tietosuojakäytännöt viestitään kunnolla asiakkaille (Capistrano ym. 2015, 29). Signaaliteorian nojalla voidaan siis todeta, että organisaation julkaiseman tietosuojakäytännön tehokkuus riippuu osittain yksilön kyvystä havaita ja löytää tietosuojakäytäntö, millä taas saattaa olla vaikutuksia käyttäjän kokemaan luottamukseen organisaatiota ja tämän tarjoamia palveluita kohtaan. Jälkimmäinen ominaisuus eli signaalin kustannus viittaa siihen, että jotkut organisaatiot ovat toisia paremmassa asemassa signaloinnista aiheutuvien kustannusten hallinnassa. Esimerkkinä voidaan käyttää sertifiointia: ISO9001-(laatu)sertifiointi on edullisempi korkealaatuiselle valmistajalle kuin heikkolaatuiselle valmistajalle, sillä jälkimmäisen täytyisi toteuttaa huomattavasti enemmän muutoksia saadakseen sertifikaatin. Nämä muutokset toisivat lisäkustannuksia organisaatiolle, mikä voidaan nähdä ”luotettavuudesta signaloinnin” kustannuksena (Connelly ym. 2011, 45).

4.4. Käyttäjien mahdollisuudet hallita tietojaan ja vaihtaa palveluntarjoajaa

Rekisteröidyn oikeuksien toteutuminen

Tietosuoja voidaan määritellä yksilön mahdollisuudeksi hallita henkilökohtaisia tietojaan (Smith ym. 1996, 167; Wolf 2012; Pentina ym. 2016, 410). Toisin sanoen yksilöiden tiedollista itsemääräämisoikeutta voidaan toteuttaa esimerkiksi antamalla keinoja omien tietojen hallintaan (Kowalewski ym. 2015, 816). Tutkimukseen haastateltujen asiantuntijoiden mukaan käyttäjillä tulisi olla tietyt oikeudet hallita tietojaan ilman, että heidän tulisi osata vaatia niitä erikseen. Rekisteröidyn oikeuksien tavoitteena on taata henkilötiedoille suoja valtuudettomalta tai yksilöä

vahingoittavalta tietojen käytöltä. Käyttäjien mahdollisuudet hallita tietojaan ja vaihtaa palveluntarjoajaa ovat keskeisiä tietosuoja-asetuksen asettamia rekisteröidylle annettavia oikeuksia. Asetuksen mukaan rekisteröidyllä tulee olla taulukon 5 mukaiset oikeudet tietojensa hallintaan ((EU) 2916/679, 15–22, 34 artiklat). Tietosuoja-asetuksessa määritellyt rekisteröidyn oikeudet ovat osittain samoja kuin henkilötietolaissa säädetyt oikeudet. Asetuksen myötä oikeudet kuitenkin laajenevat, ja uusina tulevat esimerkiksi rekisteröidyn oikeus siirtää tiedot järjestelmästä toiseen ja saada ilmoitus henkilötietojen tietoturvaloukkauksesta.

Taulukko 5: Käyttäjien mahdollisuudet hallita tietojaan kaupallisissa palveluissa.

Rekisteröidyn oikeus	Nykylainsäädäntö	Tuleva lainsäädäntö
Oikeus antaa tai olla antamatta suostumus henkilötietojen käsittelylle		(EU) 2016/579, 7 artikla
Oikeus saada pääsy tietoihin	HetiL, 26 § (tarkastusoikeus)	(EU) 2016/579, 15 artikla
Oikeus tietojen oikaisemiseen	HetiL, 29 § (tiedon korjaaminen)	(EU) 2016/579, 16 artikla
Oikeus tietojen poistamiseen	HetiL, 29 § (tiedon korjaaminen)	(EU) 2016/579, 17 artikla
Oikeus käsittelyn rajoittamiseen		(EU) 2016/579, 18 artikla
Oikeus siirtää tiedot järjestelmästä toiseen		(EU) 2016/579, 20 artikla
Oikeus vastustaa tietojen käsittelyä, automaattista päätöksentekoa ja profilointia	HetiL, 31 § (automatisoitu päätös)	(EU) 2016/579, 21–22 artiklat
Oikeus saada ilmoitus henkilötietojen tietoturvaloukkauksesta		(EU) 2016/579, 34 artikla

Asiantuntijoiden mukaan käyttäjien oikeudet eivät toteudu täysmääräisesti useimmissa viestintäsovelluksissa ja pilvipalveluissa. Tutkimuksen tulokset osoittavat, että vaikka käyttäjille annetaan oikeuksia hallita tietojaan, oikeudet ovat usein *näennäisiä*. Näennäisyydellä tarkoitetaan sitä, että käyttäjän mahdollisuudet hallita tietojaan saattavat olla tosiasiassa rajallisemmat kuin palveluntarjoaja antaa ymmärtää. Haastateltavat korostivat rekisteröityjen oikeuksien tärkeyttä. Heidän mukaansa kuluttajille tulee antaa mahdollisuus hallita tietojaan, vaikka he eivät osaisi sitä itse vaatia tai etsiä. Myös tietosuoja-asetuksen nähdään ohjaavan siihen, että käyttäjää suojellaan häneltä itseltään. Näin ollen palveluntarjoajien tulee miettiä entistä tarkemmin sekä tietojenkäsittelyn riskejä yksittäisen kuluttajan kannalta että heille annettavia mahdollisuuksia hallita tietojaan.

Mikäli tietojenkäsittely perustuu käyttäjän antamaan suostumukseen, suostumuksen antamista koskeva pyyntö tulee esittää muista asioista erillisenä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä kielellä. Rekisteröidyllä on oikeus peruuttaa suostumuksensa milloin tahansa, ja peruuttamisen tulisi olla yhtä helppoa kuin suostumuksen antaminen. ((EU) 2016/679, 7 artikla.) Haastatteluissa kävi ilmi, että käytännössä suostumuksen peruuttaminen ei ole aina mutkatonta. Usein kun sovellus tai palvelu otetaan käyttöön, käyttäjän on sitouduttava tietojenkäsittelyä koskeviin vakioehtoihin voidakseen käyttää palvelua. Käyttäjä saattaa tällöin joutua antamaan suostumuksensa sellaisille toimille, jotka loukkaavat hänen yksityisyyttään. Toisin sanoen mikäli henkilö haluaa käyttää palvelua, hänen on väistämättä suostuttava kaikkiin tietosuojakäytännössä määriteltyihin tietojen keräys- ja käsittelytoimiin. Jos ja kun käyttäjä haluaa peruuttaa suostumuksensa, ainoa keino tähän saattaa olla palvelun käytön lopettaminen. Rekisteröidyn oikeuksien tehokkaan toteutumisen kannalta tämä nähdään ongelmallisena, sillä se on ristiriidassa suostumuksen vapaaehtoisuusvaatimuksen kanssa. Tietosuoja-

asetuksen mukaan suostumuksen vapaaehtoisuus tarkoittaa, että rekisteröidyllä tulisi olla todellinen vapaan valinnan mahdollisuus. Käyttäjän on voitava näin ollen kieltäytyä suostumuksen antamisesta tai peruuttaa se ilman, että siitä aiheutuu hänelle haittaa ((EU) 2016/679, kohta 42).

Tietosuoja-asetus ((EU) 2016/679) ohjaa organisaatioita antamaan kuluttajille oletusarvoista (”Privacy by Default”) ja sisäänrakennettua (”Privacy by Design”) suojaa, jota voidaan toteuttaa esimerkiksi suostumuksen hallinnan avulla. Palveluntarjoajien tietosuojakäytännöissä suostumusta käsitellään eri tavoin. Google kertoo pyytävänsä rekisteröidyltä aina erillisen suostumuksen arkaluonteisten henkilötietojen jakamiseen. Muita kuin arkaluontoisia henkilötietoja jaetaan yrityksille, organisaatioille ja kolmansille osapuolille vain, mikäli ”olet antanut siihen luvan”. Käyttäjän katsotaan antaneen suostumuksensa eli ”luvan” tietosuojakäytännössä ilmoitettuihin tietojenkäsittelytoimiin hyväksyessään käytännössä määritetyt ehdot ennen palvelun käyttöönottoa. Tietosuojakäytännössä ei kuitenkaan tarkenneta, mihin asti käyttäjän antama suostumus ulottuu tai mitä mahdollisuuksia hänellä on hallita antamaansa suostumusta (Google 2016). WhatsApp puolestaan ilmoittaa, että käyttäjä voi poistaa tilinsä milloin tahansa, jonka lisäksi hän voi peruuttaa suostumuksensa tietojenkäsittelylle. Käyttäjän peruuttaessa suostumuksensa mahdollisuus käyttää palvelua kuitenkin lakkaa, sillä viestintäsovelluksen käyttö edellyttää henkilötietojen tallentamista, käsittelyä ja jakamista (WhatsApp 2016a).

Tietojen poistaminen eli ”oikeus tulla unohdetuksi” nähtiin kaikissa haastatteluissa yhtenä tärkeimmistä rekisteröidyn oikeuksista. Oikeuden tehokkaasta ja tosiasiallisesta toteutumisesta voi kuitenkin olla vaikea varmistua. Erityisesti pilvipalveluiden kansainvälisyys lisää haasteita; miten voidaan varmistua siitä, että tieto poistuu kaikista niistä paikoista, minne se on tallentunut. Myös tietojenkäsittelyn levinneisyys monimutkaistaa tietojen tehokasta poistamista. Tietosuoja-asetuksen mukaan henkilötiedot julkistaneen rekisterinpitäjän tulisi ilmoittaa muille näitä tietoja käsitteleville rekisterinpitäjille, että rekisteröity on pyytänyt tietojen poistamista. Huomionarvoista on, että kaikki tietoihin liittyvät linkit tai tietojen jäljennökset tai kopiot tulee poistaa. ((EU) 2016/679, johdanto-osan kappale 66.) Oikeus tulla unohdetuksi tulee kyseeseen erityisesti silloin, jos suostumus on annettu rekisteröidyn ollessa lapsi. Lapsen ei voida katsoa olevan täysin tietoinen tietojenkäsittelyyn liittyvistä riskeistä, joten hänelle tulee antaa mahdollisuus poistaa tietojaan myöhemmin Internetistä. Lapsiin kohdistuu muitakin erityishuomioita. Tietosuoja-asetuksen mukaan esimerkiksi alle 16-vuotiaan lapsen henkilötietojen käsittely on lainmukaista vain, mikäli lapsen vanhempainvastuunkantaja on antanut siihen suostumuksen ((EU) 2016/679, 8 artikla). Eräs haastateltava kertoi tapauksesta, jossa alaikäisten oikeudet otettiin huomioon jo palvelua suunniteltaessa. Kyseessä oli nuorten chat-palvelu, jossa lapset saivat asiantuntija-apua esimerkiksi mielenterveysongelmiin. Palveluntarjoaja päätti toteuttaa palvelun siten, että käyttäjät pysyivät anonyymeinä palvelussa. Palvelun toteutuksen kannalta ei ollut olennaista kerätä käyttäjiä yksilöivää tietoa, kuten ip-osoitteita, jolloin heille voitiin tarjota anonyymi palvelu. Tietojen poistamista ja anonymisointia käsitellään tarkemmin seuraavassa seuraavaksi.

Tietosuoja-asetuksen ((EU) 2016/679, 21–22 artiklat) myötä jokaisella luonnollisella henkilöllä on oikeus kieltäytyä profiloinnista, eli häneen merkittävällä tavalla vaikuttavasta toimenpiteestä, joka on tehty yksinomaan automaattisella tietojenkäsittelyllä henkilön tiettyjen yksilöllisten ominaisuuksien tai esimerkiksi taloudellisen tilanteen perusteella hänen käyttäytymisensä analysoimiseksi tai ennakoimiseksi. Tällaiseen tietojenkäsittelyyn perustuva päätöksenteko on sallittua, mikäli jokin seuraavasta kolmesta ehdosta täyttyy:

1. siihen annetaan eksplisiittinen lupa rekisterinpitäjään sovellettavassa unionin tai kansallisessa lainsäädännössä

2. rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekeminen tai täytäntöönpano edellyttää sitä

3. rekisteröity on antanut siihen nimenomaisen suostumuksensa.

Mikäli tietojen käsittely, automaattinen päätöksenteko tai profilointi perustuu käyttäjän antamaan suostumukseen, sen antamisesta tulisi voida kieltäytyä ilman, että siitä aiheutuu käyttäjälle haittaa. Haastatteluissa nousi esiin erityisesti kysymykset profiloinnin laajuudesta ja tarpeellisuudesta. Asiantuntijoiden mukaan useimmissa viestintäsovelluksissa ja pilvipalveluissa käyttäjiä profiloidaan usein enemmän kuin palvelun toteuttamisen kannalta olisi tarpeen. Toisin sanoen käyttäjistä halutaan saada enemmän tietoja, jotta heidän käyttäytymistään voitaisiin analysoida paremmin. Profilointi ei kuitenkaan usein ole käyttäjän kannalta epäedullista. Asiantuntijat näkivät sen pääosin positiivisena teknologisena kehityksenä, sillä siten asiakkaille voidaan räätälöidä parempia ja yksilöllisempiä palveluita. Pulmallista sen sijaan on se, että profilointi ei ole kuluttajille aina läpinäkyvää ja helposti ymmärrettävää.

Kaupallisista palveluntarjoajista esimerkiksi Google antaa käyttäjälle oikeuden rajoittaa automaattista tietojenkäsittelyä. Organisaation julkaiseman tietosuojakäytännön mukaan käyttäjä voi hallita Google-tiliinsä liittyviä tietoja ja mainosasetuksia sekä estää evästeet. Mikäli evästeet poistetaan käytöstä, kaikki palvelut eivät toimi kunnolla. Hallintamahdollisuudet ovat rajalliset, sillä käyttäjä ei voi vastustaa täysin automaattisten järjestelmien analysointia. Google tekee automaattista tietojenkäsittelyä käyttäjän sisältöjen, mukaan lukien sähköpostiviestien, analysoimiseksi, minkä tavoitteena on parempien palveluiden tarjoaminen. (Google 2016.) Haastateltujen asiantuntijoiden mukaan tällaiset käytännöt ovat erittäin yleisiä ja käyttäjien tosiasiallisten oikeuksien kannalta haasteellisia. Moni palveluntarjoaja antaa asiakkailleen näennäisiä mahdollisuuksia hallita tietojaan, mutta oikeastaan varaa itselleen laajat oikeudet hyödyntää käyttäjistä kerättyjä tietoja. Keskivertokuluttajan yksityisyydensuojan kannalta tämä on riski, sillä hän ei välttämättä ymmärrä henkilötietoihinsa kohdistuvien tietojenkäsittelytoimien laajuutta.

Oikeus siirtää tiedot järjestelmästä toiseen

EU:n tietosuoja-asetuksen myötä rekisteröidyillä on jatkossa oikeus siirtää tiedot järjestelmästä toiseen. Käytännössä tämä tarkoittaa sitä, että rekisteröidyn tulee saada häntä koskevat henkilötiedot yleisesti käytetyssä, jäsennellyssä ja yhteentoimivassa siirtomuodossa, jotta hän voi siirtää ne toiselle palveluntarjoajalle (valtiovarainministeriö 2016, 16; (EU) 2016/679, johdanto-osan kappale 68). Haastateltavien näkemykset vaatimuksen käytännön toteuttamisesta poikkesivat toisistaan. Osa näki oikeuden välttämättömänä osana digitalouden luotettavaa toimimista, osa taas koki oikeuden vähemmän merkittävänä kuluttajan yksityisyydensuojan kannalta. Kaikki haastateltavat olivat kuitenkin sitä mieltä, että käyttäjän tulee saada palveluun itse syöttämänsä tiedot mukaansa halutessaan vaihtaa palveluntarjoajaa. Tiedon omistajuuden nähtiin olevan tällöin selkeä: käyttäjä omistaa tiedot, jotka hän on itse toimittanut palveluntarjoajalle. Myös asetusteksti määrittelee siirto-oikeuden koskevan ”henkilötietoja, jotka hän [rekisteröity] on toimittanut” ((EU) 2016/679, johdanto-osan kappale 68).

Haastateltavien näkemykset siitä, ulottuuko oikeus palvelun aikana syntyneisiin tietoihin, vaihtelivat. Eräs haastateltava käytti esimerkkinä pankki- ja vakuutuspalveluita, jotka usein tuottavat laskelmia ja muita tietoja asiakkaidensa datasta. Hänen mukaansa sellaiset tiedot, jotka palveluntarjoaja on tuottanut käyttäjän antamista tiedoista, kuuluisivat palveluntarjoajalle. Asiakkaiden henkilötiedot ovat kuitenkin erityislaatuinen omaisuuserä, koska niiden ei voida katsoa olevan yrityksen omaisuutta. Teoriassa on mahdollista, että luonnollinen henkilö haluaisi kaikki häneen liittyvät tiedot itselleen. Tiedon omistajuusnäkökulmasta ei näin ollen ole itsestään selvää, että vain rekisteröidyn toimittamat tiedot kuuluisivat siirto-oikeuden piiriin.

Vaihtoehtona tietojen poistamiselle nähtiin tietojen *anonymisointi* eli tietojen käsittely siten, että niistä poistetaan tunnistetiedot peruuttamattomasti. Anonymisoinnin käsitteellinen määritelmä voidaan muodostaa direktiivin 95/46/EY johdanto-osan kappaleesta 26 (Tietosuojatyöryhmä 2014 (WP 216), 5). Sen nojalla tietojen anonymisoimiseksi niistä on poistettava elementtejä siten, ettei rekisteröityä voida enää tunnistaa niiden perusteella. Tietoja on siis prosessoitava siten, ettei rekisterinpitäjän tai kolmannen osapuolen ole enää mahdollista käyttää tietoja yksilön tunnistamiseen, kun huomioidaan kaikki kohtuullisesti käytettävissä olevat keinot (Tietosuojatyöryhmä 2014 (WP 216), 5). Määritelmässä tärkeä tekijä on käsittelyn peruuttamattomuus, eli tunnistetiedot eivät saa olla palautettavissa tietoihin. Täytyy muistaa, ettei anonymisoitu data ole täysin riskitöntä tietosuojan näkökulmasta. Jos esimerkiksi tilastolliset otokset väestöstä ovat pieniä ja ne yhdistetään kapeisiin maantieteellisiin alueisiin, harvaan asutuilla alueilla yksittäisten henkilöiden tunnistaminen saattaa helpottua (Castrén 2015, 27). Tiedon anonymisoinnin on oltava tehokasta ja kestävää. Menettelyn tehokkuutta mitataan sillä, kuinka hyvin se vähentää uudelleenidentifikaation riskiä (Information Comissioner's Office 2012, 16). Haastattelujen pohjalta voidaan todeta, että moni palveluntarjoaja harvoin luopuu käyttäjistä kerätyistä tiedoista täysin palvelun käytön lakattua. Näin ollen rekisteröidyn siirtäessään tietonsa toiselle palveluntarjoajalle, nykyinen palveluntarjoaja voisi säilyttää tiedot anonymisoituina tietojen poistamisen sijaan. Tämä nähtiin hyvänä menettelynä myös kansantalouden kannalta. Suomalaisista kuluttajista kerättyjä tietoja voitaisiin hyödyntää laajalti tilasto- ja tutkimustarkoituksiin, ja näin ollen kehittää digiyhteiskunnan palveluita entistä paremmiksi ja kannattavimmiksi. Yksityisyydensuojan kannalta käytäntö on toimiva, kunhan edellä mainitun mukaisesti anonymisointi toteutetaan tehokkaasti ja peruuttamattomasti. Todellisuudessa voi kuitenkin olla haastavaa määritellä, onko tieto tehokkaasti anonymisoitu vai onko se edelleen yhdistettävissä tiettyyn yksilöön. (Information Comissioner's Office 2012, 16.) Asiantuntijat ovat esittäneet ajatuksia kansallisesta anonymisointikeskuksesta. Datalla ja kansantaloudella on väistämättä suora kytkös toisiinsa; datamassojen tehokas hyödyntäminen kasvattaisi talouttamme merkittävästi. Nykytila on se, että tietoa viedään Suomesta pois ulkomaisten palveluntarjoajien toimesta. Mikäli Suomi kehittäisi esimerkiksi tiedon anonymisointitaitoja ja mahdollisuuksia, sillä olisi suoraan kansantaloutta piristävä vaikutus (Tietosuojaseminaari 2016).

4.5. Yhteenveto ja johtopäätökset

Nykyaikaiset digitaaliset hyödykkeet, kuten viestintäsovellukset ja pilvipalvelut, tekevät elämästämme helpompaa, mukavampaa ja toisinaan edullisempaa. Palveluita tarjotaan ympäri maailmaa niin kuluttajakäyttäjille kuin yrityskäyttäjille. Pilvipalveluiden eli verkkoyhteyden välityksellä tarjottavien tietojenkäsittely- ja tallennuspalveluiden etuja ovat muun muassa kustannustehokkuus, saatavuus ja käytettävyys. Uudenlaisten teknologioiden tuomien mahdollisuuksien lisäksi niihin liittyy merkittäviä riskejä, jotka saattavat vaarantaa käyttäjien yksityisyydensuojan. Tulosten perusteella riskit voidaan jakaa kahteen näkökulmaan: yhtäältä palveluntarjoajien tietosuojakäytännöt ovat epäselviä tai puutteellisia, ja toisaalta kuluttajien saattaa olla vaikea ymmärtää ja tunnistaa hyödykkeisiin liittyviä riskejä. Keskeisimpiä viestintäsovelluksiin ja pilvipalveluihin liittyviä tietosuojahaasteita ovat avoimuuden puute, liiallinen tietojenkeruu, sopimusehtojen epäselvyys ja tietojen käyttäminen muihin tarkoituksiin kuin palvelun toteuttamiseen. Käyttäjästä kerättyjen henkilötietojen hyödyntäminen esimerkiksi markkinointitarkoituksiin ei ole aina henkilön yksityisyyttä loukkaavaa, mutta se saattaa vaarantua, mikäli käyttäjältä ei pyydetä riittävää suostumusta tai tietojenkäsittelytoimista annettu informaatio on puutteellista.

Yksityisyyden määrittelyyn liittyy eri näkökulmia, joista yksi on tiedollinen itsemääräämisoikeus. Yksityisyydensuoja eli tietosuoja tarkoittaa yksityisyyden suojaamista henkilötietoja käsiteltäessä. Tiedollista itsemääräämisoikeutta on mahdollista toteuttaa tietosuojan avulla, eli se voidaan nähdä myös yksilön mahdollisuutena hallita henkilötietojensa käyttöä. Ihmisten halut ja tarpeet yksityisyytensä suojaamiselle vaihtelevat. Siinä missä yksi on äärimmäisen huolestunut yksityisyydestään, toinen kokee, ettei hänellä ”ole mitään salattavaa”. Tutkimuksen tulokset osoittavat, että palveluntarjoajilta vaaditaan entistä enemmän panoksia tietosuojan varmistamiseen ja osoittamiseen. Mikäli yritykset informoivat asiakkaidensa henkilötietoihin kohdistuvista tietojenkäsittelytoimista avoimesti, läpinäkyvästi ja ymmärrettävästi, kuluttajien luottamus digitaalisia palveluita kohtaan kasvaa. Luottamuksen on nähty olevan yksi digiyhteiskunnan peruspilareista, joka on edellytys markkinoiden tehokkaalle toiminnalle.

Tutkimustulokset vahvistavat aiempien tutkimusten tuloksia siitä, että käyttäjän luottamus palvelua kohtaan kasvaa, mikäli hänelle annetaan mahdollisuuksia hallita tietojaan. Palveluntarjoajat toteuttavat velvollisuuksiaan pääsääntöisesti hyvin, ja käyttäjiä informoidaan heidän oikeuksistaan tietosuojakäytännöissä. Työn keskeinen johtopäätös on, että rekisteröityjen oikeudet toteutuvat useimmissa palveluissa kuitenkin vain näennäisesti. Näennäisyydellä tarkoitetaan sitä, ettei kuluttajilla tosiasiassa ole täyttä kontrollia omista tiedoistaan. Ensinnäkin käyttäjä saattaa joutua antamaan suostumuksensa sellaisille tietojenkäsittelytoimille, jotka ovat ristiriidassa hänen yksityisyydensuojatarpeidensa kanssa. Suostumuksen tulisi olla eksplisiittinen ja vapaaehtoinen, eli käyttäjän tulisi olla mahdollista myös kieltäytyä antamasta suostumusta tai peruuttaa se ilman, että hänelle aiheutuu siitä haittaa. Toiseksi tietojen poistamiseen liittyy haasteita. Vaikka käyttäjälle annetaan mahdollisuus poistaa tietojaan, niiden tehokkaasta ja tosiasiallisesta poistumisesta voi olla vaikea varmistua.

Organisaatioiden tulisi huomioida tietosuojakäytännöissään yksilöihin kohdistuvat tietosuojariskit entistä tehokkaammin. Mikäli henkilötietojen käsittely perustuu suostumukseen, tulisi suostumuksen olla myös tehokkaasti peruutettavissa. Palveluntarjoajien tulisi kiinnittää huomiota myös liialliseen tietojenkeruuseen: on osoitettu, että moni kuluttaja kokee olonsa epämukavaksi, mikäli palvelu pyytää pääsyä kaikkiin hänen tietoihinsa. Mikäli palvelun toteuttamisen kannalta ei ole olennaista saada käyttäjän yhteystietoja tai sijaintitietoja, käyttäjän tulee voida olla suostumatta näiden tietojen antamisesta ilman, että siitä aiheutuu hänelle olennaista haittaa. Moni nykyaikaisista viestintäsovelluksista ja pilvipalveluista on kansainvälinen. Tietojen siirto Suomen tai EU:n ulkopuolelle on paitsi riskialttiimpaa, myös Suomen kansantalouden kannalta epäedullista. Tutkimuksen johtopäätöksenä on, että Suomen potentiaalia digitalisaation hyödyntämiseen voitaisiin hyödyntää esimerkiksi tietosuojanäkökulmasta.

Tutkimuksen tulokset osoittavat, että kuluttajien luottamusta digitaalisiin hyödykkeisiin voidaan lisätä tietojenkäsittelytoimien läpinäkyvyyden lisäksi antamalla heille mahdollisuuksia hallita tietojaan. Nykyisellään rekisteröidyn oikeudet toteutuvat monissa viestintäsovelluksissa ja pilvipalveluissa, mutta tietojen hallintamahdollisuudet ovat usein näennäisiä. Tietosuojakäytännössä tai palvelun käyttöehdoissa tulisi ensinnäkin varmistaa, että suostumuksen laajuus on selvää käyttäjälle. Suostumuksen on oltava myös helposti peruutettavissa. Mikäli suostumuksen peruuttaminen tarkoittaa palvelun poistamista, voidaan sen katsoa aiheuttavan käyttäjälle haittaa, mikä on paitsi tietosuoja-asetuksen vastaista, myös kuluttajan kannalta epäsuotuisa menettely. Käyttäjällä tulisi olla mahdollisuus tarkistaa, mitä tietoja hänestä on kerätty, keillä on pääsy niihin ja ketkä ovat käsitelleet niitä. Tarkastusoikeuden lisäksi käyttäjällä tulisi olla valintamahdollisuuksia: käyttäjä voisi tehdä valintoja esimerkiksi viestintäsovelluksen osalta, mitä tietoja se kerää ja käyttää. Tutkimus osoitti, että käyttäjiä on usein suojeltava heiltä itseltään. Tietosuoja-asetus asettaa vähimmäisvaatimukset hyville tietosuojakäytänteille, ja asetuksen noudattaminen takaa kuluttajille tietyn suojaustason. Organisaatioiden tulisi kuitenkin katsoa asetusta pidemmälle: enää ei riitä pelkkä vaatimustenmukaisuus, vaan tietosuoja tulisi

rakentaa kantavaksi osaksi palvelua. Kuluttajille tulisi antaa aito vapaus valita yksityisyytensä taso nykyaikaisissa viestintäsovelluksissa ja pilvipalveluissa. Näin ollen palveluntarjoajien on jatkossa kiinnitettävä yhä tarkemmin huomiota kuluttajien yksilöllisiin tarpeisiin.

Lähteet

Aïmeur, E., Lawani, O. &– Dalkir, K. (2016). When changing the look of privacy policies affects user trust: An experimental study. *Computers in Human Behavior*, 368–379.

Aljukhadar, M., Senecal, S. &Oullette, D. (2010). Can the media richness of a privacy disclosure enhance outcome? A multifaceted view of trust in rich media environments. *International Journal of Electronic Commerce*, Vol. 14, No. 4, 103–126.

Baun, C., Kunze, M., Nimis, J. & Tai, S. (2011). *Cloud Computing. Web-Based Dynamic IT Services*. Springer, Berlin.

Brown, B. (2001). *Studying the Internet Experience. Publishing Systems and Solutions Laboratory*. Hewlett-Packard Company, HP Laboratories Bristol.

Capistrano, E. P S. & Chen, V. J. (2015). Information privacy policies: The effects of privacy policy characteristics and online experience. *Computer Standards & Interfaces*, 24–31.

Castrén, K. (2015). Viisas johtaja sijoittaa tietosuojaan ja tietoturvaan. Tietosuoja-lehti, 4/2015. <https://www.tietosuoja-lehti.fi/index.php?mid=2&pid=32&aid=3529>, haettu 28.12.2016.

Chandramohan, D., Vengattaraman, T. Rajaguru, D. & Dhavachelvan, P. (2016). A new privacy preserving technique for cloud service user endorsement using multi-agents. *Journal of King Saud University – Computer and Information Sciences*, 28, 37–54.

Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2011). Signaling Theory: A Review and Assessment. *Journal of Management*, Vol. 37 No. 1, 39–67.

Crowe, D., & Al-Hamdani, W. A (2013). *Google Privacy: Something for Nothing?* Information Security Curriculum Development Conference, 27–32.

De George, R. T. (2003). *The Ethics of Information Technology and Business*. Blackwell Publishing Ltd, Cornwall.

Duncan, G. (2014). 7 Ways Your Apps Put You at Risk, and What You Can Do About It. Digital Trends 26.2.2014. http://www.digitaltrends.com/mobile/seven-ways-apps-put-risk-cant-really/ haettu 6.10.2016.

Earp, J. B., Antón, A. I., Aiman-Smith, L. & Stufflebeam, W. H. (2005). Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, 52 (2), 227–237.

Eriksson, P. & Kovalainen, A. (2008). *Qualitative Methods in Business Research*. SAGE Publications, Lontoo.

Eskola, J. & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen*. Vastapaino, Tampere.

ETLA, Elinkeinoelämän tutkimuslaitos (2015) Suomalainen teollinen Internet – haasteesta mahdollisuudeksi. Taustoittava kooste. https://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-42.pdf haettu 6.1.2017.

Euroopan komissio (2015) Eurobarometri. http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_fact_fi_fi.pdf haettu 2.1.2017.

Euroopan unionin neuvosto (2016) Tietosuojauudistus. http://www.consilium.europa.eu/fi/policies/data-protection-reform haettu 15.11.2016.

Gefen, D., Karahanna, E. & Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. *MIS Quarterly*, Vol. 27, No. 1, 51–90.

Geng, J., Liu, L. & Bryant, B. R. (2010). *Towards a Personalized Privacy Management Framework*. SESS'10, 58–64.

Google (2016) Tietosuojakäytäntö. https://www.google.fi/intl/fi/policies/privacy/ haettu 1.12.2016.

Helsingin Sanomat (2016) *Korispomo Aleksi Valavuori sai potkut Espoo Unitedista – syynä seksuaalivähemmistöjä halventaneet tviitit.* Julkaistu: 26.10.2016. http://www.hs.fi/urheilu/art-2000002927207.html haettu 29.12.2016.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2004). *Tutki ja kirjoita*. Gummerus, Jyväskylä.

Hirschprung, R., Toch, E., Bolton, F. & Maimon, O. (2016). A methodology for estimating the value of privacy in information disclosure systems. *Computers in Human Behavior*, 443–453.

Hoffman, D. L., Novak, T. P. & Peralta, M. (1999). Building consumer trust online. Communications of the ACM, Vol. 42, No. 4.

Information Comissioner's Office (2012) *Anonymisation: managing data protection risk code of practice*. https://ico.org.uk/media/1061/anonymisation-code.pdf haettu 22.9.2016.

ITIL-sanasto ja lyhenteet, Suomenkielinen. (2001) https://www.exin.com/assets/exin/frameworks/108/glossaries/finnish_glossary_v1.0_201404.pdf haettu 19.6.2016.

Kirmani, A. & Rao, A. R. (2000). No pain, no gain: A critical review of the literature on signaling unobservable product quality. *Journal of Marketing*, vol. 64, no. 2, 66–79.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 122–134.

Korhonen, R. (2003). *Perusrekisterit ja tietosuoja*. Edita Publishing Oy. http://www.edilex.fi/kirjat/1126.pdf haettu 9.4.2015.

Koskinen, I., Alasuutari, P. & Peltonen, T. (2005). *Laadulliset menetelmät kauppatieteissä*. Vastapaino, Tampere.

Kowalewski, S., Ziefle, M., Ziegeldorf, H. & Wehrle, K.s (2015). Like us on Facebook! – Analyzing user preferences regarding privacy settings in Germany. *Procedia Manufacturing*, 815–822.

KPMG International (2016) *Crossing the line: Staying on the right side of consumer privacy*. https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/11/crossing-the-line.pdf haettu 1.12.2016.

Kunelius, Ri. (1998). *Viestinnän vallassa – Johdatus joukkoviestinnän kysymyksiin*. WSOY, Juva.

Kuo, F.-Y., Lin, C. S. & Hsu, M.-H. (2007). Assessing Gender Differences in Computer Professionals' Self-Regulatory Efficacy Concerning Information Privacy Practices. *Journal of Business Ethics*, 145–160.

Kyberturvallisuuskeskus (2014). Ohje 5/2014 Pilvipalvelujen turvallisuus. https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf haettu 30.8.2016.

Laaksonen, M., Nevasalo, T. & Tomula, K. (2006). *Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö*. Edita Publishing Oy. Helsinki.

Lacity, M. C., Khan, S. A., Yan, A. & Willcocks, L. P. (2010). A review of the IT outsourcing empirical literature and future research directions. *Journal of Information Technology*, Vol. 25, Issue 4, 395–433.

Malmelin, N. & Hakala, J. (2005.) *Yhdessä – Viestinnän ja markkinoinnin integraatio*. Gummerus Kirjapaino Oy Jyväskylä.

Martin, K. E. (2012). Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract. *Journal of Business Ethics*, 519–539.

Martin, K. E. (2016). Understanding Privacy Online: Development of a Social Contract Approach to Privacy. *Journal of Business Ethics*, 551–569.

Mell, P. & Grance, T. (2011). *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology, U.S. Department of Commerce*. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf haettu 19.10.2016.

Michota, A. & Katsikas, S. (2015). Designing a Seamless Privacy Policy for Social Networks. *PCI 2015*, 139–143.

Neilimo, K. & Näsi, J. (1980). *Nomoteettinen tutkimusote ja suomalainen yrityksen taloustiede. Tutkimus positivismin soveltamisesta.* Yrityksen taloustieteen ja yksityisoikeuden laitoksen julkaisuja, sarja A2: Tutkielmia ja raportteja. Tampereen yliopisto, Tampere.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus, the Journal of the American Academy of Arts & Sciences*, 32–48.

OECD (2013). *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*. OECD Digital Economy Papers, No. 220, OECD Publishing, Paris. http://www.oecd-ilibrary.org/docserver/download/5k486qtxldmq-en.pdf?expires=1480349020&id=id&accname=guest&checksum=010ED5A2A680DC245CE2B8535FA66FBB haettu 28.11.2016.

Paananen, J. (2005). *Tietotekniikan peruskirja*. WS Bookwell, Porvoo.

Pentina, I., Zhang, L., Bata, H. & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, 409–419.

Pitkänen, O., Tiilikka, P. & Warma, E. (2013). *Henkilötietojen suoja*. Talentum, Helsinki.

Pohjonen, R. (2002). *Tietojärjestelmien kehittäminen*. Docendo Finland Oy, Jyväskylä.

Pollach, I. (2005). A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent. *Journal of Business Ethics*, 221–235.

Ramachandran, M. & Chang, V. (2016). Towards performance evaluation of cloud service providers for cloud data security. International *Journal of Information Management*, Vol. 36, Issue 4, 618–625.

Ricker, B., Schuurman, N., & Kessler, F. (2015). Implications of smartphone usage on privacy and spatial cognition: academic literature and public perceptions. *GeoJournal*, 637–652.

Salste, T. (2000). *Digitaalisten tuotteiden menestymisen edellytykset Internetissä: toimialatarkastelu: valmisohjelmistot ja musiikkiäänitteet*. Markkinoinnin pro gradu -tutkielma, Helsingin kauppakorkeakoulu.

Schoeman, D. (1984). *Philosophical Dimensions of Privacy: An Anthology*. Cambridge University Press, Cambridge, UK.

Simitis, S. (2010) Privacy – An Endless Debate. *California Law Review*, Vol. 98, Issue 6, 1989–2006.

Smith, H., Milberg, S. & Burke, S. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, Vol. 20, 167–196.

Spence, M. (2002). Signaling in Retrospect and the Informational Structure of Markets. *American Economic Review*, 92, 434–459.

Spiekermann, S., Grossklags, J. & Berendt, B. (2001). E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. *Proceedings of the 3rd ACM conference on Electronic Commerce*, 38–47.

Liikenne- ja viestintäministeriö (2016). Suomen tietoturvallisuustrategia – maailman luotetuinta digitaalista toimintaa. Liikenne- ja viestintäministeriön julkaisuja, Helsinki.

Suomen virallinen tilasto (SVT) (2015). *Internetin käyttö mobiilia, laitteet henkilökohtaisia*. Väestön tieto- ja viestintätekniikan käyttö [verkkojulkaisu]. Tilastokeskus, Helsinki. http://www.stat.fi/til/sutivi/2015/sutivi_2015_2015-11-26_tie_001_fi.html haettu 7.9.2016.

Svantesson, D. & Clarke, R. (2010). Privacy and consumer risks in cloud computing. *Computer law and security review*, 26 (4), 391–397.

Tiainen, T., Luomala, H., Kurki, S. & Mäkelä, K. (2004). *Luottamus sähköisissä palveluissa – kuluttajan ja palvelun tarjoajan vuorovaikutus*. Tampereen yliopisto.

Tietosuojatyöryhmä (2014). Lausunto 5/2014 anonymisointitekniikoista. (0829/14/FI) WP 216, annettu 10.4.2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fi.pdf haettu 22.9.2016.

Tietosuojavaltuutetun toimisto (2014). *Käyttötarkoituksen määrittely ja käsittelyn suunnittelu*. http://www.tietosuoja.fi/fi/index/rekisterinpitajalle/kayttotarkoituksenmaarittelyjakasittelynsuunnittelu.html haettu 15.10.2016.

Tuominen, P. (2014). *Digitalisaatio tulee kuin talvi Suomeen – varmasti, mutta "yllätyksenä*". Market-Visio Oy. http://www.marketvisio.fi/fi/ajankohtaista/blogi/1926-digitalisaatio-tulee-kuin-talvi-suomeen-varmasti-mutta-yllatyksena haettu 6.1.2017.

Valtiovarainministeriö (2016). *EU-tietosuojan kokonaisuudistus*. VAHTI-raportti 1/2016. https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128 haettu 10.12.2016.

Voutilainen, T. (2012). *Julkisuus ja tietosuoja viranomaistoiminnassa*. Oikeustieteiden laitos, Itä-Suomen yliopisto. http://wanda.uef.fi/oikeustieteet/netti11-12/Jutivi.pdf haettu 19.6.2016.

Warren, S. D. & Brandeis, L. D. (1890). *The Right to Privacy*. Harvard Law Review, Vol. IV, No. 5. http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html haettu 19.12.2016.

WhatsApp (2016a). WhatsApp Privacy Policy. https://www.whatsapp.com/legal/?l=fi haettu 1.12.2016.

WhatsApp (2016b). Tietoja WhatsAppista. https://www.whatsapp.com/about/ haettu 28.12.2016.

Wolf, C. (2012). Privacy and data security in the cloud: What are the issues? *The IP Litigator: Devoted to Intellectual Property Litigation and Enforcement*, 18(6), 19–28.

Youseff, L., Butrico, M. & Da Silva, D. (2008). *Toward a Unified Ontology of Cloud Computing.* In Procedure of Grid Computing Environments Workshop, (GCE08). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.176.3634&rep=rep1&type=pdf haettu 19.10.2016.

LUKU 5.

LIIKETOIMINTAA AVOIMILLA RAJAPINNOILLA JA AVOIMELLA DATALLA

Koskinen Jani

Suomi Reima

5.1. Avoin data

Mikä tahansa data, ja varsinkin mikä tahansa avoin data, on digitaalista raaka-ainetta, joka on uusiutuvaa ja lähes rajattomasti jaettavissa. Tässä on myös syy, miksi sen käyttö on ekologisesti perusteltua verrattuna keskittymiseen pelkästään fyysisiin raaka-aineisiin ja tuotteisiin[10]. Avointa dataa voidaan kutsua digitaalisen vallankumouksen polttoaineeksi – vallankumouksen, jonka merkitystä olemme vasta alkamassa ymmärtää, kuten oli tilanne myös muissa teollistumisen vallankumouksissa.

Kun puhutaan datasta, jota voidaan jakaa avointen rajapintojen kautta, on hyvä tarkentaa, mitä näillä termeillä tarkoitetaan ja mitä ne sisältävät. Näin terminologiasta kumpuavat väärinkäsitykset voidaan paremmin välttää. On selvää, että tässä raportissa kyseessä on siis digitaalinen data. On kuitenkin tärkeää huomioida, että data on vain yksi tiedon muodoista. Suomen kielessä tieto kuvaa useita asioita, joille esimerkiksi englannin kielessä on vastineena useampia sanoja. Selvennämme datan eroa muusta tiedosta esittelemällä tunnetun ja yleisesti käytetyn tiedon jaon mallin; DIKW-hierarkian. DIKW-hierarkiassa tieto jaetaan neljään eri tasoon: dataan, informaation, tietämykseen ja viisauteen (Rowley 2007). Keskeistä mallissa on se, että mitä korkeammalle hierarkiassa edetään, sitä enemmän sisältöä ja tulkintaa tarkasteltavaan tietoon on upotettu. Esimerkkinä tästä hierarkiasta voidaan esittää raaka ilmanpainedata paikkaan sidottuna (data) ja sen pohjalta muodostettu meteorologinen ennuste (informaatio/tietämys). Tämä vertailu tuo hyvin esiin datan ja siitä johdetun informaation tai tietämyksen eron.

Avoin data on dataa, jota voi vapaasti käyttää ja käyttää uudelleen ja jota kuka tahansa voi jakaa. Kattavampi määritelmä löytyy esimerkiksi Open Knowledge Internationilta (2016), joka kiteyttää sen kolmeen osa-alueeseen seuraavasti:

Saatavuus ja oikeus käyttää dataa: Datan tulee olla saatavilla kokonaan, ja siitä voidaan periä vain kohtuullinen, datan tuottamisen kustannuksiin perustuva maksu. Datan tulee ensisijaisesti olla helposti saatavissa verkosta, ja sen tulee olla muokkaukseen soveltuvassa muodossa.

10 Edellyttäen, että datan käyttö ei lisää fyysisten raaka-aineiden käyttöä. Lisäksi tulee huomioida, että itse informaatioteknologian käyttö ja valmistaminen kuluttavat energiaa ja raaka-aineita. Tuleekin siis huolehtia, että rasitus ympäristölle pysyy hallinnassa nyt ja tulevaisuudessa.

Datan uudelleenkäyttö ja jakaminen: Datan jakamisen ehtojen tulee mahdollistaa datan uudelleenkäyttö ja eteenpäin jakaminen ja sen yhdistäminen muihin tiedostoihin/aineistoihin.

Universaali oikeus dataan: Kaikilla tulee olla mahdollisuus käyttää, käyttää uudelleen ja jakaa dataa – minkäänlaista diskriminaatiota ei tule kohdistaa käyttöä tai käyttäjiä kohtaan. Esimerkiksi datan käytön rajoittaminen kieltämällä sen käyttö ”ei-kaupallisiin tarkoituksiin” tai vastaavilla muilla rajoituksilla ei ole sallittua.

Avoimessa datassa on useita yhtymäkohtia avoimen lähdekoodin (open source) käsitteeseen. Käsitteet avoin ja ilmainen sekoitetaan usein. Avoin ei välttämättä tarkoita ilmaista, ja viime kädessä ”ilmaisia lounaita” ei ole, kuten kaikki tietävät. Avoimen (=näennäisesti ilmaisen) datan etsiminen, haltuunotto ja hyödyntäminen ovat kaikki työintensiivisiä vaiheita, jotka vaativat resursseja ja aiheuttavat kustannuksia. Aivan kuten avoimen lähdekoodinkin kohdalla, avoin data voi olla ilmaista, mutta sen käyttöön liittyy usein vaikeuksia, joita varten tarvitaan konsulttipalveluita, konsultointia ja neuvontaa. Nämä on usein hinnoiteltu melko raskaasti, sillä ajatuksena on samalla kattaa ”ilmaiseen” hyödykkeeseen – dataan tai lähdekoodiin – upotettu työkustannus.

Avointa dataa voi tuottaa kuka tahansa. Dataa tuotetaan usein tarkoituksellisesti, tai sitten sitä syntyy tavallaan luonnostaan (engl. *naturally occurring data*). Termi on sikäli harhaanjohtava, että on toki tarvittu jonkinlainen järjestelmä datan hallinnoimiseen, vaikka järjestelmän alkuperäinen tarkoitus ei kuitenkaan ole ollut datan tuottaminen. Sosiaalinen media on hyvä esimerkki luonnostaan syntyvästä datasta. Sosiaalisen median alkuperäinen funktio on ihmisten välinen kommunikaatio, mutta samalla syntyy suuri määrä dataa. Sosiaalisen median tuottama transaktiodata on sisällöllisesti mielenkiintoista ja muodoltaan rikasta, mutta vähemmän mielenkiintoista transaktiodataa kertyy jatkuvasti miljoonista tapahtumankäsittelyjärjestelmistä ympäri maailmaa. Maailman suurimmaksi tietovarastoksi on luonnehdittu Facebookin tietokantaa Social Graph (Ugander, Karrer, Backstrom & Marlow 2011).

Avoin data ei tarkoita pelkästään rakenteellista tietoa, kuten sosiaalisen median esimerkit osoittavat. Myös rakenteeton data voi olla avointa. Esim. Wikipedia, Pinterest ja Youtube ovat esimerkkejä avoimesta rakenteettomasta datasta. Niissä kaikissa avoimen datan tarjoaminen on ydinliiketoimintaa.

Suomalaisessa ajattelutavassa lähdetään siitä, että viranomaisten ja julkisen hallinnon tulee avata tietovarantojaan julkiseen, avoimeen käyttöön. Tämä on luontevaa, koska tieto on julkisin varoin tuotettua. Myös tieteellisessä työssä tiedon avoimuutta edellytetään nykyisin hyvin voimakkaasti, kuten esim. Suomen Akatemian ja EU:n tutkimusrahoitusehdot osoittavat. Myös yksityiset toimijat voivat kuitenkin tuottaa avointa dataa, ja usein avoin data on koko liikeidean ydin, kuten Youtube ja Wikipedia osoittavat.

Jokainen kansalainen voi tietenkin halutessaan julkaista omistamansa datan, mutta harvoin yksilöillä on merkittäviä tietovarantoja. Yksilöiden panos tulee keskiöön käsitteen joukkouttaminen eli crowdsourcing myötä. Suuret joukot pystyvät tuottamaan suuren määrän dataa yhteisellä panostuksella, mutta ohjatussa ympäristössä (kuten esim. Wikipedia). Kun tieto on tuotettu yhteisesti ja korvauksetta, sen avoimuus kaikille on myös luonnollinen lähtökohta. Aina näin ei tietenkään tapahdu, vaan joukkouttamalla tuotettu data saattaa päätyä suljetuksi dataksi.

5.2. Avoimet rajapinnat

Viime vuosikymmenen aikana avoimen datan ja samalla avoimien rajapintojen määrä on kääntynyt jyrkkään kasvuun Internetin käytön ja laajenemisen myötä. Avoimet rajapinnat ovat keskeinen osa nykytilaa ja tulevaisuuden murrosta, jossa asiat ja esineet ovat kasvavassa määrin liittymässä osaksi Internetiä. Tätä tulevaa ilmiötä kutsutaan termillä esineiden Internet (engl. *Internet of Things/ IoT*).[11]

Avoimista rajapinnoista puhutettaessa ongelmana on kuitenkin termin yleisyys ja monitulkintaisuus. Rajapinnalla tarkoitetaan tietokoneohjelman osaa, joka vastaa tiedon siirrosta eri ohjelmien tai ohjelmien osien välillä. Rajapinnalla määritellään siirrettävän tiedon tyypit ja tarpeelliset toiminnallisuudet, jotta tiedon siirto on mahdollista. Kaikki verkkoliikenne perustuukin rajapintoihin[12], joiden avulla tiedon siirto Internetissä tai missä tahansa muussa tietoverkossa on mahdollista.

Tässä raportissa avoimista rajapinnoista puhutettaessa tarkoitetaan rajapintoja, jotka toteuttavat seuraavat ehdot:

- Ovat avoimia ja näin ollen kaikkien saatavilla ilman erillistä korvausta tai lupaprosessia.
- Ovat avoimesti dokumentoituja. Tämä tarkoittaa, että dokumentaatio on vapaasti saatavilla ja että se kuvaa rajapintaa riittävällä tarkkuudella.
- Rajapinta on käytettävissä, eli sen kautta on saatavilla tietoa. Rajapinnalla pitää olla saatavilla jotain informaatiota sitä pyydettäessä. Vähimmillään tämä tarkoittaa, että tarjolla on dataa, jolla toiminnollisuuksia voidaan kokeilla (tiedon tarjoaminen vapaasti rajapinnan kautta ei ole välttämätöntä, vaikka itse rajapinta olisikin avoin).

Avoimuus rajapinnoissa on pitkälti saavuttamaton haave, samoin kuin ajatus avoimesta datasta. Vaikka rajapinnat ovat periaatteessa avoimia, monet käytännön seikat rajoittavat niiden avointa käyttöä. Rajapintojen käytännön hallintaan saatetaan tarvita kalliita ohjelma- tai laiteratkaisuja, joihin kaikilla potentiaalisilla tiedon käyttäjillä ei ole varaa. Rajapinnat ovat periaatteessa avoimesti dokumentoituja, mutta käytännössä rajapintoja kuvaavat dokumentit ovat maksullisia. Tästä ovat esimerkkinä kansainväliset standardit, joihin ei suinkaan yleensä pääse vapaasti käsiksi, vaan jotka pitää ostaa maksullisina suoritteina erilaisilta standardiorganisaatioilta. Kuten avoimen lähdekoodinkin kohdalla, avoimen rajapinnan käyttö saattaa käytännössä edellyttää kalliiden konsultointi- ja koulutuspalveluiden ostamista.

Koko digitaalinen tiedonsiirto perustuu rajapintoihin ja erilaisiin protokolliin niiden käytössä. Samaan aikaan haasteiksi nousevat määrän kasvun mukana rajapintojen löytäminen, eri rajapintastandardien erot, luotettavuus rajapintojen kautta saatavaan ja kulkevaan tietoon sekä tietoturvan korostuminen. Onkin tärkeää löytää keskeiset tekijät ja toimintatavat, joiden avulla voidaan

- edistää avoimien rajapintojen tarjontaa ja käyttöä sekä niiden yhdistämistä/hyödyntämistä liiketoiminnan näkökulmasta
- edistää julkisen hallinnon toimintaa uusien julkisten palvelujen luonnissa
- tukea liiketoimintaa tarjoamalla julkisen sektorin tuottamaa tietoa rajapintojen kautta

11 Internet of Things (IoT) / Esineiden (asioiden) Internet / Teollinen Internet kuvaa tilannetta, jossa esineet, ohjelmistot, palvelut ja jopa mahdollisesti ihmiset ovat liittyneet Internetiin ja ovat reaaliaikaisesti saavutettavissa

12 Internetin toiminta perustuu verkkoprotokolliin ja niiden rajapintoihin, joiden kautta tiedon siirto tapahtuu.

- tukea avointen rajapintojen kautta saatavan tiedon luotettavuutta ja eettisesti kestävää käyttöä.

Avoimien rajapintojen kautta tarjotaan dataa tai parhaimmillaan informaatiota. Yrityksen tai muun sitä käyttävän organisaation pitää pystyä luomaan lisäarvoa asiakkaille, ja tämä lisäarvon luominen on liiketoimintamallien ydin ja edellytys. Siirtyminen korkeampaan tiedon muotoon (data→ informaatio → tietämys → viisaus) on se tilanne, missä yrityksen luoma arvonlisä usein tapahtuu, erityisesti digitaalisesta liiketoiminnasta tai digitaalisten hyödykkeiden luomisesta puhuttaessa.

Avoimen datan ja avoimien rajapintojen käyttömahdollisuudet

Aidosti avoimen datan tulevaa käyttöä on vaikea kontrolloida ja ennakoida. Vahvan kontrollin ei pitäisi olla lähtökohta avoimen datan kohdalla, koska avoimen datan ideana on nimenomaan avoimuus ja vapaus sen käyttöön tulisi olla ohjenuorana kun päätetään tiedon avaamisesta Suomessa. Vastaavasti suomalaisilla toimijoilla on käytännön mahdollisuus hyödyntää kansainvälistä ja ulkomaalaista avointa dataa.

Huijboom & Van den Broek (2011) luokittelevat eri maiden syyt avoimen datan jakamiseen kolmeen ryhmään:

- lainkäyttö, tavoitellaan poliisitoiminnan ja lainkäytön vahvistamista
- demokraattinen vaikuttaminen, kansalaisten demokraattisen kontrollin ja vaikuttamisen tehostaminen
- palvelutuotanto, palvelu- ja tuoteinnovaatiot.

Suomessa painopiste avoimen datan tavoitteissa lienee vahvasti ollut innovaatioissa, ja tämäkin raportti on tehty pitkälti kyseinen tavoite mielessä. Muitakaan näkökulmia ei pidä laiminlyödä. Huijboomin ym. (2011) selvityksen mukaan esim. Yhdysvalloissa demokraattinen vaikuttaminen on Eurooppaa selkeämmin esillä.

Saman Huijboom ym. (2011) selvityksen mukaan valtiot voivat edistää avoimen datan käyttöä neljällä eri tavalla:

- koulutus ja valmennus
- vapaaehtoisuuteen perustuvat kannustimet
- taloudelliset instrumentit
- lainsäädäntö ja kontrolli.

Artikkelissa esitetyn analyysin mukaan kaikki valtiot käyttävät näitä keinoja varsin täysipainoisesti. Yksityiskohtana voitaneen mainita, että artikkelin mukaan Isossa-Britanniassa ja Yhdysvalloissa painottuvat taloudelliset instrumentit, kun taas esim. Tanskassa koulutus ja valmennus. Tutkiessaan viranomaisten avoimen datan strategioita lähinnä Hollannissa Janssen ym. (2012) päätyivät johtopäätökseen, että viranomaisten tulisi oppia paljon nykyistä enemmän toistensa parhaista käytännöistä.

Janssen ym. (2012) identifioivat avoimen datan käyttöön liittyen viisi myyttiä:

- Tiedon julkaiseminen tuottaa automaattisesti hyötyjä.
- Kaikki tieto pitäisi saattaa rajoittamattomasti saataville.
- Kyseessä on yksikertaisesti julkisen datan avoimeksi saattaminen.

- Kuka tahansa voi hyödyntää avointa dataa.
- Avoin data johtaa avoimeen hallintoon.

Tässä raportissa keskitytään julkisen sektorin tarjoamiin avoimiin rajapintoihin ja niiden kautta tarjottavaan avoimeen julkiseen dataan sekä tämän datan tarjonnasta syntyvään liiketoimintaa mahdollistavaan vaikutukseen. Kuten edellä olevan johdannon oli tarkoitus tuoda esille, tämä on kuitenkin vain yksi ja erittäin rajallinen näkökulma avoimeen dataan.

Pelkästään se, että tarjotaan saataville avoin rajapinta, ei riitä varmistamaan uuden ja kannattavan liiketoiminnan syntyä. Uuden liiketoiminnan tukemiseen tarvitaan myös muita toimenpiteitä, jotka tukevat uuden liiketoiminnan syntymistä suuressa mittakaavassa. Keskeisenä tekijänä tässä on ekosysteemiajattelu, kun puhutaan menestystarinoista digitaalisessa liiketoiminnassa.

5.3. Avoin data ja sen hyödyntämisen haasteet julkisella sektorilla

Kun avoin data ja sen hyödyntäminen aloitettiin viime vuosikymmenen lopulla Yhdysvalloissa ja myös muualla, tavoitteena oli avoimuuden lisääminen ja uusien toimintatapojen aikaansaaminen julkisella sektorilla. Avoimen datan hyödyntäminen jäi Yhdysvalloissa nopeasti kaupunkien toteutettavaksi, ja sama kehitys on ollut trendinä myös Euroopassa (Lee, Almirall & Wareham 2015). Esimerkkeinä tästä ovat Barcelona, Manchester, Amsterdam ja Helsinki (Ojo, Curry & Zeleti, 2015). Yhdysvalloissa huomattiin, että ensimmäisen sukupolven avoimen datan kokeilut eivät vastanneet odotuksia ja että niiden tulokset jäivät varsin vaatimattomiksi ja tuotetut sovellukset usein lyhytikäisiksi.

Avoimen datan ensimmäinen ”aalto” perustui yleensä kilpailuihin, joihin kehittäjillä oli mahdollisuus osallistua. Lee ym. (2015) listasivat kahdeksan asiaa, jotka menivät pieleen avoimen datan eteenpäin viemisessä sen ensimmäisessä ”aallossa:

- Suosittujen datasettien ylenpalttinen käyttö.
- Samoihin tarpeisiin vastaavien sovellusten liian suuri määrä.
- Sovelluksia kehittäjiltä, joiden intressit ja taustat olivat liian samanlaiset.
- Data avattiin muuttamatta mitään organisaation toiminnassa – organisaatiot olivat passiivisia.
- Olemassa olevien sovellusten käyttö, joita oli vain muokattu kilpailua varten.
- Rahalliset palkinnot olivat symbolisia, eivätkä ne mahdollistaneet pitkäaikaista kehittämistä.
- Rajoitettu omaksuminen ja tuki julkiselta hallinnolta, kaupunkien osallistuminen jäi datan julkaisuun.
- Datan läpinäkyvyyden vastustus julkisen hallinnon puolelta.

Lee ym. (2015) kuitenkin huomasivat, että virheistä oli opittu ja seuraavan sukupolven avoimen datan hyötykäytössä oli edistytty. Jotta avoimen datan käyttö sovelluksissa onnistuu ja niistä saadaan oikeaa, pysyvää toimintaa, seuraavien asioiden oli huomattu olevan tärkeitä:

- Yrittäjät ja pääomasijoittajat kutsuttiin mukaan paneeleihin, ja näin kehittäjille saatiin näkyvyyttä rahoittajien suuntaan.
- Kunnalliset toimijat pakotettiin säädöksillä avaamaan dataa riittävän nopeasti.

- Kaupungit ilmoittivat julkisesti kohtaamistaan operationaalista ongelmista kehittäjien huomion ohjaamiseksi niihin.
- Kehittäjiä sitoutettiin määräajaksi osaksi kaupunkien organisaatioita, jotta nämä saisivat riittävän ymmärryksen toiminnasta ja molemminpuolinen sitoutuminen vahvistuisi.
- Tarvitaan vahvempaa johtamista ja suoraa koordinaatioita kaupungin taholta.
- Sitoutumista tukemaan tarvitaan sovellusten kehittämistä myös rahallisesti.
- Kannattaa käyttää yleisesti käytössä olevia sovelluksia ja alustoja, jos mahdollista, eikä aina uutta omaa sovellusta (monesti tarve ei ole niin yksilöllinen kuin julkisella sektorilla luullaan, vaan löytyy jo valmis tai nopeasti räätälöitävä versio, joka täyttää oikeat tarpeet).
- Avoimen lähdekoodin lähestymistapa ja tiedon standardointi.

Edellä mainittujen asioiden lisäksi Lee ym. (2015) toteavat, että kolme ongelmaa sailyy, vaikka edellä mainittuihin asioihin kiinnitetään huomiota. Ensinnäkin sovellusmarkkinoiden yleinen käyttömaksuihin tai mainostuloihin perustuva rahoitusmalli ei ole mahdollinen julkisen sektorin palveluissa, mikä pakottaa ne panostamaan vaihtoehtoiseen arvonmuodostukseen. Toiseksi luottamus, vakaus ja jatkuvuus ovat edellytys avoimelle datalle ja sen pohjalle rakennetuille palveluille. Tämä ei ole aina varmaa turbulentissa kunnallisessa politiikassa (Huijboom ym. 2011). Kolmanneksi luontainen ero julkisen sektorin ja sovellustoteuttajien toimintatapojen välillä aiheuttaa haasteita johtamiselle näissä monimutkaisissa ja erilaisissa ekosysteemeissä (Lee ym. 2015).

5.4. Tyypilliset liiketoimintamallit digitaalisille hyödykkeille ja palveluille

Liiketoimintamalli

Liiketoimintamalli kuvaa tapaa, jolla yritys generoi liikevaihtoa ja voittoa liiketoiminnasta (Investopedia 2016). Wikipediassa (2016) liiketoimintamalli määritellään seuraavasti: ”**Liiketoimintamalli** on kuvaus keskeisistä liiketoiminnan menestystekijöitä sekä niiden välisistä riippuvuussuhteista, joilla arvoa luodaan asiakkaille”. Tyypillisesti kuvataan seuraavat asiat:

- tuotteiden, palvelujen ja informaation virtojen arkkitehtuuri
- asiakkaan lisäarvon määritys
- myyjän ansaintalogiikka.

DaSilva ja Trkman (2014) korostavat, että liiketoimintamalli on yrityksen strategian nykyhetkessä toteuttamaa toimintaa organisaation voimavaroja (engl. *dynamic capabilities*) hyödyntämällä, vaikka sitä on tulkittu eri tavoin niin akateemisessa tutkimuksessa kuin liiketoiminnassa. On siis tärkeää ymmärtää, miten se eroaa strategiasta ja muista malleista. Liiketoimintamalli on strategian nykyhetkessä toimiva tapa tehdä liiketoimintaa, ja sitä tulisi koko ajan peilata organisaation strategiaan ja haasteisiin, joita kilpailu aiheuttaa. Surullisena esimerkkinä on pitkään toiminut Nokian entinen liiketoimintamalli, jossa tuotettiin puhelimia ylivertaisen tehokkaasti. Johtavasta asemastaan huolimatta koko Nokian puhelintuotanto loppui vajaassa kymmenessä vuodessa. Entinen liiketoimintamalli ei enää ollutkaan elinkelpoinen uusien kilpailijoiden tullessa markkinoille. Nokia ei pystynyt vastaamaan kilpailuympäristön muutokseen ja kuluttajien tarpeita ei enää pystytty tyydyttämään.

Tammisto ja Lindman (2012) summaavat julkisen sektorin syyt osallistua avointa dataa käsittelevään liiketoimintaan (taulukko 6). He jakavat avoimen datan käytön sisäiseen ja ulkoiseen (asiakkaille tuotettavat palvelut) käyttöön.

Taulukko 6: Syyt osallistua avoimen datan liiketoimintaan (Tammisto & Lindman 2012, 300).

Tavoitteet sisäisen avoimen datan hyödyntämiselle	Tavoitteet ulkoisen avoimen datan hyödyntämiselle	Yhteistä
Lisää tuotosten ja varantojen näkyvyyttä	Lisää läpinäkyvyyttä	Tehosta kommunikointia
Muuta organisaation rakenteita	Ilmaise organisaation identiteettiä	
Muuta julkista taloutta	Hyödy useiden eri datasettien yhdistämisestä	Tehosta päätöksentekoa
Kaupallinen käyttö	Mahdollista ulkoinen kontribuutio palvelujen tuottamiseen ja toteuttamiseen	Kehitä ja tuota uusia palveluita
	Edistä taloutta	Tuota taloudellista arvoa

Avointa dataa hyödynnetään usein julkisen sektorin ja yritystoiminnan kumppanuuksissa (PPP, Public Private Partnership) (Roll & Verbeke 1998). Myös avoimen datan kohdalla on kiinnitettävä erityistä huomiota näiden kahden eri toimijaryhmän liiketoimintamallien eroon. Yksityisten yritysten tehtävänä jo osakeyhtiölain mukaan on tehdä voittoa, kun taas julkisen sektorin liiketoimintamalli on vähemmän selkeästi artikuloitu, mutta usein julkinen toimija pyrkii tyydyttävän (sovitun) tasoisten palveluiden mahdollisimman tehokkaaseen tuottamiseen. Avoimen datan hyödyntämisen yhteydessä on erityisesti panostettava keskusteluihin ja yhteisymmärrykseen siitä, miten nämä kaksi erilaista liiketoimintamallia voidaan integroida samaan palveluketjuun, ja miten järjestelystä saadaan kansalaisille riittävän läpinäkyvä ja luottamusta herättävä.

Ekosysteemi

Yksikään toimintayksikkö tai yritys ei kykene toimimaan ilman sen toimintaa tukevaa ekosysteemiä. Ekosysteemiajattelu on lähtöisin biologiasta, mutta myös taloudelliset ja sosiaaliset systeemit ymmärretään yhä useammin ekosysteemeinä.

Systeemiajattelu voidaan jakaa perinteiseen ”kovaan” ja modernimpaan ”pehmeään” systeemiajatteluun. Kovassa systeemiajattelussa systeemit toimivat konemaisesti, säännönmukaisesti ja ilman poikkeamia ja yllätyksiä. Pehmeässä systeemiajattelussa korostuu epävarmuus, häiriöt toiminnassa sekä se, että välttämättä ei oleteta, että koko systeemin toiminta ymmärretään. Kun puhutaan ekosysteemeistä, viitataan juuri pehmeään systeemiajatteluun. Kova systeemiajattelu tulkitsee teknisiä systeemeitä, pehmeä systeemiajattelu sosioteknisiä systeemeitä.

Ekosysteemiajattelu sopii hyvin avoimeen dataan ja avoimiin rajapintoihin perustuvaan liiketoimintaan. Kokonaissysteemi on hahmottumaton, eikä kaikkia sen osallistujia tunneta, näiden välisistä vuorovaikutussuhteista puhumattakaan.

Ekosysteemissä periaatteessa kaikki osallistujat ovat yhtä arvokkaita ja tärkeitä. Silti ekosysteemeissäkin asioita tarkastellaan usein jonkin keskeisen toimijan kannalta. Keskeisessä asemassa ekosysteemitarkastelussa on yleensä ihminen tai jokin ihmiselle (taloudellisesti) arvokas kohde, kuten viljelykasvi tai eläin. Avoimen datan markkinoillakin on keskeisiä toimijoita ja

ekosysteemissä marginaalisemman aseman ottavia tahoja. Maailmanlaajuisesti keskeisiä toimijoita (myös avoimen) datan ekosysteemeissä ovat suuret tietojenkäsittelyalan jätit, kuten Google, Apple tai Microsoft. Kun ajatellaan julkisten toimijoiden tuottaman datan ympärille rakennettua ekosysteemiä, on kyseinen julkinen taho, esim. ministeriö tai muu julkinen laitos, luonnollisesti ekosysteemitarkastelun ytimessä.

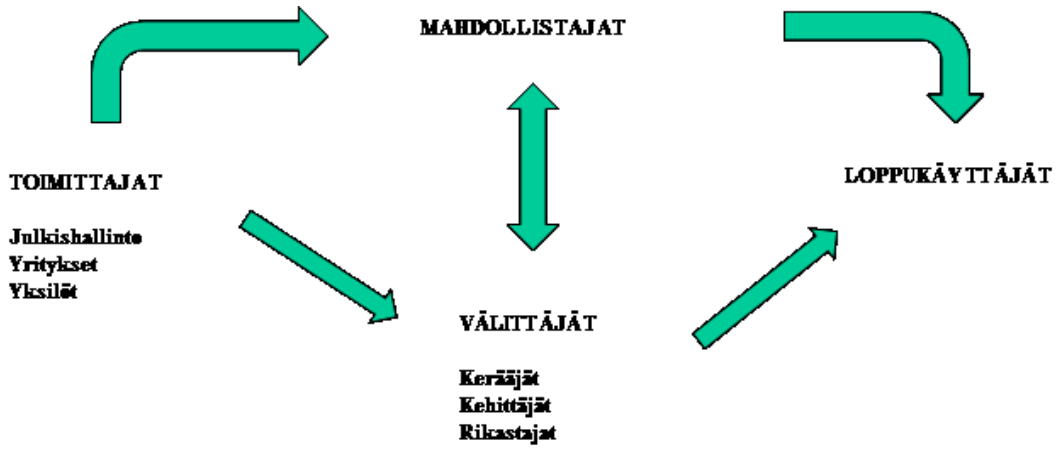
Tiedon jakaminen liiketoimintamallina

Ponte (2015) toteaa, että avoimen datan markkinat ovat vielä alullaan — markkinakatsaus osoittaa, että toimijat ovat hyvin erilaisia luonteeltaan ja liiketoimintamalleiltaan. Jakaminen, linkittäminen ja tiedon uudelleen käyttö ovat avainaktiviteettejä avoimien ekosysteemien toiminnassa. Taloudellisen hyödyn saavuttaminen avoimen datan avulla on vaikeaa, ja vaikka avoimen datan hyötyjä on korostettu, myös kriittisiä näkemyksiä avoimen datan hyödyistä/hyödyllisyydestä on esitetty.

Ponte (2015) esittelee (kuva 4) neljä ryhmää, jotka ovat keskeisiä avoimen datan ekosysteemissä: tiedon tuottajat, mahdollistajat, välittäjät ja loppukäyttäjät. Näistä mahdollistajat saattavat olla tärkeimpiä toimijoita ekosysteemissä roolissa, jonka tarkoituksena on tehdä datan käytöstä helpompaa muille ekosysteemin toimijoille. Välittäjät taas ovat toimijoita, jotka käyttävät dataa luodakseen tuotteita tai palveluita niitä tarvitseville. Mahdollistajien tärkeys perustuu siihen, että ne mahdollistavat datan käytön markkinoilla palveluja, kuten tiedon hallintaa, hakuja ja tallennusta muille toimijoille tuottavassa roolissaan. Mahdollistajien liiketoimintamallit jakautuvat kolmeen luokkaan:

- kysynnän mukaan orientoituneet
- tarjonnan mukaan orientoituneet
- lisäpalvelujen tuottoon keskittyneet toimijat.

Mahdollistajien tarve on selkeä, kun ajatellaan liiketoimintaa Suomessa ja laajemminkin: dataa tarjotaan eri toimijoiden kautta sekä erilaisilla tavoilla ja rajapinnoilla. Esimerkiksi julkishallinnon toimijoilla on perustoimintaa, johon avoimen datan tuottaminen harvoin kuuluu. Tuotantotalouden termein voidaan ajatella, että toiminnan ohella syntyy kuitenkin arvokkaita oheissuoritteita, kuten dataa, jota joku ulkopuolinen voi alkuperäistä toimijaa paremmin, motivoituneimmin ja joustavammin hyödyntää. Tällainen ajattelu on hyvin yleistä kiertotaloudessa laajemminkin.



Kuva 4: Avoimen datan ekosysteemi (Ponte 2015).

Kun halutaan luoda uutta liiketoimintaa, on tärkeää mahdollistaa uusien yritysten pääsy digitaalisten hyödykkeiden ja palvelujen markkinoille. Monesti ongelmana on se, että yrityksillä ei ole riittäviä resursseja ottaa tarjolla olevan avoimen datan käyttöä ja siihen liittyvää osaamista haltuun. Jos markkinoilla olisi riittävästi toimijoita, jotka keskittyisivät avoimen datan käytön helpottamiseen Suomessa, erilaisten yritysten kynnys lähteä markkinoille olisi matalampi. Tällöin ne voisivat keskittyä itse palvelun tai digitaalisen hyödykkeen käyttöön ja lisäarvon tuottamiseen loppukäyttäjille.

PK-yritysten ongelmaksi saattaa nousta esimerkiksi hyvän liikeidean toteuttamisen viivästyminen johtuen siitä, että avoimet rajapinnat, tarvittava data ja tukevat palvelut eivät ole sellaisia, että niiden käyttö olisi yritykselle mahdollista. Siinä vaiheessa, kun yritys on hankkinut riittävän osaamisen ja muut resurssit liikeidean toteuttamiseksi, riskinä on, että joku toinen toimija on jo toteuttanut kyseisen liikeidean.

Loppukäyttäjille suunnatut hyödykkeet ja palvelut liiketoimintamallina

Palvelujen ja hyödykkeiden tuottaminen kuluttajille on yleinen tapa tehdä liiketoimintaa avoimilla rajapinnoilla. Tästä esimerkkeinä ovat niin sovellustuotanto mobiililaitteille, henkilökohtaisille tietokoneille tehdyt sovellukset kuin verkon kautta käytetyt palvelut/sovellukset. Näihin ei tule kuitenkaan lukittua, koska digitalisaatiossa ne ovat vain osa laajempaa muutosta, vaikkakin ehkä eniten esillä.

Kuluttajamarkkinat ovat erityisen haastavia missä tahansa liiketoiminnassa, myös avoimeen dataan perustuvassa. Kuluttajat käyttävät palveluiden ja hyödykkeiden hankintaan omaa rahaansa, mikä johtaa suureen hintasensitiivisyyteen. Kuluttajia on suuri joukko, mikä edellyttää palveluiden olevan tehokkaasti skaalautuvia. Virheet ja ongelmat palvelussa näkyvät heti suurelle joukolle, ja tieto niistä kulkee tehokkaasti ja nopeasti kuulopuheena esimerkiksi sosiaalisessa mediassa (Sivadas & Jindal, 2016). Jos jokin menee pieleen, syytettyjen penkille joutuu helposti ensimmäisenä datan ja rajapinnat avannut, verorahoin toimiva viranomainen, ei niinkään yksityinen yritys, jonka toiminnassa kuluttajat luontaisesti sallivat voiton tavoittelun ja opportunismin.

Datan avaaminen altistaa sen myös kritiikille ja laaduntarkastukselle, jolloin datan laatua on mahdollista parantaa ja saada siitä korkeampilaatuista ja luotettavampaa kuin suljetusta datasta.

Avoin data tuotantoteollisuudessa

Liiketoiminta tuotantoteollisuudessa perustuu jonkin tuotteen valmistamiseen. Kuten Cusumano, Kahl & Suarez (2015) toteavat, palveluilla on ollut ja voi olla iso vaikutus yrityksen toimintaan riippumatta siitä, onko yritys uusi tai jo vakiintunut toimija. Palvelut tuotantoteollisuudessa voidaan jakaa kolmeen ryhmään seuraavasti (Cusumano ym. 2015):

- käyttöä helpottaviin, eli palveluihin, jotka helpottavat tuotteen käyttöä ilman tuotteen merkittävää muutosta; rahoitus, huolto, tuki jne.
- tuotetta mukauttaviin, eli palveluihin, jotka merkittävästi laajentavat tuotteen käyttöä
- tuotetta korvaaviin, eli palveluihin, joilla voidaan korvata tuotteen hankinta; tiedon käsittely, ohjelmiston hankkiminen palveluna jne.

Yrityksen menestyminen riippuu siitä, pystyykö se vastaamaan muuttuvien markkinoiden vaatimuksiin. Yrityksen johdon haasteena on päättää, mitä palveluja tarjotaan ja miksi. Yksi esimerkki alasta, jolla palvelut ovat olleet merkittävä osa tulonmuodostusta, on autoteollisuus. Palvelut sisältävät lainanantoa, huoltoa, korjausta, leasingia ja pidennettyjä takuita (Cusumano ym. 2015). Cusumano ym. (2015) eivät mainitse IoT:ta, mikä on selkeä puute artikkelissa. Tuotteet ovat tulevaisuudessa yhteydessä toisiinsa (Borgia, 2014), ja näin tuotteiden mukautettavuus nousee keskeiseksi tuotteen osaksi. Tämä ei myöskään enää voi olla vain tuotteen valmistajan yksin toteuttamaa. Sen rinnalle tarvitaan ekosysteemi, joka mahdollistaa monipuolisen ja laajan tarjonnan myytävälle tuotteelle, kuten mobiiliekosysteemeissä on käynyt. Mobiililaitteiden laitevalmistajat toteuttavat vain alustan ja peruspalvelut, joiden päällä sovellukset toteuttavat tarvittavat palvelut käyttäjälle (Hyrynsalmi 2014). Tuotteen menestyminen on riippuvainen siitä, kuinka hyvin sille tuotetaan palveluja ja miten vahva on ekosysteemi, jossa laitetta käytetään. Tätä ei voida ohittaa perinteisemmässäkään tuotantoteollisuudessa, koska asiakassuhteiden, avainyhteistyökumppaneiden ja toimivan verkoston merkitys ovat keskeisiä tekijöitä liiketoiminnan menestykselle (Dijkman, Sprenkels, Peeters, & Janssen 2015; Malmmose, Lueg, Khusainova, Iversen, & Panti 2015).

Dynaamiset liiketoimintamallit uusien yritysten menetystekijöinä

Spiegel, Abbassi, Zylka, Schlagwein, Fischbach ja Schoder (2016) tarkastelivat, miksi jotkut aloittavat yritykset menestyvät Internet-liiketoiminnassa ja toiset yritykset taas eivät. Keskeisenä löytönä oli, että menestys ei perustunut ainoastaan aloittavan yrityksen liiketoimintaideaan tai teknologiseen osaamiseen, vaan vahvasti myös yrityksen sosiaaliseen pääomaan. Menestyneitä yrityksiä yhdisti se, että niillä oli vahva sosiaalinen verkosto, joka oli kriittinen tekijä liiketoimintamallia muodostettaessa. Menestyvä liiketoimintamalli ei ole muuttumaton, vaan se kehittyy ja muuttuu keskeisen perusidean ympärillä. Tärkeää on, että aloittavalla yrityksellä on sosiaalinen verkosto, joka pystyy auttamaan liiketoimintamallin dynaamisessa kehittämisessä ja jatkorahoituksen saamisessa, kun yritys siirtyy seuraaviin vaiheisiin. Yritys, jolla on hyvä liikeidea, mutta ei riittävää sosiaalista verkostoa, ei tutkimuksen mukaan menesty yhtä hyvin kuin vahvan sosiaalisen verkoston omaava yritys silloin, kun yritys tarvitsee lisärahoitusta. On siis tärkeää rakentaa sosiaalista verkostoa ennen yrityksen perustamista ja esimerkiksi kutsua yrityksen hallitukseen henkilö, jolla on vahva sosiaalinen verkosto, kuten henkilö, jolla on pitkä ammatillinen kokemus, hyvin verkostoitunut pääomasijoittaja tai kokenut sarjayrittäjä.

5.5. Verkostovaikutus ja ekosysteemit

Verkostovaikutuksella tarkoitetaan tilannetta, missä tuotteesta tai palvelusta saatava hyöty riippuu niitä käyttävien kuluttajien määrästä (Farrell & Saloner 1985, 1986; Katz & Shapiro 1985). Verkostovaikutus voidaan jakaa kahteen eri tyyppiin: suoraan ja epäsuoraan verkostovaikutukseen (Katz ym. 1985). Suorassa verkkovaikutuksessa kasvanut käyttäjämäärä tuo lisää arvoa käyttäjille. Esimerkkeinä tästä ovat puhelin ja sosiaaliset mediat, joiden arvo käyttäjille riippuu toisista käyttäjistä ja niiden määrästä. Epäsuorassa verkostovaikutuksessa kasvanut käyttäjien määrä toimii kannusteena lisäpalvelujen tuottamiseen, mikä taas voi kasvattaa alkuperäisestä tuotteesta/palvelusta saatavaa arvoa ja hyötyä. Esimerkiksi pelikonsoleiden ja pelaajamäärän kasvu vetää puoleensa tuottajia tuottamaan lisää sisältöä kyseisille alustoille (Hyrynsalmi 2014).

Ekosysteemi on nykyajan trenditermi puhuttaessa ympäristöstä, teknologiasta, yritystoiminnasta ja yhteiskunnasta. Termillä voidaan käsittää monenlaisia asioita, mutta tässä digitaalisella ekosysteemillä tarkoitetaan yksinkertaistetusti digitaalista, verkottunutta elinkelpoista ympäristöä, johon kuulu toimijoita riittävän laajalta pohjalta.

VTT:n (2014) tutkimuksessa todetaan, että tulevaisuudessa globaaleilla markkinoilla ei voi enää menestyä kiinteiden, jäykkien verkostojen avulla. Globaalissa kilpailussa yritysten tulee olla mukana ekosysteemisessä liiketoiminnassa, jotta ne voivat menestyä tilanteessa, jossa asiakkaiden ongelmat vaativat yhä laajempaa ja mukautuvampaa osaamista entistä nopeammin. Asiakkaan palveleminen yhden toimijan kautta ei yksin riitä. Hyvänä esimerkkinä tästä ovat mobiiliekosysteemit. Pelkkä matkapuhelimen ja operaattorin muodostama liitto ei enää toimi nykyaikana, vaan asiakkaalle riittävän palvelun toteuttamisen edellytyksenä on elinkelpoinen ekosysteemi, joka kostuu tiedonsiirtoon keskittyvistä yrityksistä, operaattoreista, päätelaitevalmistajista, infrastruktuurin tuottajista sekä sovellusten ja palvelujen tuottajista, unohtamatta muita instansseja, kuten muita kansallisia ja kansainvälisiä toimijoita, sääntöjä ja standardeja (Hyrynsalmi 2014).

Jos suomalainen yhteiskunta aikoo menestyä globaalissa kilpailussa, on ensiarvoisen tärkeää, että julkinen sektori tukee digitaalisen ekosysteemin kehittymistä. Julkisella sektorilla on mahdollisuus olla edelläkävijä tiedon jakamisessa ekosysteemien käyttöön ja samalla olla luomassa uusia digitaalisia palveluita. Avoimet rajapinnat ovat keskeinen osa tätä tavoitetta ja valtion tulisikin avata tietojaan mahdollisimman paljon, jotta suomalainen yhteiskunta ja yritysmaailma voivat olla kilpailukykyinen ekosysteemi, jonka voimavarana on tieto ja sen avoin jakaminen.

Osaa julkisen sektorin tiedosta ei voida jakaa sellaisenaan, koska tällöin loukattaisiin yhteiskunnan perusarvoja. Esimerkiksi potilastietojen vapaa ja kontrolloimaton jakaminen olisi epäeettistä ja laitonta (Koskinen 2016). Tämä ei kuitenkaan tarkoita, että potilastietoja ei voisi lainkaan käyttää avoimen datan lähtökohdista. Potilastietojen käyttö anonyymeinä datamassoina tai potilaiden itse jakamana voi mahdollistaa uusia liiketoimintamahdollisuuksia esim. potilaan palvelemiseen aivan uudella tavalla, kunhan tietojen käytössä huomioidaan eettiset vaatimukset ja potilaiden intressit (Koskinen, Kainu & Kimppa 2016; Koskinen & Kimppa 2016). Avoin, anonyymi potilasdata voi toimia pohjana eri sektorien (julkinen, yksityinen ja kolmas sektori) terveyspalveluille ja mahdollisesti uusille ennakoimattomissa oleville innovaatioille sekä kokonaan uudelle terveydenhuollon ekosysteemin muutokselle.

Julkisella sektorilla on mahdollisuus olla luomassa elinkelpoista ekosysteemiä toimimalla ns. katalyyttina jakamalla dataa avoimesti avointen rajapintojen kautta. Lisäksi julkinen sektori voi olla luomassa uutta liiketoimintaa sitoutumalla uusien palvelujen kehittämiseen omassa toiminnassaan. Tässä palvelujen kehittämisen tulee olla tarvelähtöistä ja tähdätä esimerkiksi ongelmien ratkaisuun. Julkisen sektorin tulisi viestittää organisaatioidensa haasteista ja operatiivisessa toiminnassaan kokemistaan ongelmakohdista. Tällöin olisi todennäköisempää saada yksityiset toimijat pohtimaan liiketoimintaideoita ja -malleja yhdessä julkisen sektorin kanssa, jotta esille tuodut ongelmat voidaan ratkaista. Tällöin voitaisiin löytää myös uusia tapoja luoda arvoa ekosysteemin osille – niille, jotka tuottavat dataa (esim. julkinen sektori), jalostavat sitä (sovellusten kehittäjät) tai käyttävät sitä (loppukäyttäjät) (Janssen ym. 2012).

Julkinen hallinto ei yksin pysty aikaansaamaan ekosysteemiä digitaalisten hyödykkeiden kautta. Silti sen merkitys luotettavan tiedon tarjoajana (vaikka se ei ehkä voi taata muiden tarjoamien tietojen luotettavuutta) ja ympäristön takaajana voi toimia pohjana sille, että uusia digitaalisia liiketoimintamalleja voi syntyä yritysmaailman taholta, yhdessä julkisen sektorin kanssa. Tässä tarvitaan ketteryyttä yhteiskunnan suunnalta ja tarvittaessa myös kykyä säädellä toimintaa asetuksilla ja laeilla nopeasti, jotta informaatioteknologian nopeasti aiheuttamiin ja muuttuviin haasteisiin voidaan vastata. Tässä ongelmaksi nousevat nopeat muutokset ja ongelmat, jotka kehitys aiheuttaa yhteiskunnalle ja lainsäädännölle niiden jäykän ja hitaan luonteen takia (Moor 1985). Tähän voidaan vastata nojautumalla eettisiin koodistoihin ja RRI:n (Responsible Research and Innovation) tyyppisiin lähestymistapoihin (Burget, Bardone &

Pedaste 2016; Stahl, Eden, Jirotka & Coeckelbergh 2014), jotka kuuluvat ns. ”soft law” -ratkaisuihin (Kainu & Koskinen 2014).

5.6. API-manifesti vapaiden rajapintojen tarjonnan ja käytön ohjenuoraksi

API-manifesti (Application Programming Interface) on API-yhteisön ehdotus seitsemäksi teesiksi, joilla edistetään avoimien rajapintojen mahdollistamaa liiketoimintaa Suomessa[13]. Seuraavassa esitellään nämä seitsemän teesiä ja avataan ne tämän hankkeen lähtökohdista.

Palvele digitaalisesti rajapintapalvelun avulla

Rajapinnat mahdollistavat digitaalisten palvelujen tuottamisen sidosryhmien kesken. Niiden tulee olla palvelu- ja ohjelmistosuunnittelun keskiössä, koska tällöin voidaan mahdollistaa uudet ja eri rajapintojen kautta saatavan tiedon mahdollistamat palvelut. Jotta eri rajapintoja voidaan luotettavasti ja kestävästi hyödyntää, tulee rajapinnalla olla riittävä palvelulupaus (service-level agreement, SLA) julkisesti nähtävillä.

Suosi avoimuutta

Avoimuuden tulee olla lähtökohta, ellei jokin selkeä ja perusteltu asia ole sen esteenä. Tiedon hyöty tulee esiin vain jos sitä voi käyttää.

Tee käyttöönotosta mahdollisimman helppoa

Rajapintojen käyttöönoton tulee olla mahdollisimman helppoa. Ensimmäinen asia onkin varmistaa, että etusijalla ovat yleisesti hyväksytyt ja vakiintuneet rajapinnat, ellei jokin nouseva uusi vaihtoehto ole selkeästi parempi ja tule todennäköisesti syrjäyttämään muut vaihtoehdot nopeasti.

Mittaa, opi palautteesta ja iteroi

Jos rajapinnat vain avataan, eikä niihin sen jälkeen kiinnitetä huomiota, siitä ei todennäköisesti saada kaikkea mahdollista hyötyä. Rajapinnan käyttö vaatii arviointia ja palautetta, jotta sitä ja sen kautta tarjottavaa tietoa voidaan kehittää tarvittaessa. Kuten manifestissa todetaan: ”*Rajapinnan kehityksessä kannattaa pyrkiä jatkuvaan yhteistyöhön sen asiakkaiden kanssa*”. Toteamus on yhteneväinen Almiralin, Leen, ja Majchrzakin (2014) löydösten kanssa koskien yhteistyön merkitystä uusia palveluja kehitettäessä. On ehdottoman tärkeää, että julkinen sektori sitoutuu pitkäjänteisesti ja ottaa huomion ne toimijat, jotka rajapintoja käyttävät.

Tee yhteistyötä muiden kanssa

Useilla eri tahoilla voi esiintyä yhteneväisiä rajapintatarpeita, ja tämän takia potentiaaliset yhteistyömahdollisuudet tulee selvittää. Lisäksi julkisen sektorin tulee kiinnittää huomiota omiin toimintatapoihin, kun sen toimintaa kehitetään digitaalisilla hyödykkeillä ja palveluilla. Jos toimittajayritysten henkilökunta sitoutetaan mukaan julkisen organisaation toimintaan (määräajaksi osaksi toimintaa), on ymmärrys organisaation tarpeista hyvä ja tuotteet soveltuvat kohdeorganisaatiolle (Lee ym. 2014).

[13] Api-yhteisö 2016. http://apimanifesti.fi/ luettu 14.6.2016

Toteuta johdonmukaisesti

Rajapintojen tarjoamisessa tulee olla johdonmukainen. Käyttöehtojen tulisi olla yhdenmukaisia ja rajapintojen sisällön tulisi olla tarjolla yhden lisenssin alla. Lisäksi tulisi käyttää standardeja rajapintoja aina kun mahdollista. Toimimalla johdonmukaisesti voidaan lisätä luottamusta ja vakautta, jota tarvitaan luotaessa uutta liiketoimintaa ja rakentaessa elinkelpoista ekosysteemiä[9].

Tee tarkoituksenmukaisia rajapintoja

Hyvä rajapinta vastaa tiettyyn tarpeeseen, ja sille tulee olla ajateltuna myös suunniteltu elinkaari - rajapinnatkaan eivät ole ikuisia. Tätä varten rajapinnalla tulee olla selkeä ja ajantasainen dokumentaatio, minkä lisäksi niiden tulee siis olla rajattuja, käytännöllisiä ja helppokäyttöisiä.

5.7. Vastuullinen liiketoiminta luottamuksen edellytyksenä

Pysyvyyttä tarvitaan, kun kehitetään avoimeen dataan ja rajapintoihin perustuvaa liiketoimintaa tai edistetään julkisen sektorin tehostamista. Jos luottamusta tähän ei ole, ei kehitykseen panosteta ja tavoitteet jäävät saavuttamatta. Yksi keskeisistä – mutta ei ainoa – motivaatiotekijä avoin data -liikkeen taustalla on hallinnon läpinäkyvyyden lisääminen ehkäisemässä korruptiota. Yhteiskunnat, joissa korruptio on vahvaa, ovat myös niitä yhteiskuntia, joissa kansalaisten luottamus yhteiskuntaa ja sen päättäjiä kohtaan on vähäistä (Attard, Orlandi, Scerri & Auer 2015). Lisäksi luottamus, syrjimättömyys ja avoimuus ovat perustavaa laatua olevia mahdollistajia verkostoituneen liiketoiminnan arvon luomisessa (Pera, Occhiocupo & Clarke 2016)

Luottamuksen kannalta on ensiarvoisen tärkeää tarkastella avointa dataa, avoimia rajapintoja ja niiden soveltamista myös eettisestä näkökulmasta, ja tässä julkisella sektorilla on keskeinen asema. Yhteiskunta tuottaa suuren osan jakoon kelpaavasta informaatiosta. Tiedon jakajan ja lainsäätäjän ominaisuudessa se voi ajaa eettisesti kestävää tiedon jakoa ja kontrollia. Tässä voidaan käyttää viitekehyksenä RRI:tä, joka vastaa informaatioteknologian tuomiin eettisiin haasteisiin tutkimuksessa ja kehitystyössä (Stahl ym. 2014). RRI on esimerkiksi otettu mukaan Euroopan unionin Horizon 2020 ohjelmaan läpileikkaavana teemana (cross-cutting issue). Tämä puoltaa sen käyttöä yleisesti käytössä olevana viitekehyksenä[14].

RRI:ssä eri osapuolet (tutkijat, kansalaiset, päättäjät ja yritykset jne.) yhdessä toimivat saavuttaakseen tulokset, jotka toteuttavat yhteiskunnan arvoja ja odotuksia, mikä on myös julkisen sektorin tavoitteena (Burget ym. 2016). Tämä on linjassa Leen ym. (2015) suosituksen kanssa sitouttaa toimittajat, rahoittajat ja julkisen sektorin tekijät yhteen, jotta voidaan saada elinkelpoisia palveluja, jotka hyödyttävät yhteiskunnan kaikkia osapuolia.

Liiketoimintanäkökulmassa otetaan huomioon taloudelliset realiteetit, ja RRI-lähestymistapa taas varmentaa, että ehdotukset ovat eettisesti vahvalla pohjalla ja siten tukevat oikeudenmukaista ja luotettavaa toimintaa yhteiskunnassa. Molemmat lähestymistavat osaltaan lisäävät luotettavuutta, jos ne otetaan osaksi liiketoimintaa yhteiskunnassa. Tämä vaatii julkisen sektorin sitoutumista ja eettisen analyysin aktiivista käyttöönottoa kaikessa toiminnassa. Ongelmana

[14] Horizon 2020, the EU Framework Programme for Research and Innovation. https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation Luettu 15.1.2016

nousee esiin eettisen osaamisen puute organisaatiossa, ja etiikka tulisikin ottaa osaksi koulutusta, koska kuten SITRA:n (Kataja 2016) raportissa todetaan: ”*yksi tulevaisuuden tärkeimmistä aiheista voi olla digitaalinen etiikka. Suurimmat kysymykset teknologian suhteen eivät välttämättä ole kysymyksiä teknologiasta vaan ihmisistä ja ihmisyydestä*.”

5.8. Pohdintaa ja johtopäätöksiä

Globaalisti tarkasteltuna suurimpia menestystarinoita rajapintojen osalta ovat sosiaalisen median toimijat (esim. Facebook), jotka tarjoavat rajapinnan tuhansille eri sovelluksille, sekä mobiilipuolen ekosysteemin perustan muodostavat käyttöjärjestelmät Googlen Android ja Applen iOS, muiden toimijoiden jäädessä marginaaliseen asemaan. Hyrynsalmi, Suominen, Mäkilä & Knuutila (2014) toteavat, että alusta, joka mahdollistaa helpon sovellusten toteuttamisen on kehittäjille ja näin ollen myös alustalle hyödyksi. Tässä siis korostuvat huomiot, joita API-manifestissa korostetaan: avoimuus, yksinkertaisuus, yhteistyö ja tarpeisiin vastaaminen.

Aloittavien yritysten kohdalla menetystekijäksi nousee sosiaalinen pääoma, jonka avulla voidaan löytää oikeat toimijat ja riittävä rahoitus yritykselle. Avoimien rajapintojen ja avoimen datan kohdalla tämän voidaan todeta olevan myös totta: yritys, jolla on hyvä sosiaalinen verkosto, saa helpommin tukea ja osaamista, mikä on erittäin tärkeää digitaalisien palvelujen ja tuotteiden kohdalla niiden verkostoituneen luonteen takia. Erityisesti tämä korostuu asioiden ja esineiden Internetin yleistyessä, missä lähes kaikki toiminta perustuu laajempaan ekosysteemiin. Erityisesti PK-yritysten tulee vastata tähän haasteeseen lisäämällä sosiaalista pääomaansa, verkostoituen eri toimijoiden kanssa.

Suomessa julkisen sektorin esimerkkinä rajapintoihin perustuvasta järjestelmästä voidaan nostaa esiin Kanta-palvelut, jotka edustavat avoimiin rajapintoihin perustuvaa terveydenhuollon perusalustaa. Kanta-palveluiden ympärille rakennetaan terveydenhuollon palvelukokonaisuutta, ekosysteemin perustaa. Kanta-hanke on esimerkki siitä, miten julkisen sektorin panosta usein tarvitaan, jonka jälkeen yksityinen sektori voi alkaa kehittää toimintaa omalta osaltaan.

Julkisen sektorin tulee miettiä rooliaan sekä avointen rajapintojen ylläpitäjänä ja avoimen datan julkaisijana että niiden hyödyntäjänä. Julkaisijana tulee olla avoin ja luotettava toimija, joka palvelee yhteiskuntaa mahdollisimman hyvin. Tässä on hyvä pitää ohjenuorana API-manifestia, jota noudattamalla varmistetaan hyvä palvelu. Jotta tässä onnistutaan, tulee varmistaa, että kaikki eri julkisen sektorin organisaatiot omaksuvat ja toteuttavat API-manifestin ajatuksen. Kaikilta julkisen sektorin organisaatioilta voidaan edellyttää avointa, sitoutunutta ja yhdenmukaista toimintaa avointen rajapintojen ja avoimen datan kautta palvelemisessa.

Hyödyntämisroolissa tulee erityisesti korostaa sitä, että tarjotaan oikeisiin ongelmiin ratkaisuja, joita organisaatiot ja operatiiviset toimijat julkisella sektorilla tarvitsevat. Tässä keskeistä on ottaa kehittäjät mukaan organisaation toimintaan. Näin voidaan varmistaa, että sovellukset ja palvelut ratkaisevat oikean ja todellisen ongelman. Hyödyntämisroolissa tulee myös pohtia tarkkaan, mitä palveluja tuotetaan itse ja mitä ostetaan ulkopuolelta. Varsinkin palveluiden ulkoistaminen kokonaan on kyseenalaista[15] erityisesti, jos ne ovat perusinfrastruktuuria tai muuten kriittistä osaamista digitaaliselle palvelujen kehittämiselle.

Julkinen sektori voi siis toimia mahdollistajana jakaessaan avointa dataa avointen rajapintojen kautta, ja sen lisäksi se voi ottaa aktiivisen otteen ja sitouttaa toimijoita, kun se kehittää omien organisaatioidensa tuottamia palveluita.

[15] Esimerkkeinä sähköverkon myynti Carunalle ja TV-lähetysten myynti Digitalle.

Lähteet

Almirall, E., Lee, M. & Majchrzak, A. (2014). Open innovation requires integrated competition-community ecosystems: Lessons learned from civic open innovation. *Business Horizons*, 57 (3), 391-400. doi:http://dx.doi.org/10.1016/j.bushor.2013.12.009

Attard, J., Orlandi, F., Scerri, S. & Auer, S. (2015). A systematic review of open government data initiatives. *Government Information Quarterly, 32*(4), 399–418. doi:http://dx.doi.org/10.1016/j.giq.2015.07.006

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications, 54*, 1–31. doi:http://dx.doi.org/10.1016/j.comcom.2014.09.008

Burget, M., Bardone, E. & Pedaste, M. (2016). Definitions and Conceptual Dimensions of Responsible Research and Innovation: A Literature Review. *Science and Engineering Ethics*, 1–19. doi:10.1007/s11948-016-9782-1

Cusumano, M. A., Kahl, S. J. & Suarez, F. F. (2015). Services, industry evolution, and the competitive strategies of product firms. *Strategic Management Journal, 36*(4), 559–575. doi:10.1002/smj.2235

DaSilva, C. M. & Trkman, P. (2014). Business Model: What It Is and What It Is Not. *Long Range Planning, 47*(6), 379–389. doi:http://dx.doi.org/10.1016/j.lrp.2013.08.004

Dijkman, R. M., Sprenkels, B., Peeters, T. & Janssen, A. (2015). Business models for the Internet of Things. *International Journal of Information Management, 35*(6), 672–678. doi:http://dx.doi.org/10.1016/j.ijinfomgt.2015.07.008

Farrell, J. & Saloner, G. (1985). Standardization, Compatibility, and Innovation. *The RAND Journal of Economics, 16*(1), 70–83. doi:10.2307/2555589

Farrell, J. & Saloner, G. (1986). Installed Base and Compatibility: Innovation, Product Preannouncements, and Predation. *The American Economic Review, 76*(5), 940–955.

Huijboom, N. & Van den Broek, T. (2011). Open data: an international comparison of strategies. *European journal of ePractice, 12*(1), 4–16.

Hyrynsalmi, S. (2014). *Letters from the War of Ecosystems.* (Doctor of Philosophy), University of Turku, Turku.

Hyrynsalmi, S., Suominen, A., Mäkilä, T. & Knuutila, T. (2014). The Emerging Application Ecosystems: An Introductory Analysis of Android Ecosystem. *International Journal of E-Business Research (IJEBR), 10*(2), 61–81. doi:10.4018/ijebr.2014040104

International, O. K. (2016). *What is Open Data?* Haettu osoitteesta http://opendatahandbook.org/guide/en/what-is-open-data/

Investopedia. (2016). *Business Model*. Haettu osoitteesta http://www.investopedia.com/terms/b/businessmodel.asp

Janssen, M., Charalabidis, Y. & Zuiderwijk, A. (2012). Benefits, Adoption Barriers and Myths of Open Data and Open Government. *Information Systems Management, 29*(4), 258–268. doi:10.1080/10580530.2012.716740

Kainu, V. & Koskinen, J. (2014). *Why (and) Ethics code for information system development needs institutional support: there is even an upside for computnig practitioners and businesses*. Ethicomp 2014.

Kataja, E. (2016). *Megatrendit 2016.* In SITRA (Series Ed.) 56.

Katz, M. L. & Shapiro, C. (1985). Network Externalities, Competition, and Compatibility. *The American Economic Review, 75*(3), 424–440.

Koskinen, J. (2016). *Datenherrschaft – an Ethically Justified Solution to the Problem of Ownership of Patient Information.* (Ph.D.), Turun Yliopisto, Suomen yliopistopaino oy, Turku. http://urn.fi/URN:ISBN:978-952-249–467-2

Koskinen, J., Kainu, V. & Kimppa, K. (2016). The concept of Datenherrschaft of patient information from a Lockean perspective. *Journal of Information, Communication and Ethics in Society, 14*(1), 70–86. doi:10.1108/JICES-06-2014-0029

Koskinen, J. & Kimppa, K. (2016). An Unclear Question: Who Owns Patient Information? Teoksessa D. Kreps, G. Fletcher, & M. Griffiths (Eds.), *Technology and Intimacy: Choice or Coercion: 12th IFIP TC 9 International Conference on Human Choice and Computers, HCC12 2016, Salford, UK, September 7-9, 2016, Proceedings* (3–13). Cham: Springer International Publishing.

Lee, M., Almirall, E. & Wareham, J. (2015). Open data and civic apps: first-generation failures, second-generation improvements. *Commun. ACM, 59*(1), 82–89. doi:10.1145/2756542

Malmmose, M., Lueg, R., Khusainova, S., Iversen, P. S. & Panti, S. B. (2015). Charging customers or making profit? Business model change in the software industry. *Journal of Business Models (2014), 2*(1), 19–32.

Moor, J. H. (1985). What is computer ethics? *Metaphilosophy, 16*(4), 266–275.

Ojo, A., Curry, E. & Zeleti, F. A. (2015, 5-8 Jan. 2015). A tale of open data innovations in five smart cities. in *System Sciences (HICSS), 2015 48th Hawaii International Conference on Systems Sciences* (pp. 2326-2335). IEEE.

Pera, R., Occhiocupo, N. & Clarke, J. (2016). Motives and resources for value co-creation in a multi-stakeholder ecosystem: A managerial perspective. *Journal of Business Research, 69*(10), 4033–4041. doi:http://dx.doi.org/10.1016/j.jbusres.2016.03.047

Ponte, D. (2015). *Enabling an Open Data Ecosystem.* Paper presented at the ECIS.

Roll, M. & Verbeke, A. (1998). Financing of the trans-European high-speed rail networks:: New forms of public–private partnerships. *European Management Journal, 16*(6), 706–713. doi: http://dx.doi.org/10.1016/S0263-2373(98)00047-4

Rowley, J. (2007). The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of Information Science, 33*(2), 163–180.

Sivadas, E., & Jindal, R. P. (2016). Alternative Measures of Satisfaction and Word of Mouth. *Journal of Services Marketing*, *31*(2), 119-130.

Spiegel, O., Abbassi, P., Zylka, M. P., Schlagwein, D., Fischbach, K. & Schoder, D. (2016). Business model development, founders' social capital and the success of early stage Internet start-ups: a mixed-method study. *Information Systems Journal, 26*(5), 421–449. doi:10.1111/isj.12073

Stahl, B. C., Eden, G., Jirotka, M. & Coeckelbergh, M. (2014). From computer ethics to responsible research and innovation in ICT: The transition of reference discourses informing ethics-related research in information systems. *Information & Management, 51*(6), 810–818. doi: http://dx.doi.org/10.1016/j.im.2014.01.001

Tammisto, Y. & Lindman, J. (2012). Definition of Open Data Services in Software Business. Teoksessa M. A. Cusumano, B. Iyer, & N. Venkatraman (Eds.), *Software Business: Third International Conference, ICSOB 2012, Cambridge, MA, USA, June 18-20, 2012. Proceedings*. (297–303). Berlin, Heidelberg: Springer Berlin Heidelberg.

Ugander, J., Karrer, B., Backstrom, L., & Marlow, C. (2011). The anatomy of the facebook social graph. *arXiv preprint arXiv:1111.4503*.

VTT. (2014). Ekosysteemit ja verkostojen parviäly. Haettu osoitteesta https://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi8kpzTjYXQAhVEGZoKHa74AZQQFggbMAA&url=http%3A%2F%2Fwww.vtt.fi%2Finf%2Fpdf%2Ftechnology%2F2014%2FT152.pdf&usg=AFQjCNFDy5KZwHKKnUKsZRAjNMFjtccl3g&sig2=K_oLVrLXanDdXz0GiqWX5Q

Wikipedia. (2016). *Liiketoimintamalli*. Haettu osoitteesta https://fi.wikipedia.org/wiki/Liiketoimintamalli

LUKU 6.

Anonyymeihin datamassoihin liittyvät liiketoimintamahdollisuudet

Niemimaa Marko

Kuulemme usein, kuinka data on digitaalitalouden uusi öljy. Dataa syntyykin alati kiihtyvällä tahdilla. Jo 2010 Eric Schmidt, toinen Googlen perustajista, totesi, että tuotamme kahdessa päivässä niin paljon dataa kuin koko ihmiskunnan aikana oli ennen vuotta 2003 tuotettu (TechCrunch, 2010). Tälle kehitykselle ei näyttäisi olevan loppua. Johtava markkina-analytiikkayritys, International Data Corporation (IDC) (2014), arvioi selvityksessään datan määrän kymmenkertaistuvan vuosien 2013–2020 välillä 4,4 tsettatavusta 44 tsettatavuun. Tämä tarkoittaisi, että vuonna 2020 maailmassa olisi lähes yhtä monta bittiä kuin koko universumissa on arvioitu olevan tähtiä, ja tähän tallennustilaan mahtuisi nauhoitettuna kaikki ihmiskunnan puhe alkuajoista lähtien (Ziberman 2003). Nämä valtavat datamassat sisältävät kaikki ne kuvat ja videot, jotka sosiaaliseen mediaan lisäämme, kaikki ne viestit, jotka vaihdamme ystäviemme ja kollegoidemme kanssa, mutta myös yhä enenevissä määrin koneiden välistä kommunikointia ja tietoa, joita sensorit meistä ja ympäristöstämme luovat. Nämä suuret datamassat ovat kuin raakaöljyä – ne vaativat jatkojalostamista liiketoiminnallisen hyödyn saamiseksi.

Datamassojen liiketoiminnallinen hyöty tulee niiden sisältämän tiedon jalostamisesta erilaisin analyysimenetelmin. Tyypillisesti datamassoja hyödynnetään markkinointitarkoituksiin edistämään tuotteiden myyntiä tai poliittisiin tarkoituksiin ehdokkaiden tai puolueiden tavoitteiden ajamiseksi. Tämä ei itsessään ole uutta. Vastaavia keinoja on hyödynnetty jo pitkään esimerkiksi televisio-, radio- ja sanomalehtikampanjoissa. Mainostus on tehokkaampaa, kun viesti räätälöidään oletetun kohdeyleisön mieltymysten mukaiseksi. Datamassat ovat kuitenkin tuoneet täysin uusia mahdollisuuksia markkinoinnin kohdentamiseen. Keräämällä suuret määrät dataa voidaan toteuttaa yhä tarkempia kampanjoita, jotka vetoavat juuri tiettyyn pieneen ryhmään kuluttajia (tai äänestäjiä) tai kohdentaa viesti jopa yksittäiselle yksilölle. Tunnetut yritykset, kuten Google, Facebook ja Twitter tallentavat valtaviin konesaleihin yksityiskohtaisesti lähes kaiken sen, mitä palveluissa teemme. Yksi keskeinen syy tällaisen yksilöitä identifioivan tiedon tallentamiseen on kaupallinen. Datamassojen kerääminen ja niiden analysointi ovatkin tehneet Googlesta ja Facebookista maailman menestyneimpiä yrityksiä. Myös kuluttajat hyötyvät analysoinnista, kun tuotemainonta on heille relevanttia ja uusia tuotteita voidaan datamassojen avulla suunnitella paremmin kuluttajien tarpeisiin.

Tällaisen yksilöivän ja tarkan datamassan käsittelyyn ja hyödyntämiseen liittyy kuitenkin vakavia tietosuojaongelmia. Tunnettu tietosuoja-asiantuntija, Aral Balkan, on puheissaan kiinnittänyt huomiota datamassojen tietosuojaongelmiin. Hän on väittänyt, hieman provosoiden, että se, mitä näiden yritysten suurissa konesaleissa säilötään ja kultivoidaan, on kaikki se, mikä tekee meistä yksilöitä, pois lukien fyysinen vartalomme (Balkan 2015). Vaikka väite voi kuulostaa äkkiseltään liioittelulta ja jopa järjettömältä, on selvää, että yritykset käyttävät miljardeja louhiakseen datamassoista yhä tarkempia keinoja profiloida, mitkä tekijät ajavat yksilöiden käyttäytymistä. Esimerkiksi hiljattain selvisi, että Facebook muokkasi käyttäjille näytettäviä syötteitä tehdäkseen käyttäjillään kokeita koskien sitä, millaiset viestit aiheuttavat käyttäjissä eri tunnetiloja, kuten ärtymystä tai iloa (Booth 2014). Lisäksi tietoturva-asiantuntija Mikko Hyppönen on puheessaan todennut, että kuten öljyn kanssa tapahtuu öljyvuotoja, niin myös datan

kanssa tapahtuu datavuotoja (Hyppönen 2017). Lähes päivittäin saamme lukea, kuinka suuria datamassoja on vuotanut vääriin käsiin joko erehdyksen kautta tai tahallisen tietomurron seurauksena. Usein tällaisissa vuodoissa on mukana myös luonteeltaan yksityistä tietoa, kuten henkilötunnuksia, luottokorttitietoja, tai potilastietoja. Suurten datamassojen säilyttämiseen liittyy siis vakavia tietovuodon riskejä.

Datamassat näyttäytyvätkin kaksiteräisenä miekkana – samalla, kun datamassat sisältävät valtavan liiketoiminnallisen potentiaalin, ovat ne kyseenalaisia yksityisyydensuojan kannalta. Onkin keskeistä tutkia, millaisia liiketoimintamalleja voitaisiin luoda *anonyymien* datamassojen ympärille, eli datamassojen, jotka *eivät* sisällä yksittäistä käyttäjää yksilöivää tietoa. Tässä raportissa paneudutaan tähän ongelmaan.

6.1. Anonyymit datamassat ja liiketoiminnan haasteet

Anonymiteetti – mitä se on ja miten se voidaan saavuttaa?

Anonymiteetti voidaan ymmärtää EU:n tietosuoja-asetuksen mukaan niin, että tieto on anonyymiä, kun se ei liity tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (Euroopan unioni 2016). Toisin sanoen anonymiteetti viittaa vapauteen olla tunnistamattomissa, piilossa ja yksilöimättömissä (Scott & Orlikowski 2014). Datamassat ovat anonyymejä, kun niiden sisältämästä tiedosta ei pystytä tunnistamaan tai yksilöimään ketään yksittäistä luonnollista henkilöä. Näitä ajatuksia mukaillen tässä raportissa tarkoitetaan anonyymeillä datamassoilla tietovarantoja, jotka sisältävät yksilöistä tietoa, jota ei kuitenkaan voida yhdistää kehenkään tiettyyn yksilöön. Muut datamassat, jotka eivät sisällä yksilöiden käyttäytymiseen liittyvää tietoa, eivät näin olleen kuulu anonyymien datamassojen piiriin. Tällaisia datamassoja voisivat olla esimerkiksi suuret tietovarannot, jotka liittyvät moottoreiden toiminnan valvontaan, hiukkaskiihdyttimen toimintaan tai järjestelmien keskinäiseen kommunikointiin.

Käyttäjän yksityisyyden turvaamisen lisäksi mahdollisuudella toimia verkossa anonyymisti on myös käänteisiä puolia. Jos käyttäjille tarjotaan mahdollisuus toimia verkossa täysin anonyymisti, usein myös häiriökäyttäytyminen lisääntyy (Levmore & Nussbaum 2010). Kun käyttäjät voivat toimia anonyymisti, he eivät koe olevansa vastuussa teoistaan ja sanomisistaan samalla tavoin kuin oikealla nimellään toimiessaan (Scott & Orlikowski 2014). Tällaisen haitallisen käyttäytymisen kitkemisen lisäksi on kuitenkin myös kaupallisia syitä siihen, miksi yksilöivää tietoa halutaan kerätä.

Kun asioin verkkokaupassa ja ostan itselleni vaatteita, jää ostoksistani merkintä verkkokaupan tietoihin. Mikäli ostoksen tiedot tallennetaan niin, että ne voidaan yksilöidä minuun, ei anonymiteetti toteudu. Jos verkkokauppa tietää nimeni, sähköpostiosoitteeni, ostokseni ja mahdollisesti myös luottokorttini numeron, on sillä riittävät tiedot yksilöidä ostokset juuri minuun. Tällaisen tiedon tallentaminen on arvokasta tietoa yritykselle. Tiedon avulla voidaan esimerkiksi lähettää kohdennettua markkinointia tai tietoja voidaan myydä muille toimijoille. Voidaan miettiä, onko yrityksen tarpeen tallentaa ja yksilöidä kaikki ostokseni, vai pitäisikö sen tyytyä keräämään vain yleisempiä trendejä siitä, mitkä tuotteet ovat suosittuja koko asiakaskunnan tai tiettyjen asiakasryhmien keskuudessa. Tällaiset yleiset trendit eivät vaadi yksittäisten henkilöiden ja ostosten tietämistä, vaan riittää, kun tiedetään yleisellä tasolla, mitä tuotteita verkkokaupasta ostetaan. Tällöin kuitenkin tallennetun datamassan liiketoiminnalliset mahdollisuudet vähenevät. On kuitenkin olemassa tilanteita, joissa yksilöivän tiedon tallennus on välttämätöntä.

Lääkärissä asioiminen ja vakuutuskorvausten hakeminen ovat esimerkkejä, joissa henkilön tunnistaminen ja tarkan, yksilöivän tiedon kerääminen on välttämätöntä. Hoidon kannalta on tärkeä tietää, mitä lääkkeitä henkilölle on määrätty. Samoin vakuutusyhtiöissä on tärkeä tietää

henkilöiden hakemat korvaukset, jotta voidaan välttyä maksamasta korvauksia useampaan otteeseen ja näin estää vakuutuspetoksia. Näiden datamassojen tallentaminen ja käsittely vaativat kuitenkin vastuullisuutta niitä säilyttäviltä yrityksiltä ja tiukkaa lainsäädäntöä niiden käsittelyyn sekä selkeitä tietoturvapolitiikkoja ja ohjeistuksia (ks. Niemimaa & Niemimaa 2017). Tällaisissa tiedoissa piilee kuitenkin suuria kaupallisia ja tutkimuksellisia mahdollisuuksia, joiden takia datamassoja on pyritty saamaan jatkohyödynnettäväksi. Miten on mahdollista myydä ja jakaa tällaista tietoa, joka koetaan usein arkaluonteiseksi?

Datamassojen anonymisoimisella tarkoitetaan tekniikoita, joiden avulla kerätystä datamassasta pyritään poistamaan yksilöivää tietoa tai korvaamaan sitä (esimerkiksi pseudonymisoimalla[16]). Tiedot, kuten henkilön nimi, osoite ja syntymäaika poistetaan datamassasta, jolloin se saadaan anonymisoitua. Tällaista tekniikkaa on hyödynnetty esimerkiksi vakuutustietojen suhteen (Ohm 2010). Anonymisoidut datamassat voidaan tämän jälkeen myydä eri tahoille jatkojalostettavaksi. Tässä kuitenkin piilee vaara.

Anonymiteetti on harvoin absoluuttista tai täydellistä. Anonymiteettiä ei voida nähdä vain binäärisenä eli niin, että anonymiteetti joko on tai ei ole. Pikemminkin anonymiteetti tulisi nähdä jatkumona anonyymin tiedon ja täysin yksilöivän tiedon välillä (Smith ym. 2011). Tällöin esiin nousee kysymyksen ”onko datamassa anonyymiä” sijaan kysymys siitä, ”onko datamassa *riittävän* anonyymiä”. Eri organisaatioiden hallussa olevien datamassojen avulla ja niistä löytyviä tietoja yhdistelemällä voidaan henkilön identiteetti joissain tapauksissa selvittää, vaikka datamassa olisikin pyritty anonymisoimaan. Voidaankin sanoa, että poistamalla tietoa ja anonymisoimalla datamassaa voidaan lisätä sen todennäköisyyttä, että yksilöä ei pystytä tunnistamaan datamassasta, mutta tunnistamisen mahdollisuutta ei voida täydellisesti poissulkea.

Tutkijat ovat osoittaneet, että joissain tapauksissa datamassasta, joka on pyritty anonymisoimaan, on pystytty tunnistamaan yksilöitä suurella todennäköisyydellä tai jopa varmuudella. Eräässä kuuluisassa tutkimuksessa Sweeney (2002) hyödynsi kahta saatavilla olevaa tietokantaa, joista toinen sisälsi anonymisoidut tiedot Massachusettsin julkisen sektorin työntekijöiden terveysvakuutuksista ja toinen alueen äänestysrekisterin. Yhdistämällä vakuutusdatasta löytyvät terveystiedot ja äänestysrekisteristä löytyvät tiedot hän pystyi tunnistamaan Massachusettsin sen hetkisen pormestarin terveystiedot. Koko Massachusettsin äänestäjätietokannassa vain kuudella oli sama syntymäpäivä kuin hänellä, vain kolme näistä kuudesta oli miehiä ja hän oli ainut kolmesta miehestä, joka asui tietyllä postinumeroalueella. Näin tutkija pystyi päättelemään, että kyseessä täytyi olla pormestarin tiedot. Tämä löydös oli erityisen huolestuttava, sillä tapa, jolla datamassa oli anonymisoitu, on yleisesti käytetty, ja sen on katsottu lainsäädännöllisesti täyttävän anonymiteetin vaatimukset erityisesti Yhdysvalloissa (Ohm 2010).

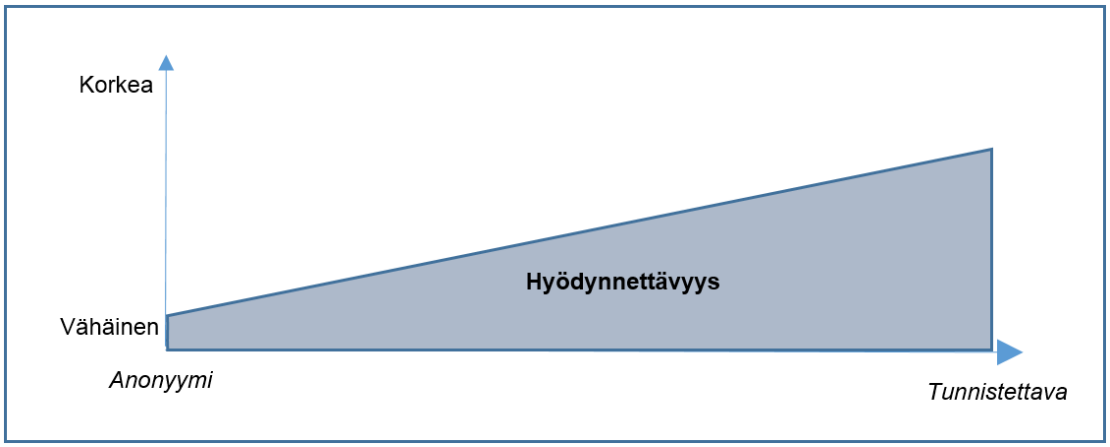
Sittemmin anonymisoitujen datamassojen analysoinnin ympärille on syntynyt tutkija- ja harrastajayhteisöjä, jotka pyrkivät löytämään keinoja siihen, miten anonymisoiduista datamassoista voitaisiin tunnistaa yksilöitä. Nämä tutkijat ovat osoittaneet muun muassa, että 87 % väestöstä voidaan tunnistaa syntymäajan, sukupuolen ja postinumeron avulla, ja yli 80 % suoratoistopalvelu Netflixin käyttäjistä voidaan tunnistaa sen perusteella, miten ja milloin he arvioivat kolme vuokraamaansa elokuvaa (Ohm 2010). Nämä uudelleentunnistustekniikat (engl. *reidentification*) ovatkin ottaneet suuria harppauksia viime aikoina. Massachusetts Institute of Technologyn tutkijat osoittivat arvostetussa Science-lehdessä julkaisemassaan artikkelissa pystyvänsä tunnistamaan muun muassa yksittäisen henkilön tekemät luottokorttiostokset yli 90 % tapauksista noin miljoonan käyttäjän anonymoidusta datamassasta (de Montjoye, Radaelli,

[16] Pseudonymisoinnilla tarkoitetaan henkilön nimen korvaamista jollakin keksityllä nimellä, eli pseudonyymillä. Ero pseudonymisoinnin ja anonymisoinnin välillä on, että anonyymiteetti vaatii kaiken tunnistetiedon poistamista, kun taas pseudonyymit mahdollistavat käyttäjän tunnistamisen, mutta tunnistettavana on vain hänen valeidentiteettinsä (Scott & Orlikowski 2014). Tällainen käytäntö on yleistä esimerkiksi keskustelupalstoilla, joissa käyttäjät kirjoittavat viestinsä käyttäjänimillään eivätkä oikeilla nimillään. On kuitenkin huomioitava, että henkilötietolainsäädännön näkökulmasta myös pseudonymisoitu datamassa on henkilötieto, joka asettaa vaatimuksia rekisterinpitäjälle.

Singh & Pentland, 2015). Tähän tunnistamiseen riitti vain neljän ostotapahtuman päivämäärä ja paikka. Tämä tutkimus sai Scott Berinaton julistamaan Harvard Business Reviewssa, ettei sellaista kuin anonyymi datamassa ole olemassakaan (Berinato 2015).

Anonymisoinnin lisäksi datamassojen yksityisyyttä voidaan myös lisätä rajoittamalla sitä, kenellä on oikeus päästä käsiksi tietoihin ja sillä, mitä tietoja datamassasta jaetaan ja kenelle. Pääsyn rajoittaminen ei täytä anonymisoinnin kriteeriä, mutta rajoittamalla pääsyoikeuksia datamassaan voidaan paremmin kontrolloida, kenelle datamassat päätyvät. Datamassasta voidaan myös jakaa vain pieniä osia eri sidosryhmille. Tällöin kerätystä datamassasta voidaan jakaa vain pieni osa eri tahoille ja vain jonkin tietyn yhteistyökumppanin saataville vastaamaan juuri heidän tarpeitaan. Näillä menetelmillä ei kuitenkaan saada kaikkia hyötyjä datamassasta, sillä usein juuri datamassojen laaja jakaminen mahdollistaa käyttötapoja, joita minkään yksittäisen tahon olisi vaikea tai jopa mahdoton kuvitella.

Datamassan hyödyllisyys ja anonymiteetti näyttäytyvät kahtena vastakkaisena tekijänä. Data voi olla joko täydellisen anonyymiä tai hyödyllistä, muttei samanaikaisesti kumpaakin (Ohm 2010). Toisin sanoen mitä enemmän poistamme tietoja datamassasta, sitä vähäisemmäksi sen hyödyllisyys näyttäisi tulevan. Täysin satunnainen datamassa on erittäin anonyymiä, mutta hyvin vähän hyödynnettävissä (ks. kuva 5).



Kuva 5: Datan hyödynnettävyys vs. anonyymius.

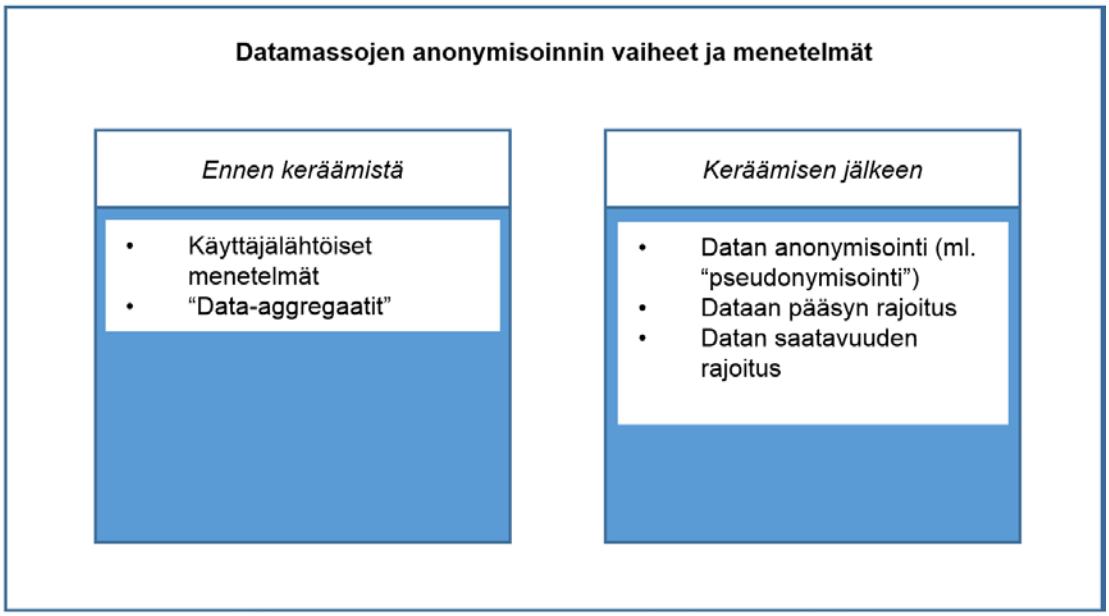
Edellä kuvatussa anonyymius on aina jotakin, jonka palvelun tuottaja tarjoaa – oli sitten kyseessä verkkokauppa tai lääkäripalvelu. Näissä tapauksissa datamassa ensin kerätään ja vasta sen jälkeen anonymisoidaan. Voidaan kuitenkin tunnistaa myös toinen tapa, jolla datamassojen anonyymiys voidaan saavuttaa. Näissä tapauksissa anonymisointi tapahtuu jo *ennen* kuin tieto tallentuu palveluntarjoajalle ja muodostaa datamassan. Tällöin palveluntarjoaja ei pysty itse vaikuttamaan samalla tavalla siihen, mitä tietoja käyttäjästä kerätään.

Käyttäjät voivat itse vaikuttaa siihen, onko heistä kerättävä tieto yksilöitävissä heihin. Erilaiset anonymisointityökalut ja -palvelut tarjoavat käyttäjille rajattua anonymiteettiä. F-Securen tuottama Freedome[17] tai Tor-työkalut[18] ovat esimerkkejä tällaisista tekniikoista. Näiden palveluiden ja työkalujen ajatuksena on, että käyttäjän liikenne kulkee yhden tai useamman liikennepisteen kautta, ja usean käyttäjän liikenteen kulkiessa saman liikennepisteen kautta yksittäistä käyttäjää on vaikea tunnistaa. Tässä mielessä nämä toimivat samankaltaisesti kuin *data-aggregaatit.* Data-aggregoinnilla tarkoitetaan joko automaattisesti tai manuaalisesti tehtävää tiedon yhdis-

[17] Ks. https://www.f-secure.com/fi_FI/web/home_fi/freedome

[18] Ks. https://www.torproject.org/

tämistä niin, että yksilöitä koskeva tieto häivytetään yhdistämällä tieto osaksi laajempia yhteenvetoja tai vähentämällä tiedon tarkkuutta yksittäisistä käyttäjistä käyttäjäryhmiin. Näin yksittäisen henkilön ostokset tai terveystiedot eivät enää näy yksittäisinä tietoina, vaan ovat osa yhteenvetoa esimerkiksi ostoksista, jotka on tehty tietyssä kaupungissa tai kaupunginosassa. Tekniikkaa voidaan käyttää esimerkiksi älykkäiden sähköverkkojen osalta niin, että sähkön hinnoitteluun vaikuttavaa kulutustietoa ei kerätä yksittäisten talouksien tarkkuudella, vaan aggregoidaan tieto osaksi koko korttelin kulutusta. Tällaisten tekniikoiden käyttö sopii kuitenkin vain tiettyihin tilanteisiin. Niiden hyödyntäminen käyttäjän tunnistautumista vaativissa palveluissa on rajallista. Lisäksi anonymisointityökalujen ja -palveluiden käyttö vaatii yleensä käyttäjältä harrastuneisuutta ja ne voivat olla monelle käyttäjälle turhan monimutkaisia. Ne voivat myös luoda virheellistä anonyymiuden tuntua tilanteissa, joissa ne eivät sitä tarjoa. On kuitenkin selvää, että anonymisointityökalut ja -palvelut voisivat yleistyessään luoda haasteita nykyisille toimijoille, joiden liiketoimintamalli perustuu yksilöivän tiedon keräämiseen, sen jalostamiseen ja myymiseen. Kuva 6 tarjoaa yhteenvedon datamassojen anonymisoinnin vaiheista ja tekniikoista.



Kuva 6: Anonymisoinnin menetelmiä.

Liiketoimintamallit

Liiketoimintamalliksi kutsutaan yleensä logiikkaa, jolla yritys muuntaa tuotteensa tai innovaationsa rahavirraksi. Vaikka tämä perusajatus on yhtä vanha kuin ajatus liiketoiminnasta, konseptina liiketoimintamalli on kuitenkin tuoreempi. Vasta 90-luvun startup-piireissä termin käyttö alkoi yleistyä. Vastoin sen hetkistä käsitystä, jonka mukaan kaiken verkossa olevan tiedon piti olla ilmaista, alettiin miettiä, miten luoda arvoa digitaalisessa maailmassa (Sako 2012). Sittemmin ajatus liiketoimintamalleista on levinnyt laajemmin yritysten käyttöön. Yksinkertaisimmillaan, liiketoimintamalli viittaa tapoihin, joilla yritys luo ja toimittaa arvoa asiakkailleen (Sako 2012). Liiketoimintamalli toimii siis ikään kuin sidoksena organisaation liiketoimintastrategian ja liiketoimintaprosessien välillä (Al-Debei & Avison 2010).

Liiketoimintamallin voidaan nähdä koostuvan useista osatekijöistä. Nämä osatekijät vaihtelevat hieman eri tutkijoiden välillä. Keskeistä on kuitenkin, että liiketoimintamalli (ks. Chesbrough 2010; Sako 2012; Hartmann ym. 2014)

- määrittelee arvolupauksen (eli asiakkaalle tuotettavan arvon)
- tunnistaa markkinasegmentin
- kuvaa arvoketjun
- määrittelee liikevoiton luomisen mekanismit
- kuvailee yrityksen sijoittumisen arvoketjussa ja/tai ekosysteemissä
- suunnittelee strategian siitä, miten yritys saavuttaa ja ylläpitää kilpailuetua suhteessa muihin.
-

Liiketoimintamallien arviointiin on kehitetty työkaluja. Näiden työkalujen avulla yritys voi arvioida oman liiketoimintamallinsa kestävyyden ja järkevyyden. Hahmottamalla järjestelmällisesti liiketoimintamallinsa yritykset voivat parantaa liiketoimintaansa ja samalla lisätä yrityksen ketteryyttä (Bouwman ym. 2017).

Liiketoimintamallien on usein nähty seuraavan teknologisia innovaatioita (Hartmann ym. 2014). Yritys ensin innovoi teknologisen tuotteen, jonka jälkeen vasta mietitään, miten teknologia käännetään rahaksi. Tällainen toimintatapa on helppo ymmärtää teknologisten tuotteiden, kuten perinteisten matkapuhelinten tapauksessa. Yritys ensin innovoi kilpailukykyisen matkapuhelimen, jonka jälkeen liiketoimintamalli muotoillaan tuotteen ympärille. Tällaisessa toimintamallissa liiketoimintamalli ei usein nouse ongelmaksi. Liiketoimintamallina on yksinkertaisesti myydä tuotetta kilpailukykyiseen hintaan. Älypuhelinten tapauksessa tilanne on kuitenkin huomattavasti monimutkaisempi. Yrityksille ei enää riitä pelkän tuotteen suunnittelu, vaan niiden myynti on riippuvainen myös muista yrityksistä, jotka tuottavat älypuhelinsovelluksia. Älypuhelin ei ole vain pelkkä kiinteä tuote, joka voidaan helposti paketoida, vaan siitä on tullut *alusta*. Se on alusta, jolle muut tuottavat palveluitaan ja jonka arvo kasvaa sen mukaan, mitä enemmän muut tuottavat palveluitaan kyseisen alustan päälle. Tällainen ympäristö vaatii siis myös sen huomioimista, miten muut voivat tuottaa arvoa tätä alustaa hyödyntämällä. Tällaisessa tapauksessa liiketoimintamalli voidaan nähdä myös itsessään innovaationa.

Liiketoimintamallin innovointi tarkoittaa, että yritys järjestelmällisesti muuttaa liiketoimintalogiikkaa, jonka avulla se sekä luo että vangitsee arvoa asiakkaille (Bouwman ym. 2017). Tällöin keskiössä ei ole varsinaisesti uuden tuotteen innovointi, vaan liiketoimintamallin innovointi. Liiketoimintamallin innovoinnilla yritykset pyrkivät siirtymään pois ”punaisesta merestä” (engl. *red ocean*) päästääkseen ”siniseen mereen” (engl. *blue ocean*), kuten Kim ja Mauborgne (2004) kuvaavat. Punaisella merellä tutkijat viittaavat markkinoihin, jotka ovat täynnä kilpailijoita ja joilla toimiminen on erittäin haastavaa. Punaisessa meressä toimivat yritykset kilpailevat usein puhtaasti hinnalla, jolloin myös voittomarginaalit jäävät pieneksi. Sen sijaan strategiaansa uudistamalla yritysten tulisi pyrkiä siniseen mereen, jossa on vain vähän kilpailua ja jonne kilpailijoiden on vaikea päästä. Google on hyvä esimerkki tällaisesta liiketoimintamallin innovoinnista. Alun perin Google toimi puhtaasti hakukoneen tarjoajana. Käyttäjien määrä lisääntyi jatkuvasti, mutta käyttäjien tekemien hakujen avulla oli vaikea tehdä liiketoimintaa. Googlen eräs innovaatio olikin kehittää uusi liiketoimintamalli, joka perustui käyttäjille näytettäviin kohdennettuihin mainoksiin hakujen lomassa. Teknologia oli siis jo pääosin olemassa ja sitä hyödynnettiin jo laajalti – vain liiketoimintamalli piti innovoida. Liiketoimintamallin avulla Google on ”uinut” sinisessä meressä jo useiden vuosien ajan. Tämä liiketoimintamalli nojaa kuitenkin vahvasti käyttäjiä yksilöivän tiedon hyödyntämiseen. Onkin tarpeen tutkia, millaiset liiketoimintamallit mahdollistaisivat datamassojen hyödyt yrityksille ja olisivat myös tasapainossa yksilöiden yksityisyyden suojan kanssa (Tene & Polonetsky 2012).

6.2. Datamassojen nykyiset liiketoimintamallit

Datamassoista on muodostunut yksi keskeisistä organisaatioiden resursseista. Datamassojen rooli organisaation resurssina voi olla kahdenlainen. Voidaan erottaa yritykset, joiden liiketoiminta nojaa suoraan datamassojen hyödyntämiseen, ja toisaalta yritykset, jotka hyödyntävät datamassoja vain välillisesti liiketoiminnan kehittämiseen. Tällaista välillistä hyödyntämistä on esimerkiksi yrityksen henkilöstöhallinnan kehittäminen tai terveydenhoidossa syntyvän jätteen määrän vähentäminen datamassojen avulla (Investopedia 2015). Vaikka näissä tilanteissa datamassat siis edistävät ja tukevat liiketoimintaa välillisesti, ei yrityksen liiketoimintamalli ole suoraan riippuvainen datamassoista.

Datamassoihin pohjautuvien liiketoimintamallien tarkkaa analyysia hankaloittaa niiden luottamuksellisuus. Harva yritys haluaa avoimesti julistaa, miten he kääntävät datamassat rahavirraksi. Tämä on erityisesti ongelmallista, kun puhumme datamassoista ja niiden liiketoimintamalleista. Zuboff (2015) onkin kritisoinut sitä, kuinka usein saamme vasta paljastusten kautta kuulla sen, mitä tietoa meistä on kerätty ja miten sitä on myyty ja käsitelty. Hän käyttää esimerkkinä Googlen kamera-autoja. Nämä autot kiersivät yleisiä teitä ottaen 360°-kuvia Street-view-palvelua varten, jonka avulla kuka tahansa voisi virtuaalisesti ajella samoja katuja ja nähdä samat maisemat. Vasta myöhemmin kuitenkin selvisi, että samalla kun autot kiersivät kaupunkiemme katuja kuvia ottaen, keräsivät autot myös tietoa kaikista WiFi-verkoista ja niiden sijainnista. Joudumme siis usein tyytymään spekulointiin siitä, miten yritykset liiketoimintaa tekevät.

Kuten yllä olevasta esimerkistä ilmenee, liiketoimintamallit ja yksityisyys ovat kiinteästi sidoksissa toisiinsa. Usein ilmaisena mainostetut palvelut ovat vain näennäisesti ilmaisia, sillä ne perustuvat näitä palveluita tarjoavien yritysten harjoittamaan käyttäjien tarkkaan valvontaan (Balkan 2014).

Datamassojen liiketoiminnan toimintatavat

Kuten tässä raportissa on yllä kuvattu, datamassojen kerääminen markkinointitarkoituksiin on eräs keskeisistä liiketoimintamalleista. Tämä pohjautuu ajatukseen siitä, että mitä enemmän tiedämme yksittäisen kuluttajan ostokäyttäytymisestä, sitä tarkemmin voimme kohdentaa mainontaa juuri hänelle. Tällainen kohdennettu markkinointi vetoaa paremmin kuluttajan tunteisiin ja herättää enemmän ostohaluja kuin yleinen, kohdentamaton markkinointi. Tällaisissa tapauksissa liiketoimintaa syntyy toisten yritysten tuotteiden markkinoinnista kohdennetuille käyttäjille. Tämän markkinoinnin ei välittämättä tarvitse olla luonteeltaan kaupallista, vaan se voi myös olla poliittista. Erään johtavan datamassojen analysointiyrityksen, Cambridge Analytican, sanotaan hyödyntäneen yksilöiden tarkkaa profilointia poliittisten päämäärien ajamiseksi. Onkin väitetty, että yrityksellä oli rooli sekä Britannian EU-eroon johtaneessa äänestyksessä että Donald Trumpin valinnassa presidentiksi (Doward & Gibbs 2017). Datamassat eivät siis näissä tapauksissa ole itsessään yrityksen myytävä tuote, vaan liiketoimintamalli perustuu datamassojen louhinnan kautta tehtyyn käyttäjien profilointiin. Steve Faktor (2014) onkin Forbesissa argumentoinut, ettei yrityksen kannata ikinä myydä dataansa. Hän perustelee väitettään sillä, että datan myymisessä piilee aina suuri maineriski. Usein datan myynti on yrityksille vain sivuliiketoimintaa ja kerätyn datan myyminen vastaa sitä, että tekisi töitä jonkin muun yrityksen puolesta. On kuitenkin tilanteita, jossa datan myyminen voi tulla kyseeseen, minkä myös Faktor myöntää.

Erityisesti avoimen hallinnon (engl. *open government*) ideologia on korostanut tarvetta saattaa julkiset tietovarannot laajemman yleisön saataville. Julkishallinnon hallussa olevat tiedot, kuten

terveystiedot, voivat tarjota arvokkaita liiketoimintamahdollisuuksia yksityisille yrityksille. Datamassat ovat siis tällöin itsessään kauppatavaraa. Tällainen toimintatapa on jo laajalti käytössä. Anonymisoidut vakuutustiedot, luottokorttiostokset ja terveystiedot ovat tulleet kauppatavaraksi. Näissä tapauksissa liiketoimintamalli pohjautuu datanomistajien osalta datan myymiseen, ja toisaalta datan ostajat pyrkivät hyötymään datan analysoinnista taloudellisesti. Myös ”esineiden Internet” (engl. *Internet of Things*) tarjoaa lupaavia liiketoimintamahdollisuuksia tällä liiketoiminta-alueella. Esineiden Internetillä tarkoitetaan yleensä perinteisten teknologisten laitteiden (kuten kodinkoneiden, työkalujen, rannetietokoneiden jne.) yhdistämistä Internetiin ja niiden varustamista erilaisilla dataa keräävin sensoreilla. Laitteiden keräämän sensoritiedon välittäjät eli ”Sensing-as-a-Service” -yritykset keräävät ja välittävät eri sensoreiden keräämää tietoa (Perera, Ranjan, Wang, Khan & Zomaya 2015). Tällöin eri organisaatiot voivat kerätä sensoritietoa ympäristöstämme ja välittää niitä toisille yrityksille organisaatiorajojen yli. Sensoreiden jatkuva lisääntyminen siis muuttaa myös fyysistä ympäristöämme jatkuvasti digitaalisempaan muotoon. Jopa vartaloistamme on tullut yhä enemmän tällaisen tiedon lähteitä, kun aktiivisuusrannekkeet ja muut elintoimintojamme ja aktiivisuuttamme mittaavat sensorit ”dataistavat” meidät.

Datamassojen ympärille on kehittynyt liiketoimintaa, joka pohjautuu ajatukseen datan aggregoinnista ja sen välittämisestä. Nämä datan välittäjät (engl. *data brokerage*) toimivat siis ikään kuin keskipisteenä mahdollisimman suurelle määrälle dataa, jota he keräävät useista eri lähteistä. Näin liiketoimintamalli pohjautuu siis ajatukseen datan keräämisestä eri tietolähteistä ja tämän yhdistetyn datamassan (tai sen osien) myymisestä. Vaihtoehtoisesti datamassoja ei myydä, vaan ainoastaan lisensoidaan tai annetaan niihin käyttöoikeus, josta peritään käyttömaksu. Datamassat ovat siis tuote, jota nämä yritykset myyvät, mutta data ei sinällään ole alun perin heidän, vaan datamassat on hankittu useista eri lähteistä yhdistelemällä. Usein kuitenkin näiden yritysten kauppatavarana ovat tarkat tiedot yksilöiden verkko-ostoksista ja online-käyttäytymisestä. Tästä johtuen nämä yritykset perinteisesti toimivat taka-alalla niin, että kuluttajilla on usein vain vähän tietoa niiden toiminnasta tai edes olemassaolosta (Singer 2013).

Näissä edellä kuvatuissa liiketoimintamalleissa käyttäjä itse on passiivinen kohde, josta yritykset keräävät tietoa. Yritykset kuten Datacoup[19] ja Citizenme[20] ovat pyrkineet muuttamaan tätä asetelmaa. Datacoup tarjoaa alustan, jonka kautta käyttäjien on mahdollista kerätä yhteen tietojaan esimerkiksi sosiaalisesta mediasta, pankkipalveluista ja vakuutuksista ja myydä nämä tiedot itse niitä tarvitseville yrityksille. Citizenme toimii hieman vastaavalla tavalla. Sen avulla käyttäjät voivat analysoida omaa online-käyttäytymistään itse keräämänsä datamassan avulla. Sen lisäksi käyttäjille tarjotaan mahdollisuus myydä itseään koskevat datamassat yrityksille, tai käyttäjä voi niin halutessaan vaikkapa lahjoittaa datamassojaan hyväntekeväisyyteen. Näissä palveluissa datamassat siis edelleen sisältävät hyvin yksilöivää ja jopa arkaluonteista tietoa, mutta datan käytön kontrolli säilyy käyttäjällä.

Datamassat itsessään kertovat hyvin vähän ilman niiden jatkojalostamista. Suurten datamassojen jalostamiseen tarvittavien työkalujen ympärille on kehittynyt laaja kirjo eri yrityksiä. Datamassojen jalostamiseen erikoistuneiden yritysten liiketoimintamalli ei pohjaudu sinällään suurten datamassojen omistamiseen tai niiden hankkimiseen, vaan sellaisten työkalujen ja palveluiden tarjoamiseen, joiden avulla muut yritykset voivat prosessoida omistamiaan datamassoja sekä yhdistellä niitä muihin datamassoihin. Tällaisiin yrityksiin lukeutuu muun muassa Trifacta[21], joka tarjoaa ratkaisuja organisaatioon eri lähteistä tulevien datojen muuttamisesta määrämuotoon.

[19] Ks. https://datacoup.com/

[20] Ks. https://www.citizenme.com/

[21] Ks https://www.trifacta.com/

Miten siis anonyymius sopii näihin liiketoimintamalleihin? Kuten aiemmin on todettu, tarkemman datamassan liiketoimintamahdollisuudet ovat paremmat kuin anonymisoidun (Ohm 2010). Lisäksi anonyymiksi kuviteltu datamassa voi osoittautua harhakuvitelmaksi. Erityisesti silloin, jos yksilöivän datamassan hyödyllisyys on suurempi kuin anonymisoidun, on yrityksillä erityisen suuri kannustin yrittää tunnistaa yksilöt anonymisoidusta datamassasta. Lisäksi kilpailu yritysten kesken ajaa helposti yrityksiä pyrkimään kohti yhä yksilöivämpää tietoa, jos asiakkaat sellaista toivovat. Jos on kysyntää, niin usein on myös tarjontaa.

Yksityisyydensuojan ja datamassojen liiketoimintamahdollisuuksien nähdään kulkevan käsi kädessä. Datamassojen arvo näyttäisi pohjautuvan niiden sisältämän tiedon yksityisyyteen. Kuuluisa yksityisyydensuojan puolestapuhuja ja aktivisti Aral Balkan onkin useissa puheissaan todennut nykyisten yksityisyyttä loukkaavien käytäntöjen olevan ensisijaisesti liiketoimintamalleihin liittyviä ongelmia (Balkan 2014; 2015). Hänen mukaansa start up -tyyppinen liiketoimintamalli pohjautuu ajatukseen, jossa jo alkuvaiheessa käyttäjien yksityisyys myydään sijoittajien rahaa vastaan. On siis mielekästä tutkia anonyymien datamassojen hyödyntämistä liiketoiminnassa.

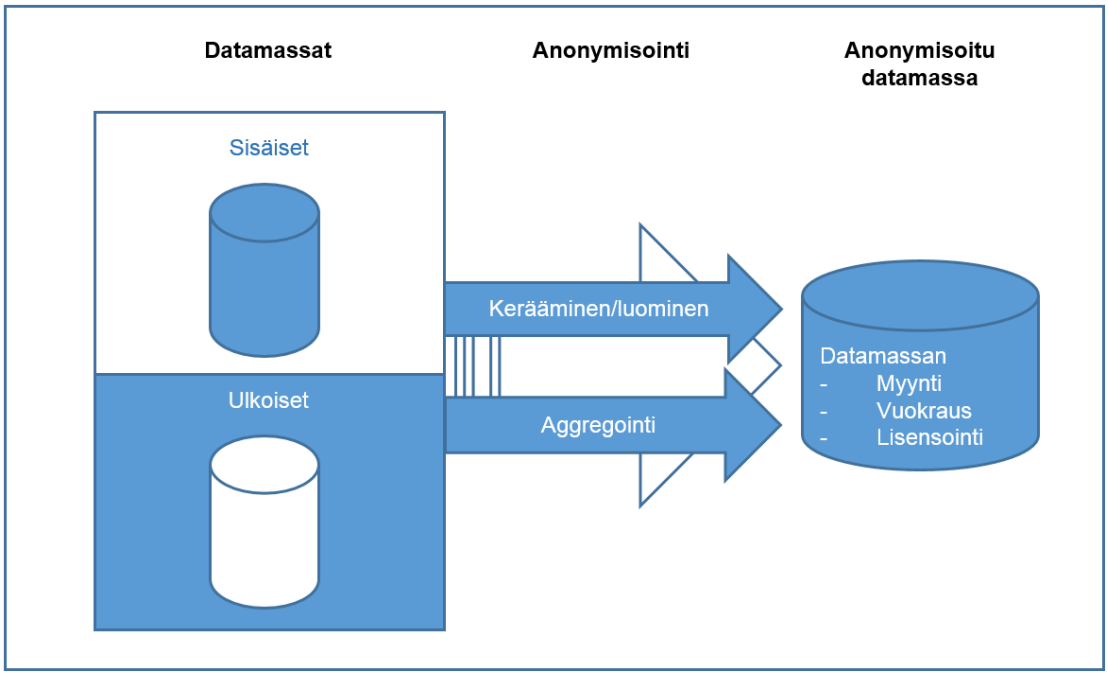
6.3. Anonyymit Datamassat ja Liiketoimintamallit

Datamassojen liiketoiminta voidaan jaotella karkeasti datamassojen myyntiin tai niiden analysointiin. Datamassat voivat olla joko yrityksen itsensä keräämiä tai ulkoisesti hankittuja. Vaikka liiketoiminta näyttäisi usein olevan business-to-busines- myyntiä (B2B), voi se myös olla business-to-consumer- (B2C) sekä myös consumer-to-business-myyntiä (C2B) (Hartmann ym. 2014). Miten nämä liiketoimintamallit suhtautuvat anonyymeihin datamassoihin?

Myös anonyymien datamassojen liiketoimintamallien suhteen voidaan tunnistaa kaksi tapaa tehdä liiketoimintaa. Yritykset voivat tehdä liiketoimintaa joko *anonymisoimalla dataa* tai *hyödyntämällä anonymisoitua dataa*. Seuraavaksi näitä tapoja tarkastellaan tarkemmin.

Liiketoiminta datamassojen anonymisoinnilla

Yritykset, jotka pystyvät keräämään suuret määrät dataa, voivat tehdä liiketoimintaa anonymisoimalla datansa (ks. kuva 7).



Kuva 7: Liiketoiminta datamassojen anonymisoinnilla.

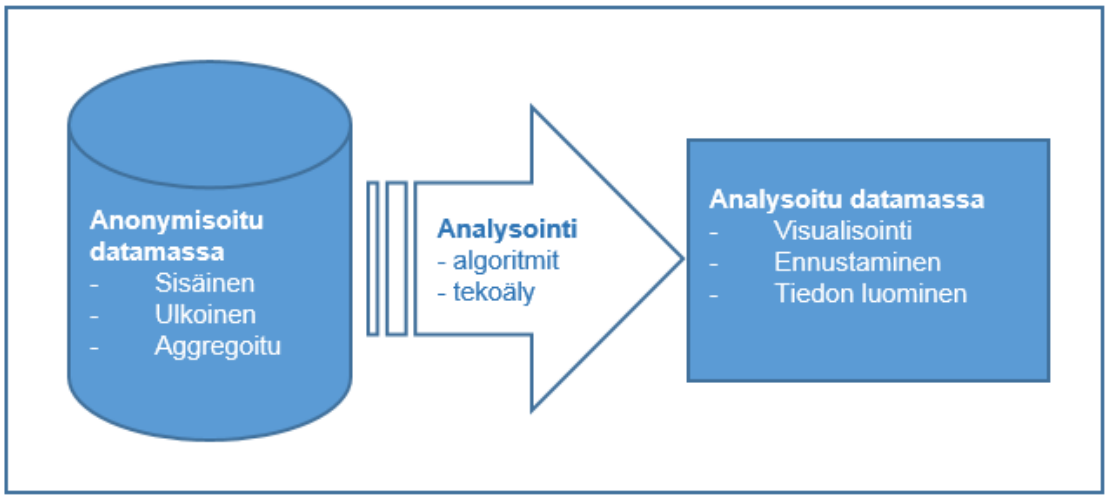
Tällaisia yrityksiä ovat esimerkiksi vakuutusyhtiöt, jotka voivat keräämiensä vakuutustietojen pohjalta luoda myytäväksi anonymisoitua vakuutustietoa. Tämä anonymisoitu datamassa voi olla koostettu yrityksen omista tietolähteistä (kuten vakuutustietokannasta), ostettu ulkopuolelta tai yhdistelmä sekä sisäisiä että ulkoisia tietolähteitä. Anonyymin datamassan liiketoiminnassa voidaan hyödyntää joko datamassan myymistä, vuokrausta tai lisensointia. Kun datamassaa vuokrataan tai lisensoidaan, voidaan datamassaa myydä tilausmaksun maksaneille (esimerkiksi 12 kuukauden käyttöoikeus datamassaan) tai laskuttaa käytön mukaan (esimerkiksi laskutus per käytetty gigatavu). Nämä vuokraukseen ja lisensointiin pohjautuvat mallit sopivat erityisesti datamassoille, jotka muuttuvat ja kasvavat jatkuvasti. Tällöin datamassan ostajalle voidaan tarjota jatkuvasti uutta datamassaa.

Datamassan anonymisointiin perustuvan datamassan liiketoiminnassa datamassan laatu, määrä ja saatavuus ovat kriittisiä. Jos yrityksen myymä datamassa on laadultaan huonompaa tai epätarkempaa kuin kilpailijoilta saatava, voi datamassan myynti olla haasteellista. Myös myytävän datamassan määrä on kilpailutekijä. Jos yrityksellä on hallussaan kilpailijoitaan kattavampi datamassa, se toimii myös kilpailuetuna. Viimeisenä datamassan ainutlaatuisuus on keskeinen tekijä. Jos yrityksen tarjoama datamassa on hyvin ainutlaatuista, eikä sitä ole näin ollen saatavilla muilta toimijoilta, anonymisoidun datamassan myynti voi olla erityisen kannattavaa.

Kuten tässä raportissa on aiemmin todettu, sisältyy datamassan myyntiin kuitenkin aina riskejä liittyen siihen, että anonymisointi voidaan poistaa. Tällaiset tapaukset voivat olla erittäin vahingollisia yrityksen maineelle. Jos anonymisoidun datan myyminen onkin vain sivuliiketoimintaa, tulee yritysten arvioida päätöstään huolella riskianalyysin kautta. Tietyillä datamassoilla voi kuitenkin olla sen rahallista arvoa suurempi yhteiskunnallinen arvo. Tällaisia ovat esimerkiksi terveystietoihin liittyvät datamassat, joiden avulla voidaan löytää ja jopa ennustaa sairauksia. Esimerkiksi tietyn geenin vaikutusta sairauksien syntyyn voidaan tutkia datamassojen avulla, ja sitä kautta datamassalla voi olla suuri yhteiskunnallinen arvo. Tällaiset käytöt tuovat myös esiin anonymisoinnin haittapuolen – jos datamassasta löydetään uutta tietoa sairauksiin liittyen, pitäisikö olla jokin keino, jolla yksilöt voidaan tunnistaa datamassasta niin, että heille voidaan kertoa mahdollisesta sairaudesta?

Liiketoiminta anonymisoidulla datamassalla

Anonymisoitujen datamassojen liiketoiminnassa datamassaa analysoidaan ja näiden analyysien myyminen muille yrityksille muodostaa yrityksen liiketoiminnan. Anonymisoidut datamassat voivat olla siis muualta (kuten edellä kuvatuilta yrityksiltä) ostettuja, tai sitten datamassa voidaan kerätä muuten saatavilla olevista lähteistä yhdistelemällä. Liiketoiminta ei perustu datamassojen myyntiin tai vuokraukseen, vaan siihen, millaisia analyysejä yritys pystyy tuottamaan näistä datamassoista. Yrityksen liiketoiminta on siis riippuvainen siitä, kuinka hyvin yritys pystyy kääntämään datamassat asiakkaalleen merkitykselliseen muotoon. Datamassojen analysointiin perustuvat yritykset voivat visualisoida dataa, tehdä ennustuksia datamassan perusteella tai muuttaa datan tiedoksi (ks. kuva 8).



Kuva 8: Liiketoiminta anonymisoidulla datamassalla.

Datamassoista on vaikea tai mahdoton saada kokonaiskuvaa vain tutkailemalla niiden sisältöä. Datan visualisoinnin avulla miljoonia ja miljoonia tietoja sisältävä datamassa voidaan saada ymmärrettävämpään muotoon. Tällaisen kokonaiskuvan saaminen datamassasta lisää sen hyödyllisyyttä ja tekee siitä helpommin käsiteltävää. Esimerkiksi tietoturvayhtiö F-Secure hyödyntää anonymisoidun datamassan visualisointia globaaleja tietoturvahyökkäyksiä koskevassa esityksessä. Visualisoimalla hyökkäykset kolmiulotteisen karttapallon avulla F-Secure pystyy tarjoamaan koko maailman laajuisen näkymän siitä, missä aktiivisimmat tietoturvahyökkäykset sillä hetkellä tapahtuvat[22]. Näin valtavasta ja jatkuvasti muuttuvasta datamäärästä saadaan selkeitä näkymiä ja voidaan tunnistaa alkavia tietoturvahyökkäyksiä sekä havaita niiden leviäminen. Samalla tällainen näkymä tuottaa anonyymiä palvelua, jossa yksittäiseen käyttäjään tai yritykseen kohdistunut hyökkäys näkyy vain osana visualisoitua datamassaa.

Datamassojen avulla voidaan menneiden tai tämän hetken trendien lisäksi ennustaa myös tulevaa. Tutkijat Liu ym. (2015) ovat osoittaneet sään merkityksen ostokäyttäytymiseen. Yhdistelemällä säätä ja ostokäyttäytymistä koskevia datamassoja tutkijat huomasivat, että huonolla säällä ihmiset ovat aktiivisempia verkko-ostoksissa kuin muulloin. Datamassat siis mahdollistavat uusien kysymysten kysymisen datan avulla, kuten ”miten paljon kokonaismyynti vaihtuu rankkasateella” sen sijaan, että tarkisteltaisiin vaikka vain tietyn kuukauden myyntiä (Chauhan 2015). Vastaavasti yhdistämällä luottokorttiostoksia koskeva anonymisoitu tieto sääennusteeseen voidaan varautua paremmin sään vaikutukseen kysyntään ja tarjontaan (Chauhan 2015).

[22] Ks. http://globe.f-secure.com/

Datamassoja analysoimalla voidaan tuottaa myös muunlaista tietoa kuin visualisointia tai ennusteita. Tällaiset analysoinnit tarjoavat tietoa laajemmista trendeistä ja niiden avulla yritykset voivat varautua paremmin tulevaan. Anonymisoitujen luottokorttitietojen avulla voidaan tarjota tietoa ostokäyttäytymisestä. Voidaan esimerkiksi tunnistaa ostokäyttäytymisestä tiettyjä sekvenssejä, kuten tietoa siitä, miten usein henkilöt kävivät vaateostoksilla ennen kuin tankkasivat autonsa (Chauhan 2015). Tämän lisäksi anonymisoitujen luottokorttiostosten avulla voidaan luoda tietoa siitä, missä kaupunginosissa ihmiset kuluttavat eniten rahaa erityyppisiin ostoksiin. Tällainen tieto voi olla erittäin arvokasta yrityksille, jotka miettivät uuden kivijalkaliikkeen avaamista. Myös matkapuhelinoperaattorit ovat lähteneet mukaan datamassojen hyödyntämiseen. Erityisesti Yhdysvalloissa operaattorit ovat hyödyntäneet keräämiään tietoja siihen, milloin eri ihmisryhmät asioivat kaupoissa. Näin kauppiaat voivat varautua paremmin eri käyttäjäryhmien vierailuun tarjoamalla kävijäryhmälle suunnattuja tarjouksia ja mainoksia vuorokauden ajan mukaan.

Datamassojen analysointi voi pohjautua myös koneoppimiseen ja tekoälyyn. Tämä on erityisesti tarpeen, kun yhdistellään datamassoja eri lähteistä, jotka eivät ole määrämuotoisia. Tekoälyn avulla voidaan datamassaa analysoimalla oppia datasta ilman, että etsitään suoraan vastausta mihinkään ennalta määrättyyn kysymykseen. Kirontech[23] on erikoistunut tämän tyyppiseen anonymisoitujen terveystietojen analysointiin tekoälyn avulla. Tekoälyn avulla yritys on pystynyt tunnistamaan datamassasta harvinaisiin sairauksiin liittyviä piirteitä ja antamaan näiden harvinaisten tautien parempaa tunnistamista ja tehokkaampaa käsittelyä koskevia suosituksia (Kirontech 2017).

Kohti tulevaisuuden liiketoimintamalleja – liiketoimintamallien innovointi

Pärjätäkseen anonyymien datamassojen liiketoiminnassa yritysten täytyy jatkuvasti uudistua. Uudet analysointimenetelmät, avautuvat julkiset datamassat ja mahdollisuudet kerätä täysin uudentyyppistä dataa eivät vain vaadi teknologisia innovaatioita, vaan myös liiketoimintamallien innovointia. Samaan aikaan yritykset joutuvat toimimaan alati kiristyvän tietosuojalainsäädännön puitteissa. Se, minkä uskottiin aiemmin olevan anonyymiä datamassaa, voikin uusien tekniikoiden tullessa olla hyvinkin yksilöivää tietoa. Näin ollen datamassat, jotka nyt ovat sallittuja, voivat tulevaisuudessa olla kiellettyjä tai niiden käyttö voi olla rajoitetumpaa. Näiden haasteiden edessä yritysten tulee jatkuvasti löytää uusia liiketoimintamalleja.

Tutkijat ovatkin kritisoineet yrityksiä siitä, että usein yrityksiltä löytyy kattavat prosessit teknologioiden ja muiden tuotteiden innovointiin, mutta prosessit liiketoimintamallien innovointiin puuttuvat (Hartmann ym. 2014). Yritysten tulisi olla rohkeampia liiketoimintamalliensa suhteen ja yrityksen ja erehdyksen kautta tutkia uusia mahdollisuuksia (Sosna ym. 2010; McGrath 2010; Sako 2012; Chesbrough 2010; Bouwman ym. 2017). Matkimalla muita yrityksiä yritys voi saada liiketoimintamallin. Innovatiivisten liiketoimintamallien kehittäminen vaatii kuitenkin aina kokeilua ja riskinottoa (Sako 2012). Innovointi on välttämätöntä erityisesti liiketoiminta-alueella, joka muuttuu yhtä nopeasti kuin datamassojen liiketoiminta.

Innovaatioille on yleensä tyypillistä se, että niiden ennustaminen on vaikeaa. Sama pätee myös liiketoimintamalleihin, kun lähestymme niitä innovointeina huolellisen ja rationaalisen suunnittelun sijaan. Innovointi voi kuitenkin olla kallista ja hankalaa, erityisesti, jos yrityksen täytyy jatkuvasti muuttaa liiketoimintaansa kokeillessaan uusia liiketoimintamalleja. Innovoidessaan uusia liiketoimintamalleja yritykset voivatkin turvautua liiketoimintamallien stressitestaamiseen

[23] Kts. http://www.kirontech.com/

(Bouwman ym. 2015)[24]. Työkalujen avulla liiketoimintamallien toimivuutta voidaan arvioida tekemättä varsinaisia muutoksia yrityksen toimintaan.

Kaksi laajempaa trendiä näyttäisivät kuitenkin jatkavan vahvistumistaan tulevaisuudessa. Datamassojen koko, reaaliaikaisuus, muutoksen nopeus ja monimuotoisuus tulevat vain lisääntymään siirryttäessä ”Big Datan” aikakauteen. On siis myös odotettavissa, että yritysten, joiden liiketoiminta pohjautuu datamassojen myyntiin, täytyy etsiä uusia datalähteitä ja luoda liiketoimintamalleja, jotka eivät pohjaudu vain datan kertamyyntiin, vaan vuokraamiseen ja lisensointiin. Kun datalähteet lisääntyvät, tulee myös data vääjäämättä monimuotoistumaan, eli sisältämään yhä enemmän strukturoimatonta dataa. Pelkän jäsentelemättömän datan myyminen voi olla tulevaisuudessa kestämätön liiketoimintamalli. Datan jäsentely (engl*. data wrangling*) määrämuotoon tuleekin varmasti lisääntymään tulevaisuudessa avaten uusia mahdollisuuksia siihen erikoistuneille yrityksille[25].

Datamassojen kasvun ja monimuotoistumisen lisäksi on selvää, että tulevaisuudessa tekoälyn rooli datamassojen analysoinnissa tulee olemaan entistä suurempi. Tekoälyn kohdalla korostuvat erityisesti algoritmit, jotka pystyvät oppimaan datasta ja luomaan uutta tietoa ilman, että tarkalleen tiedetään, mitä datamassasta etsitään. Tulevaisuuden voittajat voivatkin löytyä niistä, joilla on parhaat, tehokkaimmat ja älykkäimmät algoritmit datamassojen käsittelyyn ja jotka pystyvät kääntämään näiden algoritmien tuottamat tulokset merkitykselliseen muotoon. Tekoälyä hyödyntämällä on mahdollista löytää jopa uusia liiketoimintamahdollisuuksia. Tällainen datavetoinen liiketoiminnan kehittäminen tarjoaa yrityksille mahdollisuuden uusiin aluevaltauksiin. Myös tässä liiketoimintamalli nousee keskeiseksi – yrityksen täytyy innovoida liiketoimintamalli uuden alueen valtaamiseen ja suunnitella strategia sille, miten saavutettu asema säilytetään.

6.4. Yhteenveto

Tässä luvussa on tarkasteltu anonyymien datamassojen liiketoimintamalleja. Datamassoja liiketoiminnassa hyödyntävät yritykset voivat joko keskittyä datamassojen myyntiin tai niiden analysointiin. Datamassoja myyvät yritykset voivat pohjata liiketoimintansa omistamiinsa datamassoihin (kuten asiakastietoihin, vakuutustietoihin tai vastaaviin), ulkopuolelta kerättyihin (tai luotuihin) datamassoihin tai näiden yhdistelmiin. Datamassoja analysoivat yritykset puolestaan tuottavat datamassoista merkityksellistä tietoa muille yrityksille.

Erityisesti datamassojen myyminen (mukaan lukien vuokraus ja lisensointi) sisältää suuria riskejä tällaista liiketoimintaa harjoittaville yrityksille. Jos anonyymiksi luullusta datamassasta pystytään tunnistamaan yksilöitä, datamassan myynyt yritys voi kärsiä pahan kolauksen. Tämä on erityisen huolestuttavaa, sillä mahdollisuus anonymiteetin purkamiseen näyttää tutkimusten valossa jopa todennäköiseltä. Näin ollen anonyymien datamassojen liiketoimintamallit näyttävät haasteellisilta tai jopa paradoksaalisilta. Jos anonyymejä datamassoja ei ole olemassa (ks. Berinato 2015), niin miten voisi olla myöskään niihin pohjautuvia liiketoimintamalleja? Jotta anonyymien datamassojen liiketoimintamalleja voidaan tutkia, joudutaankin luopumaan vaateesta *absoluuttisen* yksityisyyden suojan osalta. Sen sijaan anonyymius tulee nähdä suhteellisena ja täytyy hyväksyä mahdollisuus siitä, että riittävillä resursseilla ja tietotaidolla on aina mahdollista, että anonymisointi voidaan onnistua purkamaan osittain tai jopa kokonaan. On siis aina mahdollista, että yksittäisiä käyttäjiä voidaan tunnistaa datamassasta anonymisointiyrityksistä huolimatta. Tämä riski voi lisääntyä, kun uusia datamassoja tulee saataville ja mahdolli-

[24] Ks. https://www.businessmakeover.eu

[25] Ks. https://www.trifacta.com/products/wrangler/

suudet yhdistellä näitä datamassoja kasvavat. Datamassojen tulisikin tarjota *riittävä* anonyymiteetti, eli yksilöiden tunnistamisen datamassasta tulisi olla kalliimpaa ja vaatia enemmän resursseja kuin mitä siitä saatu hyöty on.

Tutkimustietoa vasten tarkasteltuna datamassojen vapauttaminen kaupalliseen käyttöön on siis aina riskialtista. Hiljattain toteutetun kyselyn perusteella (Koski & Pajarinen 2016) näyttäisi siltä, että datamassojen hyödyntämistä yrityksissä rajoittaa enemmän tietotaidon puute ja koettu hyöty kuin huoli tietosuojasta. Datamassojen myyminen vaatii kuitenkin yrityksiltä vastuullisuutta ja myös käytäntöjä, joissa datamassojen jakamiseen tarvitaan käyttäjän suostumus – myös silloin, kun kyseessä on anonymisoidut datamassat. Tässä piileekin yksi keskeisistä haasteista: miten kommunikoida käyttäjälle niin, ettei luoda valheellista kuvaa tai anneta liiallisia lupauksia yksityisyydestä, kun lupaa käyttäjältä kysytään? Datamassoja myydessä on vaikea tai mahdoton kuvitella etukäteen kaikkia mahdollisia tapoja yhdistellä tietoa. Lisäksi saatavilla olevien datamassojen määrän lisääntyessä on päätöshetkellä mahdoton tietää, mitä mahdollisuuksia datojen yhdistelyyn tulevaisuus tuo tullessaan. Yritykset joutuvatkin riskianalyysin kautta puntaroimaan saadut hyödyt ja siitä aiheutuvat riskit. Niille yrityksille, joille datamassojen myynti ei ole ydinliiketoimintaa, voivat riskit painaa vaakakupissa enemmän kuin siitä saadut rahalliset hyödyt (Faktor 2014). Datamassojen saatavuudella voi kuitenkin olla myös rahallisen arvon ylittäviä yhteiskunnallisia vaikutuksia. Erityisesti anonyymien terveystietojen tai vakuutustietojen analysointi voi tuottaa tietoa, jolla voidaan tarjota parempaa hoitoa tai estää petoksia (vrt. Kirontech 2017). Yritysten tulisi huomioida myös tämä yhteiskunnallinen merkittävyys, kun hyötyjä ja riskejä arvioidaan. Erityisesti Euroopassa, jossa on herätty datamassojen yksityisyydelle asettamiin haasteisiin, on mahdollista, että yritykset, jotka pohjaavat liiketoimintamallinsa yksilöivään tietoon, tulevat kokemaan haasteita. Lainsäädäntö voi siis ajaa tällaisia yrityksiä siirtymään markkinoille, joissa tietosuojalainsäädäntö on löyhempää. Tässä muutoksessa piilee mahdollisuus vastuullisille yrityksille, jotka ovat rakentaneet liiketoimintamallinsa anonyymien datamassojen hyödyntämiseen tai käyttävät kokonaan muita ratkaisuja liiketoiminnan perustana. Yksi lupaavalta vaikuttava ratkaisu piileekin Omadata-ratkaisuissa (engl. *MyData*), jotka eivät pohjaa anonymisointiin vaan käyttäjän mahdollisuuksiin kontrolloida itseään koskevan datan käyttöä.

Tunnettu tietoturva-asiantuntija Schneier (2010) on väittänyt, ettei yksityisyydessä ole niinkään kyse salassapidosta, kuin käyttäjän mahdollisuuksista kontrolloida tietoaan. Jaamme usein henkilökohtaista tietoa itsestämme ja kerromme ajatuksiamme, mutta haluamme itse päättää milloin, missä ja kenelle näitä tietoja jaamme. Omadatan perusperiaatteet pohjautuvat juuri tälle ajatukselle. Näiden periaatteiden mukaan käyttäjällä tulee olla oikeus (1) tietää, mitä tietoja hänestä on olemassa,(2) nähdä nämä tiedot, (3) oikaista väärät tiedot, (4) nähdä, ketkä henkilötietoja käsittelevät ja miksi, (5) siirtää henkilötiedot eri toimijoille ja antaa lupa niiden käyttöön ja (6) poistaa omat tiedot ja tulla unohdetuksi[26]. Näitä periaatteita noudattamalla myös yritykset voivat hallita datamassojen käyttöön liittyviä liiketoimintariskejä. Kun käyttäjät hallitsevat tietoaan, datan käyttö ja käyttökohteet eivät tule yllätyksenä. Yrityksille on tärkeää vakuuttaa käyttäjät siitä, että datan käytöstä on hyötyä heille joko suoraan tai välillisesti, sillä muuten käyttäjä rajoittaa datan käyttöä tai pyytää poistamaan häntä koskevan tiedon pysyvästi. Vaikka tekniset innovaatiot luovat pohjaa uusille liiketoimintamalleille, ovat menestyksekkäät ja yksilölliset liiketoimintamallit aina itsessään innovaatioita. Yritysten tulisi aktiivisesti seurata teknologisia muutoksia ja etsiä uusia tapoja hyödyntää näitä liiketoiminnassa. Liiketoimintamallien stressitestaustyökalut tarjoavat tärkeän avun nykyisten ja potentiaalisten liiketoimintamallien arvioimiseen. Ne kuitenkin kertovat itsessään hyvin vähän niistä menetelmistä ja prosesseista, joiden avulla yritykset päätyvät tiettyihin liiketoimintamalleihin ja siitä, miten yritysten tulisi organisoitua innovoidakseen uusia liiketoimintamalleja. Liiketoimintamallit syntyvät usein

[26] Omadataan liittyviä mahdollisuuksia tarkastellaan tarkemmin aiemmassa Valtioneuvoston selvityksessä Knuutila ym. (2017).

yritysten ja erehdysten kautta eivätkä suunnittelun tuloksena (McGrath 2010). Tarvittaisiinkin enemmän tutkimustietoa innovointimenetelmistä ja organisaatioiden prosesseista, joiden kautta nämä liiketoimintamallien innovaatiot syntyvät. Ymmärtämällä näitä menetelmiä ja prosesseja voidaan valmiiden ja muilta kopioitujen liiketoimintamallien sijaan luoda organisaatioprosessit liiketoimintamallien innovointia tukemaan. Vain innovaation kautta yritys voi löytää oman liiketoiminta-alueensa ja päästä ”siniseen mereen” (Kim & Mauborgne 2004), jossa kilpailu on vähäistä.

Lähteet

Al-Dabei, M. & Avison, D. (2010). Developing a unified framework of the business model concept. *European Journal of Information Systems,* 19(3), 359–376.

Balkan, A. (2014). *Fee is a lie. The Next Web*. Haettu osoitteesta https://www.youtube.com/watch?v=upu0gwGi4FE

Balkan, A. (2015). *Beyond the camera panopticon*. Haettu osoitteesta https://re-publica.com/en/file/republica-2015-aral-balkan-beyond-camera-panopticon

Berinato, S. (2015). *There's no such thing as anonymous data*. Harvard Business Review. Haettu osoitteesta https://hbr.org/2015/02/theres-no-such-thing-as-anonymous-data

Booth, R. (2014). Facebook reveals news feed experiment to control emotions. *The Guardian*. Haettu osoitteesta https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds

Bouwman, H., Heikkilä, J., Heikkilä, M., Leopold, C. & Haaker, T. (2017). Achieving agility using business model stress testing. *Electronic Markets*, 2017, 1–14.

Chauhan, R. (2015). *Transforming big data into actionable insights*. Mastercard. Haettu osoitteesta https://www.mastercardadvisors.com/_assets/pdf/150513_Transforming_Big_Data.pdf

Chesbrough, H. (2010). Business model innovation: opportunities and barriers. *Long Range Planning,* 43(2-3), 354–363.

de Montjoye, Y-S., Radaelli, L., Singh, V.K., Pentland, A. (2015). Unique in the shopping mall: on the reidentifiability of credit card metadata. *Science*, 347 (6221), 536–539.

Doward, J. & Gibbs, A. (2017). Did Cambridge Analytica influence the Brexit vote and the US election?. *The Guardian*. Haettu osoitteesta https://www.theguardian.com/politics/2017/mar/04/nigel-oakes-cambridge-analytica-what-role-brexit-trump

Euroopan unioni (2016). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Haettu osoitteesta http://eur-lex.europa.eu/eli/reg/2016/679/oj

Faktor, S. (2014). *Never sell data*. Forbes. Haettu osoitteesta https://www.forbes.com/sites/stevefaktor/2014/03/25/never-sell-data/#3d42eaf9259a

Hartmann, P.H., Zaki, M., Feldmann, N. & Neely, A. (2014). *Big Data for Big Business? A Taxonomy of Data-driven Business Models used by Start-up Firms*. University of Cambridge. Haettu osoitteesta http://www.nsuchaud.fr/wp-content/uploads/2014/08/Big-Data-for-Big-Business-A-Taxonomy-of-Data-driven-Business-Models-used-by-Start-up-Firm.pdf

Hyppönen, M. (2017). "*Netin pimeä puoli*", Digital Futures – aloitusseminaari [9.3.2017]. Turun yliopisto.

International Data Corporation (IDC) (2014). *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things*. Haettu osoitteesta https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

Kim, W.C. & Mauborgne, R. (2004). Blue ocean strategy. *Harvard Business Review*, October 2004,. 1–9.

Kirontech (2017). *Healthcare payers*. Haettu osoitteesta http://www.kirontech.com/?q=healthcare-payers

Knuutila, A., Kokkonen, V., Sundquist H., Kuittinen, O., & Thure S. (2017). *MyData muutosvoimana: Julkishallinnon henkilötiedon ihmiskeskeisen hyödyntämisen mallit ja vaikutukset*. Valtioneuvoston selvitys- ja tutkimustoiminta.

Koski, H. & Pajarinen, M. (2016). *Massadatan käyttö ja liiketoimintapotentiaali suomalaisissa yrityksissä. In Massadatasta liiketoimintaa ja tehokkaita julkisia palveluita*. J. Antikainen, J. Eskelinen, H. Koski, T. Niemi, M. Pajarinen, S. Pyykkönen, M. de Vries (toim.). Valtioneuvoston selvitys- ja tutkimustoimikunta.

Levmore, S. & Nussbaum, M.C. (2010). *The offensive internet*. Harvard University Press, Cambridge.

Liu, Y., Kostakos, V. & Li, H. (2015). Climatic effects on planning behavior. *PloS one,* 10(5), 1–9.

McGrath, R.G. (2010). Business models: a discovery driven approach. *Long Range Planning*, 43(2-3), pp. 247-261.

Nath, T. (2015). *How big data has changed healthcare*. Investopedia. Haettu osoitteesta http://www.investopedia.com/articles/investing/042815/how-big-data-has-changed-healthcare.asp

Niemimaa, E. & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. *European Journal of Information Systems*, 26(1), 1–20.

Ohm, P. (2010). Broken promises of privacy: responding to the surprising failure of anonymity. *UCLA Law Review,* 57(6), 1701–1777.

Perera C., Ranjan, R., Wang, L., Khan, S., & Zomaya, A. (2015). Big Data Privacy in the Internet of Things Era. *IT Pro,* 17(3), 32–39.

Sako, M. (2012). Technology strategy and Management: Business Models for strategy and innovation. *Communications of the ACM,* 55(7), 22–24.

Schneier, B. (2010) *Google and Facebook's Privacy Illusion*. Forbes. Haettu osoitteesta https://www.forbes.com/2010/04/05/google-facebook-twitter-technology-security-10-privacy.html

Scott, S. & Orlikowski, W. (2014). Entanglements in practice: performing anonymity through social media. *MIS Quarterly,* 38(3), pp. 873-893.

Singer, N. A data broker offers a peek behind the curtain. *The New York Times*. Haettu osoitteesta http://www.nytimes.com/2013/09/01/business/a-data-broker-offers-a-peek-behind-the-curtain.html

Smith, H.J., Dinev, T. & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly*, 35(4), 989–1015.

Sosna, M., Trevinyo-Rodríguez, R.N. & Velamuri, S.R. (2010). Business model innovation through trial-and-error learning: the Naturhouse case. *Long Range Planning*, 43(2-3), 383–407.

Sweeney, L. (2002). k-Anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems,* 10(5), 557–570.

TechCrunch (2010). Eric Schmidt: *Every 2 days we create as much information as we did up to 2003*. Haettu osoitteesta https://techcrunch.com/2010/08/04/schmidt-data/

Tene, O. & Polonetsky (2012). Privacy in the age of big data: a time for big decisions. *Stanford Law Review Online*, 64(2012), 63–69.

Ziberman (2003). *Zettascale linguistics*. Haettu osoitteesta http://itre.cis.upenn.edu/~myl/languagelog/archives/000087.html

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75–89.

LUKU 7.

Palvelut piilevien tietoturvariskien hallintaan

Haukola Timo

Pitkänen Jari

Turunen Samu

Digitalisaation myötä organisaatioihin kohdistuvat tietoturvauhkat ovat monitahoisemmiksi. Organisaatiot altistuvat hyökkäyksille aiempaa useammin, sillä teknologian ja tietojärjestelmien hyödyntämisen ja käytön yleistyessä myös vihamielisten tahojen hyödyntämien hyökkäysreittien lukumäärä kasvaa (Choo 2011; SANS 2016a; NIST 2016). Teknologian monimutkaisuuden kasvu näkyy myös 2000-luvulla räjähdysmäisesti lisääntyneessä kyberrikollisuudessa, joka on yhä enenevässä määrin ammattimaisesti organisoitunutta. Taustalla vaikuttavilla pimeillä markkinoilla liikkuvat rahamäärät mitataan miljardeissa. (KPMG LLP 2016.)

Tietoturvariskejä ennaltaehkäistään tyypillisesti laatimalla tietoturvakäytäntöjä ja varmistamalla niiden noudattaminen (Puhakainen & Siponen 2010). Niin sanotuille piileville riskeille on kuitenkin ominaista, ettei niitä tiedosteta tai havaita, ennen kuin on liian myöhäistä. Ainoastaan ennaltaehkäisevä toiminta (esim. tietoturvakäytäntöjen laadinta) ei ole riittävää ja huoli piilevistä riskeistä on kasvanut (SANS Infosec Reading Room 2016).

Tässä raportissa piilevällä tietoturvariskillä tarkoitetaan palveluun kohdistuvan uhan elinkaaren ensimmäisiä vaiheita, joissa uhan aiheuttamaa riskiä ei ole vielä havaittu tai se on havaittu vain yksittäisen toimijan taholta, ja se ei ole yleisesti tiedossa. Piilevä riski muuttuu tunnetuksi, kun sen aiheuttava haavoittuvuus julkaistaan julkiseen levitykseen tai se havaitaan muilla keinoin. Haavoittuvuus ja siihen liittyvä riski voivat muodostua inhimillisestä virheestä, tahallisesta toiminnasta tai kolmannen osapuolen toimista. (Arbaugh, Fithen & McHugh 2000; SANS Infosec Reading Room 2016.)

Piilevää riskiä kuvataan usein hyvin epätodennäköisenä tapahtumana, joka toteutuessaan aiheuttaa merkittäviä haittoja ja kustannuksia[27]. Piilevien riskien yleistyminen ei näy ainoastaan julkishallinnossa ja yrityskontekstissa, vaan myös kuluttajat Euroopan unionin alueella ovat havahtuneet vaaraan: useat Eurobarometriin (TNS opinion & Social 2015) vastanneet ovat muuttaneet käyttäytymistään tietoturvauhkien johdosta. Piileviä tietoturvariskejä ovat esimerkiksi vihamielinen taho yrityksen verkon sisällä (SANS Infosec Reading Room 2016), organisaation omasta toiminnasta aiheutuva uhka (valtiovarainministeriö 2008), erilaiset rootkit- ja bottiverkkotartunnat (US-CERT 2011), haittaohjelmat salatussa kanavassa (kuten HTTPS-liikenne, TOR ja SSH (SANS Institute 2013), tiedostojen sisään piilotetut haittaohjelmat, kohdistetut ja kehittyneet pitkäkestoiset hyökkäykset (engl. *Advanced Persistent Threat, APT*), piilopalvelimet, monitoimikoneet (kuten tulostimet ja faxit) ja tiedostojen metatietojen sisältämä luottamuksellinen aineisto (SANS Infosec Reading Room 2016). Piileviä riskejä ovat myös esimerkiksi niin kutsutut nollapäivähaavoittuvuudet (KPMG Sweden 2014; KPMG Finland 2013; KPMG Belgium 2015).

[27] Kirjallisuudessa käytetään myös termiä ”musta joutsen” (Taleb 2007).

Piileviä tietoturvariskejä voidaan havaita hyödyntämällä perinteisiä tietoturvateknologioita, kuten lokien analysointia, hyökkäysten ja haittaohjelmaliikenteen havainnointia sekä poikkeavuuksien analysointia. Uuden sukupolven päätelaitteiden suojausratkaisut sisältävä järjestelmän muutosten ja epäilyttävän toiminnan tai toimintakaavan havainnointia (Filkins & Butler 2016). Kyseisiä teknologioita käytetään myös tarjottaessa niin julkisia kuin kaupallisia tietoturvapalveluita (Forrester 2014a). Tietoturvapalvelut tunnistavat piileviä tietoturvariskejä erilaisten menetelmien avulla, joita ovat mm. automaattinen datan analysointi sekä mahdollisuus aktiiviseen lokitietojen analysointiin ja tarkasteluun. Havainnoinnin mahdollistaa myös verkkoliikenteen aktiivinen seuranta sekä automatisoidusti että manuaalisesti suoritettuna. Tietoturvariskejä tulisi myös voida etsiä aktiivisesti, toisin sanoen käyttäjän tulisi voida ”metsästää” niitä, jotta piileviä riskejä voitaisiin löytää. (SANS Infosec Reading Room 2016)

Kirjallisuudessa ei ole käsitelty piilevien riskien luonnetta, eikä luotu kartoitusta nykyisistä palveluntarjoajista, jotka vastaavat piilevien riskien aiheuttamaan uhkaan. Tämän tutkimuksen tavoitteena on ollut kartoittaa, millaisia kaupallisia ja julkisia palveluita tietojärjestelmien ylläpitäjillä sekä käyttäjillä on piilevien tietoturvariskien 1) havainnoimiseksi, 2) haitallisten vaikutusten arvioimiseksi ja 3) pienentämiseksi tietoa jakamalla. Lisäksi tässä luvussa käsitellään tutkimusten ja asiantuntijahaastatteluiden pohjalta parhaita käytäntöjä olemassa olevien palveluiden yhdistelemiseen. Mitkä ovat parhaita tapoja ehkäistä piileviä riskejä, ja mitkä käytännöt ovat parhaita piilevien riskien ehkäisemiseen erilaisia tietoturvauhkien havainnointiin, vaikutusten arviointiin ja tietojen jakamiseen tarkoitettuja työkaluja ja palveluita hyväksikäyttäen?

7.1. Tutkimuksen toteutus ja rajaukset

Tässä luvussa käsitellään tilanteita, joissa riski on jo realisoitunut ja vihamielisellä taholla on ollut pääsy kohdeverkkoon. Tarkastelun ulkopuolelle jätetään haittaohjelmatartunnat ja hyökkäysten alkuvaiheen havainnointi eri tartuntakanavien kautta. Vihamielisen tahon havaitseminen sisäverkossa eri kanavien valvonnan, kuten Internet-liikenteen monitoroinnin ja verkon sisällä tapahtuvan liikenteen monitoroinnin (monitoring) avulla, otettiin kuitenkin huomioon.

Osana tutkimusta toteutettiin syksyllä 2016 markkinakartoitus havainnointipalveluista Suomessa ja EU:ssa. Markkinakartoituksen kohteiksi valittiin Saksa, Hollanti, Ranska ja Iso-Britannia. Markkinakartoitus laadittiin hyödyntämällä alla olevassa taulukossa kuvattuja tietolähteitä, joiden joukossa on niin kaupallisia kuin julkisia tietokantoja. Hakuja tehtiin kaikissa tietolähteissä (taulukko 7) hakusanoilla: ”hidden risk, hidden information security risk, hidden threats, hidden security ja security services”.

Taulukko: 7 Käytetyt tietokannat.

Lähde	URL-osoite
SANS	http://www.sans.org
KPMG:n globaali verkosto	KPMG:n sisäinen
Google Scholar	http://scholar.google.com
KPMG:n sisäiset tietokannat	KPMG:n sisäinen
Forrester	http://www.forrester.com
Information Security Forum (ISF)	https://www.securityforum.org/
ISACA	http://www.isaca.org
(ISC)²	http://www.isc2.org

Tutkimuksen seuraavassa vaiheessa kartoitettiin tietoturva-alan asiantuntijoita kyselyllä, joka kohdistettiin tietoturvapalveluita tarjoaville yrityksille KPMG Finlandin nimissä. Kyselyn pääasiallinen tavoite oli tunnistaa mahdollisia haastateltavia asiantuntijoita, ja se lähetettiin noin 500

asiantuntijalle. Kyselyssä pyydettiin asiantuntijoiden näkemyksiä ja kommentteja tutkimushaastattelun teemoihin (liite 2). Kartoitukseen vastanneiden henkilöiden joukosta valittiin haastateltavat asiantuntijat ja haastattelut suoritettiin marraskuun 2016 ja tammikuun 2017 välisenä aikana. Haastatteluiden tulokset dokumentointiin ja analysoitiin osana tutkimusta.

7.2. Termien määrittely ja rajaukset

Tässä tutkimuksessa tietoturvauhalla (hazard, threat) tarkoitetaan "haitallista tapahtumaa, joka voi mahdollisesti toteutua, tai useampaa mahdollista häiriötä, jotka tapahtuessaan voivat aiheuttaa sen, että tiedoille, muulle omaisuudelle tai toiminnalle tapahtuu ei-toivottua haittaa". Tietoturvariskillä (information security risk) tarkoitetaan tietoon, tietoliikenteeseen tai tietojärjestelmään kohdistuvaa vahingon vaaraa. Riski muodostuu kahdesta tekijästä: riskin toteutumisen todennäköisyydestä ja vaikutusten laajuudesta riskin toteutuessa. (Valtiovarainministeriö 2008.)

Tietoturvauhan elinkaarella tarkoitetaan tässä raportissa Arbaughin, Fithenin ja McHughin (2000) esittelemää haavoittuvuuden elinkaarimallia, joka muodostuu kuudesta eri vaiheesta: syntymästä (Birth), löytymisestä (Discovery), paljastumisesta laajalle yleisölle (Disclosure), korjauksesta (Correction), julkisuudesta (Publicity), automatisaatiosta (Scripting) ja kuolemasta (Death). Haavoittuvuuden syntymä voi johtua tahattomasta virheestä ohjelman/järjestelmän luonnissa, tai se voidaan luoda tarkoituksellisesti ohjelmaan tai järjestelmään. Tietoturva-aukon löytämisen tai tunnistaminen jälkeen virhettä kutsutaan haavoittuvuudeksi eli uhaksi. Uhan löydyttyä tieto siitä jaetaan yleensä jonkin yhteisön kesken esimerkiksi sähköpostilistojen välityksellä.

Ohjelmistohaavoittuvuudella tarkoitetaan tässä tekstissä ohjelmiston turvallisuudessa sijaitsevaa heikkoutta, jonka avulla vihamielinen taho voi aiheuttaa tappioita tai haittaa ohjelmiston käyttäjälle, ohjelmistolle tai organisaatiolle (Pfleeger & Pfleeger 2002).

Haavoittuvuus voi tulla suurelle yleisölle tiedoksi eri tavoin: Uutisissa saatetaan kertoa julkisuuteen olemassa olevasta haavoittuvuudesta tai jokin uhkiin vastaava taho saattaa julkaista raportin haavoittuvuudesta. Kun tieto haavoittuvuudesta on tullut julkiseksi, ohjelman/järjestelmän kehittäjät tai ylläpitäjät julkaisevat yleensä tietoturva-aukon korjaavan päivityksen. Tässä vaiheessa haavoittuvuuden julkisuutta on enää mahdoton rajoittaa. Haavoittuvuuden elinkaarimallin ”työkaluistamisen” (Scripting) vaihe alkaa, kun uuden haavoittuvuuden hyödyntäminen on mahdollista, mutta vaatii teknistä syväosaamista. Riittävät tekniset taidot omaava hyökkääjä luo haavoittuvuutta hyödyntävän työkalun (Exploit). Näin ollen hän tulee samalla luoneeksi työkalun heille, joilla ei välttämättä ole tarvittavia taitoja hyödyntää haavoittuvuutta ilman työkalua. Tällöin haavoittuvuutta hyödyntävien tahojen määrä laajenee dramaattisesti. Haavoittuvuus ja uhka kuolevat, kun huomattava määrä järjestelmiä ja ohjelmia on vastustuskykyisiä päivitysten ja korjausten ansiosta, mutta käytännössä ylläpitäjät eivät pysty päivittämään ja korjaamaan jokaista järjestelmää ja ohjelmaa täydellisesti (Arbaugh ym. 2000).

Uhkatietojen aktiivisella etsinnällä tarkoitetaan uhkatiedustelua (threat intelligence). Sillä viitataan faktapohjaiseen tietämykseen, johon sisältyvät toimintaympäristö, mekanismit, indikaattorit, päätelmät ja toimintaohjeet jo olemassa oleviin tai nouseviin uhkiin sekä vaaroihin. Tätä tietämystä voidaan käyttää päätöksenteon tukena, kun uhkaan tai vaaraan harkitaan vastatoimia (Gartner 2013).

Uhkatiedon jakamisella (Threat information sharing) tarkoitetaan tässä kontekstissa uhkatiedon jakamista muiden osapuolten kanssa ennalta sovittujen tavoitteiden ja sääntöjen mukaisesti. Organisaatio voi hyötyä uhkatiedon jakamisesta esimerkiksi saamalla tietoonsa muualla

monitoroinnin avulla havaittuja uhkia ja siten varautua omalta kohdaltaan uhkia vastaan (NIST 2016).

Palvelulla tarkoitetaan tässä raportissa ainakin osittain aineettoman hyödykkeen tuottamista asiakkaalle. Tyypillisesti palvelu kulutetaan samanaikaisesti kuin se tuotetaan, jolloin asiakas käyttäessään palveluita osallistuu palvelutapahtuman tuottamiseen. Asiakas saa palvelusta yleensä lisäarvoa esimerkiksi huvin tai hyödyllisyyden kokemuksena (Quinn 1987).

Piilevien tietoturvariskien hallintaan käytettävän palvelun tulee pitää sisällään mahdollisuus arvioida riskien vaikutuksia jo tunnettujen tapahtumien riskien ja asiantuntijuuden avulla. Tässä määritelmässä piilevän riskin haitallisilla vaikutuksilla tarkoitetaan niitä vaikutuksia, jotka riski toteutuessaan aiheuttaa. Haitallisia vaikutuksia tulee pystyä arvioimaan luokittelemalla mahdollisia hyökkäysreittejä ja määrittämällä, keihin ja mihin uhka vaikuttaa haitallisesti. Riskin arvioimiseen tarvitaan myös tieto siitä, kuinka usein riski voi laueta ja kauanko uhka voi kestää. Mahdollisuus tarkastella riskin ajallista kestoa on riskienhallinnan kannalta olennaista, sillä haitallisia vaikutuksia on voinut olla jo ennen riskin laukeamista. Palvelun on tarjottava mahdollisuus selvittää, mistä uhka on lähtöisin. Piilevän riskin alkuperä on tärkeää tietää, jotta esimerkiksi järjestelmävirheen tuottamaan riskiin voidaan kohdistaa korjaustoimenpiteitä (Obrst;Chase;& Markeloff 2012; MITRE Corporation 2012).

Palvelun tulee pitää sisällään mahdollisuus kerätä, jakaa ja hyödyntää havaittujen tietoturvariskien avulla luotua aineistoa. Tarkoituksena on, että jo löydettyjen tietoturvariskien perusteella voidaan tunnistaa vielä havaitsemattomia riskejä. Organisaation sisällä saattaa olla erilaisia järjestelmiä ja käytäntöjä. Tällöin syntyy tarve yksiselitteiselle tavalle viestiä ja jakaa tietoa havaituista riskeistä (Burger, Goodman, Kampanakis & Zhu 2014). Tiedonjakamisen työkaluja voivat olla esimerkiksi erilaiset notaatiokielet, kuten STIX ja IODEF. Notaatiokielen avulla tietoa voidaan levittää tehokkaasti, jolloin esimerkiksi alkava ja tunnistamaton hyökkäys organisaation järjestelmään voidaan tunnistaa ja mahdollisesti torjua (Burger ym. 2014).

Ulkoistamisella tarkoitetaan tässä tutkimuksessa organisaation sisäisten toimien tuottamista ulkopuolisella toimijalla. Tällaisia ovat esimerkiksi pilvipalvelut ja niiden turvaaminen. Ulkoistaminen voidaan toteuttaa ulkoistamalla liiketoimintaprosesseja tai teknologiatoimintoja, kuten tähän tutkimukseen liittyviä tietoturvakontrolleja. Liiketoimintaprosessien ulkoistamisella (Business Process Outsourcing, BPO) tietoturvan alueella tarkoitetaan tilannetta, jossa organisaation IT-infrastruktuuri resursseineen on annettu osittain tai kokonaan ulkoisten toimijoiden hoidettavaksi (Gilley & Rasheed 2000).

Parhailla käytännöillä (best practices) tarkoitetaan tässä tutkimuksessa käytäntöjä, jotka ovat yleisesti hyviksi todettuja tai ainakin parempia kuin muut samalla toimialalla käytössä olevat käytännöt. Tässä tutkimuksessa keskitytään parhaisiin käytäntöihin tietoturvan näkökulmasta.

7.3. Palvelut piilevien tietoturvariskien hallintaan

Euroopan ja Suomen alueilla toimivat yritykset ja julkiset tahot tarjoavat erilaisia palveluita piilevien tietoturvariskien hallintaan. Tässä luvussa käsitellään ensin kirjallisuudesta tunnistettuja palveluita piilevien tietoturvariskien havainnoimiseen, jonka jälkeen käsitellään palveluita piilevien tietoturvariskien haitallisten seurausten arvioimiseen sekä pienentämiseen tietoa jakamalla. Lisäksi luvussa käsitellään kirjallisuudessa tunnistettuja parhaita käytäntöjä tietoturvapalveluiden hyödyntämiseen ja riskin pienentämiseen tietoa jakamalla.

Palvelut piilevien tietoturvariskien havainnoimiseen

Alati kasvavaan uhkamäärään on vastattu tähän mennessä pääosin tehostamalla uhkatiedustelua ja keräämällä näin dataa erilaisista tietoturvauhkista (NIST 2016). Suoraan piilevien tietoturvariskien havainnoimiseen nimettyjä palveluita ei ole tarjolla, mutta niitä on jossain määrin tarjolla olevien tietoturvapalveluiden piirissä. Tämä edellyttää, että niissä käytetään teknologioita, joissa on piilevien riskien havainnointiin tarvittavia ominaisuuksia, ja että ylläpitäjillä on riittävä osaaminen ratkaisujen konfiguroimiseen. Perinteisillä tunnistepohjaisilla ratkaisuilla määritelmän mukaisia piileviä riskejä ei voida havaita.

Forresterin vuoden 2014 tutkimus (Forrester 2014a) listaa palveluntarjoajat, joilla on suurin määrä eurooppalaisia asiakkaita sekä kattavin paikallinen läsnäolo, tuki ja eurooppalaisille asiakkaille tarjolla oleva palvelutarjonta. Tutkimuksen mukaan palvelutarjoajat vastaavat kasvavaan tietoturvapalveluiden kysyntään tarjoamalla erilaisia lokienhallinta-, laitteiden hallinta-, monitorointi-, identiteetinhallinta- ja uhka-analyysipalveluita. Tarjottavat palvelut voidaan kategorisoida kahteen luokkaan: informaatioteknologian ulkoistamispalveluihin (Information Technology Outsourcing, ITO) ja tietoturvaan liittyvien liiketoimintaprosessien ulkoistamispalveluihin (Business Process Outsourcing, BPO).

Informaatioteknologian ulkoistaminen on osa liiketoimintaprosessien ulkoistamista. Yleensä tällaiset prosessit ovat luonteeltaan teknisiä taitoja vaativia (Rohde 2004). Prosessien ulkoistamiseen liittyvät palvelut ovat kattavampia ja edellyttävät kokonaisvaltaisempaa prosessi-integraatiota palveluntarjoajan ja asiakkaan välillä. Esimerkkeinä näistä ovat jatkuva monitorointi, tietovuodon esto, sisäpiiriuhkan havainnointi, tietoturvatapahtumien havainnointi ja hallinnointi sekä uhkatiedustelu (Forrester 2014a). Tällaisia palveluita voidaan kutsua myös tietoturvanhallintapalveluiksi (Managed Security Services, MSSs). Kavanaghin ja Bussan kirjoittamassa Gartnerin raportissa vuodelta 2015 he määrittelevät tietoturvanhallintapalvelut tietoturvallisuuden etähallinnaksi tai -monitoroinniksi, jota asiantuntija ylläpitää ja monitoroi tietoturvanhallintakeskuksesta (Security Operations Center, SOC) (Kavanagh & Bussa 2015). Eurooppalaiset tietoturvanhallintapalveluasiakkaat pitävät Gartnerin raportin mukaan tärkeänä eurooppalaisten toimijoiden käyttämistä. Toinen eurooppalaisten yritysten valintaan vaikuttava seikka on saman raportin mukaan EU:n uusi tietosuoja-asetus, joka asettaa tietoja hallussaan pitävät yritykset vastuuseen tietomurroista (Kavanagh & Bussa 2015).

Julkiset palvelut

Useilla eri EU-maiden CERT-toimijoilla (Computer Emergency Response Team) on yhtenäinen toimintamalli ja palvelutarjonta, vaikka painotukset tarjotuissa palveluissa hieman vaihtelevat maittain. Eri maiden CERT-toimijat ovat usein perustaneet oman NCSA-toiminnon (National Cyber Security Alliance), jonka tehtäviin kuuluu tietoturvaloukkausten ennaltaehkäisy, havainnointi ja ratkaiseminen sekä tietoturvauhkista tiedottaminen. NCSA:t keräävät, analysoivat ja jakavat erilaisia tietoturvauhkia koskevaa tietoa sekä selvittävät kriittiseen kansalliseen infrastruktuuriin kohdistuvia tietoturvaloukkauksia ja -hyökkäyksiä. (Viestintävirasto 2017.) Eri maiden CERT:t toimivat myös aktiivisesti yhteistyössä vaihtaen tietoja keskenään.

Kyberturvallisuuskeskuksen CERT-toiminnon tehtävänä on ennaltaehkäistä tietoturvaloukkauksia ja tiedottaa tietoturva-asioista. CERT-toiminnan puitteissa Kyberturvallisuuskeskus selvittää verkko- ja viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia sekä niiden uhkia. Samalla sen tehtävä on myös kerätä tietoa tietoturvaloukkauksista ja tiedottaa tietoturva-asioista. Haavoittuvuuskoordinointi on yksi Kyberturvallisuuskeskuksen palveluista. Toiminnan tavoitteena on varmistaa yleisten viestintäverkkojen ja viestintäpalveluiden turvallinen ja häiriötön toiminta sekä turvata yhteiskunnan elintärkeät toiminnot. (Viestintävirasto 2016a.)

Saksalainen vastine Kyberturvallisuuskeskukselle on CERT-Bund. CERT-Bundin päätehtävänä on ennaltaehkäistä kriisitilanteita, ja se kerää tietoa uusista tietoturvariskeistä ja analysoi näitä. Virasto myös kehittää ratkaisuja riskien välttämiseksi. Virasto testaa järjestelmiä ja jakaa tietoturvasertifikaatteja sekä toimii yhteistyössä muiden viranomaisten kanssa. Kriisitilanteissa viraston tehtävä on koordinoida kriittisen tieto- ja viestintäliikenteen infrastruktuurin suojelemista yhteistyössä yksityisen sektorin kanssa (The Bundestag 2009).

Yhdistyneen kuningaskunnan CERT on nimeltään CERT-UK. Sen päätehtävinä ovat kansallisten tietoturvaongelmien korjaaminen, kriittisen kansallisen infrastruktuurin suojaaminen yhteistyössä yksityisen sektorin kanssa, koulutus, parhaiden käytänteiden jakaminen ja yleinen tietoturvallisuutta koskeva tiedottaminen sekä toimiminen yhteyspisteenä muiden maiden CERT:ien kanssa (CERT-UK 2014).

Alankomaiden kyberturvallisuuskeskus (NCSC-NL) suorittaa neljää perustehtävää: tietoturvaloukkausten estämistä ja niihin reagoimista, valvontaa sekä tiedottamista. Tiedottamiseen sisältyy myös parhaiden käytäntöjen jakamista. NCSC-NL tarjoaa myös yksityisen sektorin pienille toimijoille ja julkiselle sektorille julkista kyberturvallisuushälytyspalvelua (Ministry of Security and Justice of Netherlands 2015).

Kaupalliset palvelut

Perinteisten tietoturvateknologioiden uusimmat versiot tarjoavat ominaisuuksia, joiden avulla piileviä riskejä on mahdollista havaita. Ominaisuuksia ovat poikkeamien havainnointi, mainetietokannat ja käyttäytymisanalysointi. Esimerkiksi nyt yleistyvät uuden sukupolven virustorjuntaratkaisut (New Generation Antivirus, NGAV) pystyvät havainnoimaan piileviä riskejä tehokkaammin ja näin ennaltaehkäisemään ei-toivottuja tapahtumia. Uuden sukupolven virustorjuntaratkaisut etsivät haitallisia ohjelmia niiden käyttäytymisen perusteella. Tällöin on mahdollista, että ne kykenevät löytämään ja reagoimaan piilevään riskiin ennaltaehkäisevästi (Filkins & Butler 2016).

SIEM-teknologiat (Security Information and Event Management) tarjoavat eri lähteiden lokitapahtumien yhdistelemistä ja analysointisääntöjä poikkeavan käyttäytymisen havaitsemiseksi. Näitä teknologioita tarjoavat palveluina Euroopan alueella useat tietoturva-alan toimijat. Muita tutkimuksessa löydettyjä palveluita ja tietoturvaan liittyviä ulkoistettavia prosesseja on listattu taulukkoihin 8 ja 9.

Kirjallisuudessa yhtenä vaihtoehtona mainittiin uhkien metsästyspalvelut (Threat Hunting) (SANS 2015). Suomenkielinen nimi ei ole vielä vakiintunut käyttöön. Palvelut ovat asiantuntijapalveluita, joiden avulla etsitään organisaatiossa merkkejä verkossa olevista uhista. Palvelun syötteenä tai toimenpiteiden käynnistäjänä käytetään usein uhkatiedustelusta (Threat Intelligence) tai tietoturvakontrolleista saatuja havaintoja tai merkkejä tietomurrosta (IOC). Palvelua tarjoavat tietoturvaan keskittyneet yritykset joko kertaluonteisina tai jatkuvina asiantuntijapalveluina. Palvelusta saadaan paras hyöty, kun asiakkaalla on käytössään havainnointiteknologiaa sekä lokienkeräys- ja analysointiympäristö, kuten SIEM (Security Information and Event Management).

Euroopan unionin alueella toimivat yritykset tarjosivat vuonna 2014 taulukossa 2 esiteltyjä palveluita piilevien riskien hallintaan liittyvien prosessien ulkoistamiseen (BPO):

Taulukko: 8 Prosessien ulkoistamisen palvelut (Forrester 2014a).

1	Tilastollisiin poikkeamiin perustuva kohdennetun hyökkäyksen havainnointi
2	Ohjelmistojen valvonta ja kontrollointi

3	Pilvipalveluympäristön tietoturva
4	Tietovuodon esto
5	Tietoturvatiedon ja -tapahtumien hallinta
6	Tietoturvatapahtumien ja -uhkien analysointi
7	Tietoturvavalvonta
8	Uhkatiedustelu ja tiedottaminen
9	Haavoittuvuuksien hallinta
10	Web-sovellusten suojaaminen

Euroopan unionin alueella toimivat yritykset tarjoavat taulukossa 3 esitettyjä palveluita informaatioteknologian ulkoistamiseen (ITO) piilevien riskien hallintaan:

Taulukko: 9 Teknologian ulkoistamisen palvelut (Forrester 2014a).

1	Pilvestä tarjottava loppukäyttäjän tietoturva
2	Loppukäyttäjän tietoturva
3	Haittaohjelmien hallinta
4	Web-osoitteiden suodatus
5	Hyökkäysten havainnointi ja esto
6	Mobiililaitteiden tietoturva
7	Haittaohjelmien aiheuttaman liikenteen tunnistaminen

Palvelut piilevien tietoturvariskien haitallisten vaikutusten arvioimiseen

Piilevien tietoturvariskien haitalliset vaikutukset voivat olla merkittäviä. Organisaatio voi piilevän riskin realisoitumisen takia kärsiä myös liiketoiminnallisista ongelmista, jotka usein aiheuttavat taloudellista tappiota. Liiketoiminnallisia vaikutuksia aiheuttavat esimerkiksi tietovuodot ja tietosuojan vaarantuminen, jotka voivat aiheuttaa liiketoimintavaikutuksia sanktioiden tai sakkojen muodossa (Goel & Shawky 2009).

Julkiset palvelut

Suomessa Viestintävirasto toimii avustavassa roolissa ja antaa asiantuntija-apua ensisijaisesti huoltovarmuuskriittisille toimijoille vakavissa tilanteissa. Neuvonta sisältää esimerkiksi ratkaisukeinoja tai suosituksen ottaa yhteyttä kaupallisiin tietoturvapalveluihin, kuten esimerkiksi haittaohjelma-analyysi- tai forensiikkapalveluita tarjoavaan yritykseen. Virasto voi myös suositella poliisiviranomaisten puoleen kääntymistä.

Kaupalliset palvelut

Kaupalliset palvelut jakaantuvat konsultointityyppisiin asiantuntijapalveluihin sekä tietoturvariskien vaikutusten etukäteisarviointiin ja tapahtuman jälkeiseen analysointiin. Lisäksi tarjolla on ohjelmistokoodien analysointia ja uhkien metsästystä asiantuntijapalveluna.

Etukäteisarviointi pitää sisällään esimerkiksi riskikartoitukset ja riskienhallintaprosessiin liittyvät asiantuntijapalvelut. Tapahtuman jälkeen tehtävässä analysoinnissa selvitetään, miten laajalle riskiin liittyvät vaikutukset ovat levinneet, mitkä ovat tietoturva- ja liiketoimintavaikutukset ja onko riskiin liittyvät uhkatekijät saatu poistettua. Näihin perustuen hallinnollisiin ja teknisiin kontrollirakenteisiin voidaan määritellä parannusehdotuksia. Ohjelmistokoodin analysoinnilla tutkitaan, miten epäilyttävä tiedosto tai ohjelma käyttäytyy ja minkälaisia ei-toivottuja asioita se mahdollisesti tekisi aktivoiduttuaan. Uhkien metsästyspalvelussa asiantuntija tutkii yrityksen verkkoa ja järjestelmiä etsien merkkejä epäilyttävistä järjestelmämodifikaatioista tai järjestelmien vaarantumisesta hyökkäykselle.

Suomessa toimivat tietoturvaan erikoistuneet yritykset tarjoavat konsultointityyppisiä asiantuntijapalveluita sekä tietoturvariskien vaikutusten etukäteisarviointiin että tapahtuman jälkeiseen analysointiin. Lisäksi tarjolla on ohjelmistokoodien analysointia. EU:n sisällä toimivia kaupallisia tietoturvariskien haitallisten vaikutusten arviointipalveluita tarjoavia yrityksiä on hieman enemmän ja tarjolla on myös edellä mainittuja palveluita.

Palvelut piilevien tietoturvariskien pienentämiseen tietoa jakamalla

Piilevien riskien pienentämiseen voidaan hyödyntää palveluita, jotka jakavat tietoja vallitsevista uhkatekijöistä (Cyber Threat Intelligence), kuten järjestäytyneen rikollisuuden toiminnasta, aktivistien toiminnasta ja teollisuusvakoilussa käytetyistä metodeista. Tietoa jakamalla pyritään vastaamaan seuraaviin kysymyksiin: mitä haittaohjelmia on liikkeellä, mitä haittaohjelmat aiheuttavat ja tekevät sekä miten näiltä haittaohjelmilta tulee ja voidaan suojautua.

Julkiset palvelut

Viestintäviraston Kyberturvallisuuskeskus jakaa tietoa haavoittuvuuksista, eli riskeistä niiden elinkaaren kaikissa vaiheissa. Periaatteena on, että haavoittuvuudet täytyy korjata, korjaukset on saatava kaikkien ulottuville ja ne on myös saatava käyttöön (Viestintävirasto 2015). Kyberturvallisuuskeskus tarjoaa säännöllisesti koosteen haavoittuvuuksista ja uhista. Nämä julkiset tiedot ovat kaikkien tarkasteltavissa (Viestintävirasto 2016a). Euroopan tasolla CERT:ien, kuten Kyberturvallisuuskeskuksen, yhteistyöelin on ENISA. ENISA jakaa tietoa haavoittuvuuksista ja riskeistä ja koordinoi yhteistyötä näiden ongelmien paikantamiseksi, ehkäisemiseksi ja korjaamiseksi. Piilevien tietoturvariskien pienentämiseksi ENISA järjestää myös koulutuksia kyberturvallisuuden kriisinhallintaan sekä julkaisee tutkimuksia ja tekniikoita uhkien torjuntaan. (Euroopan unionin verkko- ja tietoturvavirasto 2016)

Yhdistyneen kuningaskunnan CERT-UK (CERT-UK, 2014), Alankomaiden NCSC (Ministry of Security and Justice of Netherlands, 2015) ja Saksan liittotasavallan CERT-Bund (The Bundestag, 2009) jakavat tietoa piilevien riskien ehkäisemiseen samalla tavoin kuin Suomen kyberturvallisuuskeskuksen CERT-FI.

Organisaatiot voivat jakaa tietoa anonyymisti ISAC-palveluiden (Information Sharing & Analysing Center) kautta. Euroopan unionin verkko- ja tietoturvavirasto (ENISA) tarjoaa ISAC-palvelua lainvalvontaviranomaisille sekä finanssi- ja energiasektorille.

Kaupalliset palvelut

Yksityisen sektorin tarjoamat palvelut tietoturvariskien pienentämiseen tietoa jakamalla jakaantuvat pääosin kahteen osaan, kaupallisiin ja ilmaisiin palveluihin. Kaupallisissa palveluissa asiakas ostaa joko fyysisen tuotteen tai palvelun, jonka ylläpidosta ja ajantasaisuudesta palveluntarjoaja on ainakin osittain vastuussa (Sääksjärvi, Lassila & Nordström 2005). Ilmaisella palvelulla tarkoitetaan tilannetta, jossa asiakas voi käyttää yrityksen tai yhteisön palvelua tai osaa palvelusta ilman rahallista korvausta. Ilmaisen palvelun ylläpidosta, käyttötuesta tai täysimittaisesta käytöstä voidaan kuitenkin periä maksu (Krishnamurthy 2003). Myös joidenkin palveluiden käyttöehtona voi olla käyttötapausten ja havaittujen uhkien jakaminen käyttäjäyhteisön kesken.

Useat kaupalliset palvelut toimivat globaalisti uhkatiedon luonteen takia. Suoraan Suomessa toimivia yrityksiä ei tunnistettu tämän kartoituksen yhteydessä kuin yksi, mutta Euroopan alueella operoivia yrityksiä oli useampia, niin ilmaispalvelujen kuin kaupallisten palvelujen saralla. Maksulliset palvelut keskittyivät asiantuntijatyön ja erilaisten kokonaisten ratkaisujen myymi-

seen. Ilmaispalveluissa itse tuote oli joko osittain tai kokonaan ilmainen, ja vasta tuotteen käyttäminen laajemmassa mittakaavassa tai sen ylläpito ja analysointi ovat maksullisia. Osa ilmaispalveluista ylläpiti vain erilaisia uhkatiedotelistoja, joiden käyttö on ilmaista. Tällöin palvelu ei sisältänyt muuta kuin mahdollisuuden kontribuutioon listan täydentämiseksi ja kasvattamiseksi. Taulukossa 10 on esitetty eräitä tutkimuksessa tarkasteltuja palveluntarjoajia. Taulukkoon on kirjattu palvelun tarjoaja tai palvelu sekä määrittely, onko palvelu maksullinen vai ilmaispalvelu ja onko palvelu tarjolla Euroopassa, Suomessa tai Euroopan ulkopuolella.

Taulukko 10: Kaupallisia ja ilmaisia uhkatietopalveluja tarjoavat palveluntarjoajat.

Palveluntarjoaja	**Kaupallinen**	**Ilmaispalvelu**	**Euroopassa**	**Suomessa**	**Ei EU tai Suomi**
Base System Applied Intelligence	X		X		
Booz Allen	X				X
BrandProtect	X				X
Check Point	X		X	X	
CIRA Blue Heron	X		Ei ilmoitettu	Ei ilmoitettu	Ei ilmoitettu
Crowdstrike	X		X		
Cyveillance	X				X
Digital Shadows	X		X		
DomainTools	X				X
FireEye iSight	X		X		
Flashpoint	X		X		
Hyas Threat Intelligence	X				X
Intel471	X		X		
OpenDNS Umbrella	X		X		
ThreatConnect	X				X
Recorded Future	X		X		
ShadowDragon	X		Ei ilmoitettu	Ei ilmoitettu	Ei ilmoitettu
Symantec	X		X		
TeamGymru	X				X
ThreatGrid	X		X		
ThreatStream	X		X		
Verisign	X		X		
Webroot	X		X		
BT	X		X		
Autoshun		X			USA
Critical Stack Intel		X			USA
C1fApp		X	X		
Cymon		X	X		
Deepviz Threat Intel		X	X		
FireHOL IP List		X	X		
Hail a TAXII		X			USA
I-Blocklist		X			USA
MalwareDomains.com (tarjoaa vain listoja)		X	X		
OpenPhis Feeds		X	X		
PhisTank		X	X		
SSL Blacklist		X	X		
Strongarm by Percient Networks		X			USA
VirusShare (vain listoja)		X			USA
YARA-rules (vain sääntölistoja)		X			Ei ilmoitettu

Parhaat käytännöt tietoturvapalveluiden hyödyntämiseen

Forresterin (2016) tutkimuksessa todetaan, että tietoturvapalveluiden tarjoajat eivät ole täysin lunastaneet lupauksiaan lisäarvon tuottamisesta asiakkaalle. Tutkimuksen mukaan perinteisten tietoturvatalojen palvelutarjonta perustuu pääosin päivittäisten operatiivisten rutiinitehtävien ulkoistamiseen ja tietoturvatapahtumista saatujen havaintojen perusteella tehtäviin analyyseihin sekä kontrollointitoimenpiteisiin. Palvelujen ulkoistamisen ei todettu parantavan tietoturvan kannalta tärkeiden palveluiden muutosnopeutta. Tämän päivän kehittyneisiin uhkaskenaarioihin vastaaminen edellyttää proaktiivista lähestymistapaa ja uhkatiedustelun sekä analytiikan hyödyntämistä. Palveluntarjoajan valinnassa tulee näin ollen painottaa tarjoajan kykyä mukautua ja vastata organisaatioon kohdistuviin todellisiin uhkiin mallintamalla niihin liittyvät skenaariot sekä miettimällä niihin tarvittavat vastatoimet ennakkoon. (Forrester 2016). Poikkeamatilanneanalyyseissä on tarjottava asiakkaalle asiantuntijuutta tilanteen kaikissa käsittelyketjun vaiheissa (arvio tapahtuman relevanssista, asiakkaaseen kohdistuvasta todellisesta riskistä ja tarvittavista vastatoimista). Palveluntarjoajalla on asiakkaaseen nähden etunaan laaja näköala kaikkien asiakkaittensa tietoturvatilanteeseen, ja tarjoajan tulisi osoittaa, että tätä näkemystä ja tietoa pystytään hyödyntämään tehokkaasti asiakkaan poikkeamatapahtumien hallintaan (Forrester 2016).

Forresterin (2016) mukaan palveluntarjoajalta tulisi myös vaatia osoitusta palvelujen jatkuvasta kehittymisestä ja uusien tarvittavien teknologioiden ja toimintatapojen käyttöönottamisesta ja omaksumisesta. Palveluntarjoajalta voidaan esimerkiksi kysyä, milloin se on julkaissut uusia palveluja. Soveltuvuusselvitys (Proof of concept) on hyvä tapa testata palveluntarjoajan lupausten täyttyminen käytännössä. Siihen tulisi sisällyttää todellisia hyökkäys- ja haittaliikenneskenaarioita ja käynti Tietoturvapalveluiden hallintakeskuksessa (Security Operations Center, SOC) (Forrester 2016).

Palveluntarjoajan palveluiden tulisi täydentää asiakkaan omia kyvykkyyksiä, integroitua asiakkaan prosesseihin ja tukea asiakkaan liiketoimintaa. Asiakkaan on syytä hahmottaa oman organisaation nykytilanne ennen palvelujen hankkimista (Forrester 2016).

Asiakkaan tulisi arvioida palvelujen toimivuutta säännöllisesti esimerkiksi penetraatiotestauksen (Penetration test) avulla varmistaakseen, että poikkeamatapahtumat huomataan, niistä raportoidaan ja analyysit ovat kattavia (Forrester 2016).

SANS-organisaatio ehdottaa useita erilaisia parhaita käytänteitä eri toiminnoille. Käytännöt käsittelevät sekä aktiivista uhkatiedustelun implementointia (SANS 2016b), aktiivista uhkatiedustelua ja uhkienetsimistä (SANS 2016c) että ohjelmistoturvallisuuden käsittelyä (SANS 2016d).

Parhaat käytännöt riskin pienentämiseen tietoa jakamalla

Yhdysvaltalaisen National Institute of Standards and Technologyn (NIST) julkaisema opas kyberuhkiin liittyvän tiedon jakamisesta painottaa erityisesti tiedon jakamisen tärkeyttä ja luottamuksen rakentamista. NIST:n mukaan (2016) toiminnan tulee olla ennakkoon suunniteltua, jolloin riskien toteutuessa prosessit ja vastuunjaot ovat selkeitä. Puolustautuvan organisaation tulisi esimerkiksi toimia yhdessä muiden alan organisaatioiden kanssa. Yhteistyössä olisi tarkoitus jakaa tietoa jo tapahtuneista hyökkäyksistä ja havainnoista oman yrityksen sisä- ja ulkoverkoissa yhteistyösopimusten sallimissa rajoissa. Sopimuksessa tulisi sopia, mitä tietoa kerätään ja jaetaan, miten tietoa käsitellään, mitkä ovat vastuualueet sekä miten tieto säilytetään. NIST:n ohjeen mukaan organisaatioiden tulisi käydä läpi laatimansa varautumissuunnitelma noin kahdesti vuodessa ja päivittää se nykyhetkeä vastaavaksi vähintään vuosittain (NIST 2016).

Forresterin vuoden 2014 raportissa esitellään erilaisia yksityisiä palveluita, joiden ansiosta uhkatietoa on tarjolla runsaasti. Analyytikkojen tehtävänä on muun muassa relevantin uhkatiedon poimiminen massasta sekä tietojen laadun varmistaminen ja hyödyntäminen riittävän nopeasti. Yksittäinen tieto ei ole yhtä merkityksellinen eri toimijoille. Valheellinen tai epätarkka tiedon käyttäminen voi johtaa virheellisiin päätöksiin ja toimenpiteisiin tai vähintään resurssien turhaan käyttöön. Ongelmaksi voi myös muodostua se, että saadun tiedon todentaminen oikeaksi ja sen luokittelu ei usein ole mahdollista. Tiedon hyödyntäminen edellyttää kykyä muuntaa tieto tietoturvakontrolleissa ja -monitoroinnissa käytettävissä olevaan muotoon. Kaiken tämän pitäisi tapahtua riittävän nopeasti, jotta uhkatekijät saadaan minimoitua. (Forrester, 2014a.)

Forresterin (2014) raportin mukaan uhkatiedon (Threat Intelligence) hyödyntämiskyvykkyyttä voidaan tehostaa käyttämällä seuraavaa käytäntöä: Rakenna luotettavien toimijoiden ryhmä, hyödynnä uhkatiedon analysointialustoja, jaa tietoa luotettavien toimijoiden kesken ja priorisoi tietoturvaratkaisuja, joihin uhkatieto voidaan integroida joustavasti (Forrester 2014b). Organisaation ei välttämättä tarvitse itse kerätä kaikkea uhkatietoa, vaan organisaatio voi tehdä muiden tahojen kanssa sopimuksia uhkatiedon jalostamista ja jakamista koskien.

Luotettavien toimijoiden ryhmän rakentaminen

Luotettavien toimijoiden ryhmän rakentaminen tulisi aloittaa omista resursseista ja täydentää sitä tarvittavilla ulkoisilla resursseilla. Uhkatekijät ovat usein toimialakohtaisia, ja toimijoiden, jopa kilpailijoiden, välinen uhkatiedon jakaminen olisi suotavaa. Tiedon jakaminen anonyymisti onnistuu esimerkiksi ISAC-palveluiden (Information Sharing & Analysing Center) kautta (Forrester 2014b). ISAC-palvelun tarkoituksena on toimialakohtaisesti kerätä, analysoida ja jakaa uhkatietoa oman järjestönsä jäseniltä jäsenille (National Council of ISACs 2016). Alihankkijat tulisi sisällyttää mukaan tiedonjakoverkostoon (Forrester 2014b).

Uhkatiedon analysointialustojen hyödyntäminen

Tietolähteiden tehokkuutta ja hyödyllisyyttä tulisi arvioida säännöllisesti. Vähäinen määrä merkityksellistä tietoa on parempi kuin suuri määrä vähemmän merkityksellistä tietoa. Analysointialustan tulisi suoriutua uhkaindikaattorien hallinnasta (Forrester 2014b). Uhkaindikaattoreita ovat muun muassa: IP-osoitteet, domain-nimet, SSL-sertifikaatit, tiedostonimet ja rekisteriavaimet. Analysointialustan tulisi tarjota myös työkalut, jotka auttavat analyytikkoa tekemään analyysin uhan vaikutuksista omaan organisaatioon liittyen. Esimerkkejä analysointialustoista on taulukossa 11. Lisäksi organisaatiota tukevat analysointityössä erilaiset sisäiset työkalut kuten Hadoop- tai MongoDB -ratkaisuilla rakennetut datamassan louhintatyökalut.

Taulukko 11: Uhkatiedon analysointialustat (Forrester 2014b).

Analysointialusta	Kyvykkyydet
IBM i2[28]	• Tiedustelutiedon analysointialusta • Tiedustelutietojen yhdistely ja jakelu
LookingGlass ScoutVision [29]	• Tiedustelutiedon analysointi- ja hallinta-alusta
Mitre CRITs (Collaborative Research Into Threats) [30]	• Avoimen koodin alusta • Tiedon jakelu • Tuki tiedonjakoformaateille (CybOX, STIX, and TAXII)

[28] https://www-03.ibm.com/software/products/fi/i2-analyze

[29] https://www.lookingglasscyber.com/products/threat-intelligence-management/scoutvision/

[30] https://www.mitre.org/publications/project-stories/cyber-intelligence-gets-even-smarter-with-crits

	• Tuki kehittäjien omille sovelluksille
Palantir [31]	• Isojen tietomassojen analysointialusta
Paterva Maltego CaseFile [32]	• Tiedustelutiedon visualisointisovellus
Microsoft Advanced Threat Analytics [33]	• Uhka-analyysi
ThreatConnect TC Analyze [34]	• Tiedustelutiedon analysointialusta

Uhkatiedon jakaminen

Uhkatietojen jakamisen ja reaaliaikaisen vastaanottamisen kannalta on tärkeää käyttää luotettavien toimijoiden ryhmää sovittuja standardeja käyttämällä. Standardeja on esitelty tarkemmin taulukossa 12.

Taulukko 12: Uhkatietojen jakamisen standardit (Forrester 2014b).

Standardi	**Kuvaus**
OpenIOC[35]	OpenIOC on laajennettava XML-malli, jonka avulla voidaan kuvata tunnetun tietoturvauhkan tunnusomaisia piirteitä, hyökkääjän käyttämiä menetelmiä tai muita todisteita hyökkäyksestä.
IODEF[36]	IODEF (Incident Object Description Exchange Format) on tiedostomuoto, jota käytetään kuvaamaan tietoturvallisuuteen liittyvää tietoa. Sitä käytetään tiedonvaihtotarkoitukseen eri Computer Security Incident Response Team -organisaatioiden (CSIRT) välillä.
TAXII[37]	Automaattisen luotetun indikaattoritiedon vaihtojärjestelmä TAXII™ (Trusted Automated eXchange of Indicator Information) on Amerikan Yhdysvaltojen Kotimaan turvallisuuskeskuksen (United States Department of Homeland Security, DHS) johtama yhteisöpohjainen tavoite kehittää standardoitu palvelu, jonka avulla tietoturvauhkista ja puolustusmenetelmistä voidaan välittää tietoa eri organisaatioiden ja palveluiden välillä.
STIX[38]	Structured Threat Information Expression (STIX™) on tarkasti jäsennetty kieli, jonka avulla voidaan kuvata uhkatietoa tavalla, joka mahdollistaa tiedon jakamisen, taltioinnin ja johdonmukaisen analysoinnin.
CybOX[39]	Cyber Observable eXpression (CyBOX™) on standardoitu kieli, jonka avulla voidaan täsmällisesti luokitella ja viestiä erilaisista tietoturvaan liittyvistä havainnoista. Havainnot voivat olla dynaamisia

[31] https://www.palantir.com/solutions/intelligence/

[32] https://www.paterva.com/web7/buy/maltego-clients/casefile.php

[33] https://www.microsoft.com/fi-fi/cloud-platform/advanced-threat-analytics

[34] https://www.threatconnect.com/tc-analyze/

[35] http://www.openioc.org/

[36] https://www.ietf.org/rfc/rfc5070.txt

[37] https://taxiiproject.github.io/about/

[38] https://oasis-open.github.io/cti-documentation/

[39] https://cyboxproject.github.io/about/

	tapahtumia tai tämän hetkisiä mittaustuloksia operatiiviselta kyber-alueelta.
Microsoft Active Protections Program (MAPP)[40]	Microsoftin aktiivisen suojauksen ohjelma (The Microsoft Active Protections Program, MAPP) on tietoturvaohjelmistotaloille tarkoitettu ohjelma, joka mahdollistaa niille mahdollisimman aikaisen pääsyn uuteen haavoittuvuustietoon. Tällöin tietoturvaohjelmistotalot voivat reagoida nopeasti uuteen tietoon ja jakaa päivityksiä asiakkailleen, ja näin ollen suojata heidät haavoittuvuudelta.

Viestintävirasto (2016b) esittää kaksi vapaaehtoisuuteen pohjautuvaa käytäntöä: Chatham House -säännön ja Traffic Light Protocol -käsittelyluokituksen. Chatham House -säännön ollessa käytössä kokouksessa kaikki kokoukseen osallistuvat tahot voivat käyttää saamiaan tietoja. Rajoituksena on, että tiedon lähdettä tai muita kokoukseen osallistuneita ei saa paljastaa. (Viestintävirasto 2016b) Traffic Light Protocol -käsittelyluokituksessa pyritään rajoittamaan tiedon jakelua luokittelulla. Yleisimmät neljä luokkaa ovat punainen (henkilökohtainen jakelu), keltainen (rajattu organisaatioiden sisäinen jakelu), vihreä (yhteisön sisäinen jakelu) ja valkoinen (rajoittamaton, tieto voidaan jakaa lainsäädäntö huomioon ottaen) (Viestintävirasto 2016b). Näitä käytäntöjä hyödynnetään useissa Viestintäviraston kansallisissa ja kansainvälisissä kyberturvallisuuden yhteistyöryhmissä. Käytäntöjen tarkoituksena on rohkaista ja edesauttaa eri organisaatioita jakamaan tietoa. Säännöstöissä määritellään jaetun tiedon luokittelu sekä tiedonjakokäytännöt tehdyn luokittelun perusteella (Viestintävirasto 2016b).

Suosi tietoturvakontrolleja, jotka ottavat uhkatietoa vastaan

Tietoturvaan liittyvissä tapahtumissa reagointinopeus on tärkeää. Nopean reagointikyvyn varmistamiseksi uhkatieto tulee olla integroitavissa käytössä oleviin tietoturvakontrolleihin, joita ovat palomuuri, IPS, Proxy, sähköpostin suojaus, sovelluspalomuuri, SIEM ja päätelaitteen turvallisuusratkaisut. Tietoturvakontrolleja valittaessa tulisi suosia ratkaisuja, jotka ottavat uhkatietoa vastaan (Forrester 2014b). Kontrollien teknisen yhteensovittamisen lisäksi kontrolliratkaisujen hallinnan tulisi toimia saumattomasti.

Internet Security Forum:n ohje (ISF 2016) yhdistelee yleisesti tunnetuttuja tietoturvastandardeja. Ohje kuvaa tarvittavat kontrollit käytännönläheisesti tietoturvan hallintamallin suunnitteluun, käyttöönottoon ja ylläpitämiseen.

7.4. Asiantuntijahaastattelut

Tutkimuksen osana haastateltiin seitsemää tietoturva-alan asiantuntijaa lokakuun 2016 ja tammikuun 2017 välisenä aikana. Haastattelut tehtiin teemahaastatteluina, jolloin haastattelu on puolistrukturoitu ja sen kulku rytmittyy teemoittain tiukasti määriteltyjen yksittäisten kysymysten sijaan (Hirsjärvi & Hurme 2001). Haastatteluissa käytetty haastattelurunko ja haastatellut henkilöt on esitetty liitteessä 2. Puolistrukturoituun yksilöhaastatteluun päädyttiin, koska tutkittava aihe oli jo valmiiksi rajattu ja otoksen suuruus pieni.

Puolistrukturoidussa haastattelussa kysymykset ovat kaikille samat, mutta vastauksia ei ole sidottu vastausvaihtoehtoihin, vaan haastateltavat voivat vastata omin sanoin (Eskola &

[40] https://technet.microsoft.com/en-us/security/dn467918.aspx

Suoranta 2000). Hirsijärvi ja Hurme (2001) kutsuvat puolistrukturoitua haastattelua teemahaastatteluksi. Teemahaastattelu eroaa muista haastattelumenetelmistä niin, että siinä edetään tarkkojen kysymysten sijaan ennalta valittujen teemojen varassa. Teemojen avulla haastattelutilanteessa haastateltavan mielipiteet ja näkemykset saadaan esiin ja pyritään minimoimaan haastattelijan näkökulman vaikutus käytettävään aineistoon.

Tässä kappaleessa on esitetty asiantuntijahaastatteluiden tulokset. Ensin käsitellään piilevien tietoturvariskien havainnoimispalveluita koskevat tulokset. Tämän jälkeen käsitellään piilevien tietoturvariskien haitallisten vaikutusten arviointia ja tarkastellaan piilevien tietoturvariskien pienentämistä tietoa jakamalla.

Haastattelujen hyviin käytäntöihin liittyvät tulokset on ryhmitelty tässä luvussa kahteen alilukuun: tietoturvapalveluiden hyödyntämiseen ja uhkatiedon hyödyntämiseen. Uhkatiedon hyödyntämisessä käsitellään haastateltavilta saatuja uhkatiedon hyödyntämisen parhaita käytäntöjä koskevaa tietoa ja sitä, miten uhkatietoa olisi parasta käsitellä ja hyödyntää tehokkaimmalla mahdollisella tavalla. Tietoturvapalveluiden hyödyntämisessä käsitellään haastateltujen käsityksiä siitä, mitkä ovat parhaat mahdolliset tavat erilaisten tietoturvapalveluiden hyödyntämiseen sekä mihin, milloin ja miten niitä tulisi käyttää.

Palvelut piilevien tietoturvariskien havainnoimiseen

Pieniä poikkeuksia lukuun ottamatta palveluita piilevien tietoturvariskien havainnoimiseksi tarjoavat vain yksityiset toimijat. Valtiolliset toimijat tarjoavat pääosin palveluita piilevien tietoturvariskien havainnointiin vain valtioiden huoltovarmuuskriittisille toimijoille.

Piileviä tietoturvariskejä voidaan havaita skannaamalla ohjelmistoista löytyviä heikkouksia. Tarjolla on palveluita, joissa tarkastus voidaan tehdä ohjelmiston kehittäjän tai ostajan toimesta. Kehittäjä voi käyttää palveluita varmistaakseen kolmannen osapuolen ohjelmistokomponenttien tietoturvan. Esimerkkinä tällaisesta palvelusta voidaan pitää suomalaista Codenomicon App Check -palvelua.

Organisaation verkosta (esimerkiksi verkkolaitteet, palvelimet ja työasemat) voidaan havaita piileviä tietoturvariskejä perinteisten tietoturvateknologioiden (SIEM, IDS, FW, päätelaitteiden tietoturvaratkaisut ja liikenteen analysointi) uusimmilla versioilla, joissa on mukana kyvykkyyksiä, kuten poikkeamien havainnointi, mainetietokannat ja käyttäytymisanalysointi. Haittaohjelma-analyysiä voidaan tehdä verkon reunalle asennettavilla automaattisesti toimivilla analysaattorilaitteilla, joille tunnistamattomat tiedostot voidaan ohjata tarkastettavaksi.

Haastateltavat korostivat, että analysaattorilaiteteknologioista saatava hyöty riippuu siitä, miten hyvin laitteet on konfiguroitu ja kuinka hyvin laitteet hälyttävät oikeista asioista. Ylläpitäjillä tulee olla riittävä kompetenssi yllämainittujen teknologioiden automatiikkaan perustuvien havaintojen analysoimiseen ja tarkkuuden lisäämiseen laitteiden konfiguraatioita parantamalla. Mainittuja teknologioita tarjoavat palveluina tietoturvatalot. Erityisesti mobiilisovelluksille on olemassa web-pohjaisia palveluita, joihin voi ladata sovelluksen skannattavaksi. Tällainen palvelu on esimerkiksi Nviso apk.

Piilevien tietoturvariskien haitallisten vaikutusten arviointi

Valtiolliset toimijat tarjoavat edellisessä kohdassa mainitun tavoin palveluitaan tietoturvariskien haitallisten vaikutusten arviointiin pääosin vain huoltovarmuuskriittisille toimijoille. Usein palvelut ovat reaktiivisia ja keskittyvät näin ollen jo menneiden tietoturvatapahtumien vaikutusten

arviointiin. Proaktiiviset julkiset palvelut koostuvat pääosin erilaisista yleisistä tiedonjakotavoista, kuten esimerkiksi sähköpostilistoista ja keskusteluryhmistä. Näissä tiedonjakokanavissa viestitään yleensä uusista uhkista ja niihin varautumisesta.

Yksityiset kaupalliset palvelut ovat julkisia palveluita proaktiivisempia. Palveluita on erään haastateltavan mukaan kahdenlaisia: jo tapahtuneiden tietoturvatapahtumien vaikutusten arviointia ja ennalta tehtävää analyysia. Ennalta tehtävässä analyysissa käydään läpi mahdollisia heikkouksia ja mitä heikkouksien hyödyntämisestä voi mahdollisesti seurata. Koko yrityksen verkon tai järjestelmän läpi käyminen on usein kallista, ja siksi kannattavampaa on keskittyä kriittisiin kohteisiin ja järjestelmiin. Analyysissä etsitään ja seurataan aktiivisesti myös tietoa uusista haittaohjelmista ja haavoittuvuuksista. Tunnettujen haavoittuvuuksien pohjalta voidaan havaita tunnistamattomia haittaohjelmia. Tällöin avainasemassa on asiantuntijoiden oma toiminta ja aktiivisuus.

Piilevien tietoturvariskien pienentäminen tietoa jakamalla

Piilevien tietoturvariskien pienentämiseksi tietoa jakamalla valtiolliset toimijat keskittyvät pääosin jakamaan erilaisia havaintoja ja ilmoituksia uusista ja liikkeellä olevista haittaohjelmista sekä uhista. Viranomaisten välillä on olemassa tehokkaita tiedonjakoverkostoja, joissa jaetaan informaatiota erilaisista tietoturvariskeistä ja -uhista. Myös tiedeyhteisön tekemät tutkimukset ovat yksi haavoittuvuuksien ja haittaohjelmien tiedonlähde.

Yksityisten toimijoiden työntekijät verkostoituvat usein epävirallisesti ja virallisesti ja levittävät näin tietoisuutta erilaisista uhista. Yksittäisen työntekijän henkilökohtainen panostus ympäröivän maailman ja erilaisten tiedonjakokanavien (kuten Internetin keskustelufoorumit ja seminaarit) seuraamiseen ovat avainasemassa tietoturvariskien pienentämisessä. Yksityisille yrityksille on olemassa palveluita, joissa yritys saa omaan profiiliinsa sopivaa uhkatietoa. Saatavaa uhkatietoa hyödyntämällä olisi siis mahdollista proaktiivisesti vastata piileviin riskeihin.

Usea haastateltava mainitsi, että usein yritykset ovat vastahakoisia jakamaan tietoa omista tietoturvatapahtumistaan ja kasvattamaan tietoisuutta uhista verkostossaan. Tätä varten on olemassa yhteisöjä, joiden tarkoituksena on jakaa yritysten omia tietoturvatapahtumia periaatteella ”jos jaat, niin saat”. Toisin sanoen yhteisöihin ei oteta kuunteluoppilaita, vaan kaikkien jäsenten on jaettava tietoa, jotta ne voivat olla yhteisön jäsenenä. Tällöin yrityksen on kerrottava omista tietoturvaloukkauksistaan, jotta muut yhteisön jäsenet jakaisivat omia tietoturvatapahtumiaan.

Tietoturvapalveluiden hyödyntäminen

Tietoturvapalveluiden hyödyntämisen hyväksi käytännöksi mainittiin haastatteluissa erilaisten SOC-palveluiden (Security Operations Center) käyttö. Toinen mainittu oli uhkien havainnointikyvykkyyden parantaminen erilaisten havainnointipalveluiden käytön myötä. Haastatellut asiantuntijat kuitenkin painottivat, ettei valvonta saisi olla liiallista ja haitata organisaation ydintoimintaa tai päivittäistä työntekoa. Tietoa ei tulisi suojata yli tiedon arvon. Toisin sanoen suojaukset tulee suhteuttaa tiedon menetyksestä johtuvan haitan arvoon. Yksi haastateltavista painotti yrityksen oman tietoturvaosaamisen ylläpitämisen merkitystä. Mikäli organisaatio ostaa tietoturvapalvelunsa, voi olla, että palveluntarjoajalla ei ole halukkuutta korjata puutteita ja palveluntarjoaja saattaa kaunistella asiakkaan tilannetta. Osa haastateltavista oli sitä mieltä, että yrityksellä tulisi olla omat tietoturva-asiantuntijansa, jotka olisivat näin sitoutuneempia työhönsä ja organisaationsa turvallisuuteen.

Haastatteluissa nousi esiin myös tietoa jakavien palveluiden hyödyntäminen tietoturvapalveluna: yrityksen on mahdollista tilata tietoturvauhkatiedotteita omaan profiiliinsa sovitettuna. Tällöin yritys saa olennaista suodatettua dataa, eikä yritykselle olennaisia uhkia tarvitse erikseen suodattaa suuresta datamäärästä.

Uhkatiedon hyödyntäminen

Yrityksen tulisi ottaa käyttöön sopiva uhkien hallinnan prosessi ja sille omistettu ryhmä, käyttää luotettavia uhkatiedonlähteitä sekä prosessoida ja analysoida saatava uhkatieto, jotta tieto olisi yrityksen profiilin kannalta mahdollisimman olennaista. Yrityksen tulisi myös haastateltavan mukaan jakaa omaa uhkatietoa ja -tietoisuuttaan oman uskalluksensa rajoissa sekä käyttää erilaisia uhkatiedustelun keskustelualustoja, jotta tietoa voitaisiin tehokkaasti jakaa. On hyvin todennäköistä, että yksittäiseen yritykseen kohdistuvat uhkat eivät ole vain uhan havainneen yrityksen ongelma, vaan sama uhka saattaa kohdistua useaan eri organisaatioon. Toisilta organisaatioilta saadun uhkatiedon avulla on tällöin mahdollista tunnistaa aikaisemmin huomaamattomia uhkia.

Haastateltavien mukaan on olennaista valita oikeat kanavat, joista uhkatietoa otetaan vastaan. Haastateltujen mukaan parhaat käytännöt uhkatiedon hyödyntämiseen eivät ole vielä vakiintuneet ja ne hakevat yhä muotoaan. Yksittäisen organisaation on vaikea analysoida ja seurata kaikkea tarjolla olevaa tietoa, ja olisi hyvä, jos pystyttäisiin käyttämään tahoa, joka analysoi ja käsittelee uhkatiedon valmiiksi ja jakaa sen eteenpäin. Tällaiseksi tahoksi mainittiin esimerkiksi CERT-toimijat. Toinen mainittu keino analysoidun ja käsitellyn uhkatiedon saamiseen ovat erilaiset viralliset ja epäviralliset ammattiverkostot sekä Internet-foorumit. Näissä tietoväylissä eri toimijat jakavat omakohtaisia kokemuksia erilaisista uhkista heille sopivalla tarkkuustasolla. Haastattelujen perusteella kirjallisuuskatsauksessa mainittuja Chatham House -sääntöä ja Traffic Light Protocol -käsittelyluokitusta käytettiin ainakin yhdessä toimialakohtaisessa tiedonjakoryhmässä.

Tärkeimmäksi asiaksi haastateltavat nostivat ”ympäröivän maailman seuraamisen”. Tällä he tarkoittivat yksilön itse suorittamaa uhkatietoon liittyvien kanavien, uutisten, foorumeiden ja muiden keskustelupalstojen havainnointia. Haastateltavat korostivat myös tietoturvan parissa työskentelevien kollegoiden kanssa keskustelua.

7.5. Tulosten yhteenveto

Kirjallisuuskatsauksen ja asiantuntijahaastatteluiden perusteella voidaan todeta, että julkisia palveluita tarjoavat CERT:it ovat palvelutarjonnaltaan hyvin samankaltaisia. Samat neljä peruspilaria toiminnalle löytyvät aineistossa käytetyistä organisaatioista maasta riippumatta. Samojen perustoimintojen etuna ovat selkeästi yhtenäiset toimintatavat, jotka edesauttavat yhteistyön onnistumisen mahdollisuuksia. Erona yksityisen puolen toimijoihin voidaan havaita, että julkiset toimijat tarjoavat palveluitaan omien valtioidensa julkisille organisaatioille, esimerkiksi poliisille ja valtionhallinnolle. CERT:ien toiminta keskittyy erityisesti valtion vakauden ylläpidon kannalta tärkeisiin organisaatioihin. Kirjallisuuskatsauksen ja haastatteluiden mukaan yksityiset yritykset täydentävät tätä omalla tarjonnallaan sekä suuntaavat palvelunsa laajemmin yksityisille markkinoille.

Sekä julkisen että yksityisen sektorin tarjoamat palvelut piilevien riskien ja piilevien tietoturvariskien havaitsemiseen koostuvat lähinnä perinteisistä tietoturvapalveluista ja asiantuntijapalveluista. Perinteiset tietoturvapalvelut keskittyvät piilevien uhkien osalta lähinnä poikkeama-

analysointiin perustuvaan havainnointiin. Julkiset toimijat keskittyvät selkeästi enemmän asiantuntijapalveluihin, sillä heidän resurssinsa tarjota havainnointipalveluita muille kuin oman valtionsa kriittisille toimijoille ovat rajalliset. Tätä kirjallisuuskatsauksen havaintoa tukivat myös asiantuntijahaastattelut.

Tutkimuksessa kartoitetut palvelut piilevien tietoturvariskien haitallisten vaikutusten arvioimiseen jakaantuivat palvelua tarjoavan toimialan mukaisesti. Haastatteluiden ja kirjallisuuskatsauksen pohjalta voidaan todeta, että julkisen sektorin toimijat (esim. Viestintävirasto) keskittyvät pääosin neuvontaan ja erilaisiin ohjeistuksiin. Yksityisen puolen toimijat tarjoavat erilaisia uhkien metsästyspalveluita ohjelmistojen ja järjestelmien tasolla sekä uhkien arviointipalveluita niin etukäteen kuin uhan toteuduttua.

Kirjallisuuskatsauksen ja asiantuntijahaastatteluiden mukaan palvelut, joiden avulla pienennetään piileviä tietoturvariskejä, jakautuivat tutkimuksessa selkeästi kahteen osaan. Julkiset toimijat, kuten CERT-FI, keskittyivät ensisijaisesti jakamaan tietoa erilaisten sähköposti- ja uutiskirjeiden muodossa ja tarjoamalla neuvonta-apua ajankohtaisten haittaohjelmien aiheuttamiin ongelmiin. Yksityisellä puolella toimivien yritysten palvelut tietoturvariskien pienentämiseen tietoa jakamalla koostuivat joko asiantuntija-analyysistä ja teknologiaratkaisuista tai erilaisista uhkalistoista.

Osa haastateltavista oli tietoisia piileviin tietoturvariskeihin liittyvistä parhaista käytänteistä ja osasi nimetä näistä muutamia. Haastateltavista osa painotti laitteiden konfiguraatioiden merkitystä: oikein säädetyt laitteet ovat olennainen osa hyvää tietoturvaa. Haastatteluissa korostettiin myös tietoturvan parissa työskentelevien keskuudessa käytävän vuorovaikutuksen merkitystä ja tietoturvaosaamisen jatkuvan kehittämisen tärkeyttä. Toisaalta myös tuotiin esiin tietoturvaan liittyvien tehtävien vaativuus ja huoli resurssien riittävyydestä.

Kirjallisuuskatsauksessa ja haastatteluissa havaittiin joitakin eroja. Haastatteluissa nousi esiin huoli osaamisen riittävyydestä, jota ei ole teemana kirjallisuudessa käsitelty. Kirjallisuuskatsauksen lopputulos keskittyi enemmän erilaisten palveluiden käytänteisiin ja teknologioihin, kun taas haastattelujen tulokset korostavat diskurssin sekä laitteiden konfiguroinnin ja työntekijöiden ammattitaidon merkitystä. Kirjallisuuskatsauksessa todettiin, että hankinta- ja arvottamiskriteereihin tulisi sisällyttää vaatimuksia koskien muun muassa kompetenssia ja konsultatiivista sisällön tuottamista tapahtumaraportteihin. Haastatteluissa ei löydetty tukea tälle.

Kirjallisuuskatsauksen mukaan organisaatio saa tietojen jakamisesta parhaan hyödyn, kun se rakentaa luotettavien toimijoiden ryhmän, jonka kanssa se jakaa reaaliaikaisesti jaettavaksi katsomaansa tietoa ja hyödyntää saamansa uhkatiedon käsittelyssä analysointialustoja. Relevantti uhkatieto tulee olla integroitavissa käytössä oleviin tietoturvakontrolleihin.

Haastateltavista kolme mainitsi hyvänä käytäntönä liittymisen johonkin tiedonjakokanavaan ja korosti verkostoitumisen (toimialan muiden toimijoiden kanssa) merkitystä. Esimerkiksi Viestintäviraston Kyberturvallisuuskeskus ylläpitää viestintäkanavia muun muassa huoltovarmuuskriittisillä toimialoilla. Organisaation tulisi myös miettiä, mitä tietoa voi itse tuottaa kyseiseen kanavaan ja olla halukas jakamaan muita hyödyttävää tietoa. Tietoa pitäisi myös pystyä jalostamaan liiketoiminnan ymmärtämään muotoon, jotta tarvittaviin tietoturvakontrolleihin saadaan riittävä budjetti.

Sekä kirjallisuuskatsaus että haastattelut tukivat saatua näkemystä luotettavien toimijoiden verkoston rakentamisesta ja tiedon jakamisen tärkeydestä. Haastatteluissa tuotiin lisäksi ilmi tiedon jalostamisen tärkeys liiketoiminnan tarpeisiin tietoturvabudjetin varmistamiseksi. Haastatteluissa kävi myös ilmi, että luotettujen toimijoiden toimialakohtaisia verkostoja on jo olemassa etenkin huoltovarmuuskriittisillä toimialoilla ja niissä käytetään kirjallisuuskatsauksessa

mainittuja tiedonjakamiseen liittyviä käytäntöjä, kuten esimerkiksi Chatham House -sääntöä. Sääntöä käytettäessä kynnys tietojen jakamisen laskee, sillä sääntöä noudattaessa tieto on riisuttu sen jakaneen tahon tiedoista. Tieto on tällöin hygieenistä ja helposti jaettavaa ilman, että sen jakanut organisaatio paljastaa heikkouksiaan suurelle yleisölle.

7.6. Johtopäätöksiä

Haittaohjelmien päätelaitteiden torjuntaratkaisuissa on jo jonkin aikaa ollut lisääntymässä sovelluskontrollointi (Application Control) ja siihen liittyen sallittujen sovellusten tai tiedostojen listat, sekä torjuntaratkaisut, jotka tunnistavat haittaohjelmille tyypillistä käyttäytymistä ja sitä kautta haittaohjelmia paremmin kuin tunnisteisiin perustuvat ratkaisut. Tällöin on todennäköisempää, että piileviä riskejä löydetään ennaltaehkäisevästi eikä ei-toivottuja tapahtumia esiinny luultavasti yhtä usein nykyisen kaltaisena.

Pelkillä teknologisilla ratkaisuilla ei kyetä saamaan tehokkainta mahdollista suojausta: havaintoteknologioiden tehokkuus on verrannollinen niiden havainnointitarkkuuteen ja -herkkyyteen. Olennaista on, että havainnointilaite huomaa juuri halutun kaltaisia tapahtumia, jotka poikkeavat normaalista toiminnasta. Havaintojen analysoinnissa tarvitaan asiantuntijan intuitiota, päättelykykyä ja kokonaisuuden hahmottamiskykyä. Toisin sanoen teknologioita hankittaessa tulisi varmistaa joko itse tai palvelun avulla, että käytettävissä on riittävät resurssit, prosessit ja kompetenssi laitteiden konfigurointia ja hälytysten analysointia varten.

Hankittaessa palveluita piilevien riskien pienentämiseksi tulisi varmistaa, että palveluissa käytetään mainittuja uuden sukupolven teknologioita ja että se täydentää organisaation omaa, mahdollisesti puutteellista reagointi- ja analysointikykyä. Automatiikkaa voidaan käyttää helpottamaan ja mahdollistamaan, mutta ei täysin korvaamaan ihmisen tekemää asiantuntijatyötä.

Huoltovarmuuskriittisille toimijoille valtiolliset instanssit tarjoavat asiantuntijapalveluita ensisijaisesti poikkeamahavaintojen analysointiin ja ratkaisukeinoja käytettävissä olevien resurssien puitteissa. Paljon resursseja vaativissa tilanteissa on käytettävissä kaupallisia tietoturvapalveluita, kuten esimerkiksi haittaohjelma-analyysipalveluita. Rikokseen liittyvissä tapauksissa poliisiviranomainen suorittaa oman tutkinnan. Näihin palveluihin tukeutuvien organisaatioiden tulisi etukäteen varmistaa, että vakavan tietoturvaloukkauksen sattuessa heillä on varmasti käytettävissään tarpeelliset resurssit, prosessit ja yhteistyötahot vaikutusten arvioimiseksi. Tällöin organisaatio kykenee aloittamaan ongelmatilanteesta toipumisen välittömästi tai nopeammin kuin valmistautumattomana.

Kaupalliset palvelut haitallisten vaikutusten arvioimiseksi koostuvat asiantuntija- ja konsultointipalveluista, kuten riskien vaikutusten arvioimisesta etukäteen (riskienhallinta ja ohjelmistokoodin analysointi), piilevien riskien löytämiseen liittyvistä palveluista sekä toteutuneiden riskien vaikutusten analysointipalveluista. Analyysiin tulisi sisältyä myös tietoturva- ja liiketoimintavaikutusten arviointi, juurisyyn selvittäminen ja selvitys siitä, onko tietoturvaloukkauksen aiheuttamat tekijät saatu poistettua. Näiden perusteella voidaan määritellä parannusehdotuksia tietoturvan hallinnollisiin ja teknisiin kontrollirakenteisiin.

Tietojen jakamisessa ensisijaisessa roolissa on viestintä eri organisaatioiden välillä. Julkiset toimijat jakavat tietoa hallitusti suljettujen toimialakohtaisten ryhmien kesken. Asiantuntijaverkostot ovat tärkeitä sekä yksityisten että julkisen sektorin toimijoiden tiedonvälityksen kannalta. Näiden verkostojen lisäksi on tarjolla varsinaisia kaupallisia palveluita, jotka tarjoavat uhkatietoa yrityksen omaan profiiliin ja toimintaympäristöön sovitettuna. Yksittäisten työntekijöiden

muodostamat epäviralliset ja viralliset verkostot muodostavat yksityisille toimijoille yhden tärkeimmistä tiedonjakokanavista. Epäviralliset toimintatavat eivät varmista, että tieto on saatavilla kaikille, ja väärinkäytettynä ne saattavat lisätä luottamuksellisen tiedon leviämistä. Yrityksen tietotaso voi olla riippuvainen yksittäisen asiantuntijan ajankäytöstä ja innostuksesta uhkatiedon hankkimiseen.

Kirjallisuuskatsauksen tulokset osoittavat, että hyviä yleisesti tunnettuja käytänteitä on paljon tarjolla. Käytänteitä tarjoavat muun muassa standardointielimet, tietoturvayhteisöt sekä valtiolliset ja kansainväliset toimijat. Käytänteet kattavat tietoturvan hallintamallin havainnointikykyyn liittyviä osa-alueita, kuten uhkatiedon keräämisen ja hyödyntämisen sekä poikkeamien havainnoinnin. Lisäksi niissä määritellään tarvittavia teknologiaominaisuuksia, prosesseja ja resursseja. Hankittaessa tietoturvan hallintaan liittyvää teknologiaa palveluna palveluntarjoajilta tulisi vaatia jo hankintavaiheessa näyttöä proaktiivisesta tietoturvanhallinnasta ja konsultatiivisesta poikkeamatilanteidenhallinnasta kattavine tapahtumaraportteineen ja toimenpide-ehdotuksineen.

7.7. Yhteenveto

Yleisesti tunnettuja hyviä käytäntöjä kattavan tietoturva-arkkitehtuurin määrittelemiseksi on tarjolla runsaasti. Yleisesti tunnettuja käytänteitä tietoturvapalveluiden hankkimiseen ei löytynyt. Kirjallisuuskatsauksessa kuvattiin tietoturvan ulkoistamiseen liittyviä haasteita ja niistä johdetut käytänteet, joilla parannetaan asiakkaan palvelusta saamaa hyötyä.

Niin alan kirjallisuus kuin tämän tutkimuksen yhteydessä haastatellut asiantuntijat korostivat tietoturva-ammattilaisten välisen viestinnän ja diskurssin merkitystä. Vaikka parhaita käytänteitä on jo runsaasti tarjolla, ne ovat vasta vahvistamassa omaa asemaansa. Tulevaisuudessa parhaisiin käytänteisiin tullaan todennäköisesti lisäämään huomioita viestinnän tärkeydestä eri ammattiryhmien välillä. Tällöin, viestinnän parantuessa, erilaisten ajatusten ja tietolähteiden vaihto tehostuu ja erilaisia ratkaisuja on helpommin tarjolla. Yksi tällainen ratkaisu on käyttää erilaisia tiedonjakotahoja. Olennaista parhaiden käytänteiden jalostumisen kannalta on käydä diskurssia, eikä siilouttaa ja pantata tietoturvaloukkauksia ja tietoa.

Tietoturvan täydellistä automatisaatiota ei voida pitää todennäköisenä, sillä erilaisten laitteiden konfigurointiin ja tietoturvaratkaisujen tekijäksi ja tietoturvapoikkeamahavaintojen analysointiin tarvitaan ajatteleva, ammattitaitoinen ihminen, jolla on kyky ja mahdollisuus kysyä ja keskustella muiden ihmisten kanssa. Tällöin yksittäiseen ongelmaan ja sen vaikutusten analysointiin voidaan saada erilaisia näkökulmia ja ratkaisuja.

Parhaat käytänteet valikoituvat ja jalostuvat vasta pitkällä aikavälillä. Hyvät käytänteet päivittyvät jatkuvasti vastaamaan uusia esiin tulevia tarpeita.

Lähteet

Arbaugh, W. A., Fithen, W. L. & McHugh, J. (2000). Windows of vulnerability: A case study analysis. *Computer*, 33(12), 52–59. doi: 10.1109/2.889093

Burger, E. W., Goodman, M. D., Kampanakis, P. & Zhu, K. A. (2014). Taxonomy model for cyber threat intelligence information exchange technologies. *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*. New York, NY, USA: ACM. doi:10.1145/2663876.2663883

CERT-UK. (2014). *About us*. Haettu 24.8.2016 osoitteesta https://www.cert.gov.uk/what-we-do/

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), 719–731. doi:10.1016/j.cose.2011.08.004

Euroopan unionin verkko- ja tietoturvavirasto. (2016). Perustiedot. Haettu 30.7.2016 osoitteesta https://europa.eu/european-union/about-eu/agencies/enisa_fi

Eskola, J. & Suoranta, J. (2000). *Johdatus laadulliseen tutkimukseen*. Tampere: Vastapaino.

Forrester. (2014a). Market overview: Managed security services, Europe, Q2 2014, Forrester Research. Haettu 23.8.2016 osoitteesta https://www.forrester.com/report/Market+Overview+Managed+Security+Services+Europe+Q2+2014/-/E-RES111021

Forrester. (2014b). *Four Best Practices To Maximize The Value Of Using And Sharing*. Cambridge: Forrester Research, Inc.

Forrester. (2016). *Get Your Managed Security Services In Order*. Forrester.

Filkins, B. & Butler, J. M. (2016). SANS Reading Room. Haettu 3.1.2016 osoitteesta https://www.sans.org/reading-room/whitepapers/analyst/old-new-replacing-traditional-antivirus-37377

Gartner. (2013). Definition: Threat Intelligence. (Gartner.) Haettu 9.9.2016 osoitteesta https://www.gartner.com/doc/2487216/definition-threat-intelligence

Gilley, K. M. & Rasheed, A. (2000). Making more by doing less: an analysis of outsourcing and its effects on firm performance. *Journal of management*, 26(4), 763–790. doi:10.1016/S0149-2063(00)00055-6

Goel, S. & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, 46(7), 404–410. doi:10.1016/j.im.2009.06.005

Hirsjärvi, S. & Hurme, H. (2001). *Teemahaastattelu: teemahaastattelun teoria ja käytäntö*. Helsinki: Yliopistopaino.

ISF. (2016). *The Standard of Good Practice for Information Security 2016*. Information Security Forum.

Kavanagh, K. M. & Bussa, T. (2015). *Magic Quadrant for Managed Security Services, Worldwide. Gartner*. Haettu 12.1.2017 osoitteesta https://www.gartner.com/doc/reprints?id=1-2X0FZEY&ct=160125&st=sb

KPMG Belgium. (2015). *Unknown Threat in Belgium*. KPMG. Haettu 26.8.2016 osoitteesta https://www.kpmg.com/BE/en/IssuesAndInsights/ArticlesPublications/Documents/ADV-cyber-security-study-brochure.pdf

KPMG Finland. (2013). *Unknown Threat in Finland*. KPMG Finland. Haettu 26.8.2016 osoitteesta https://www.kpmg.com/FI/fi/Ajankohtaista/Uutisia-ja-julkaisuja/Neuvontapalvelut/Documents/unknown-threat-in-finland.pdf

KPMG LLP. (2016). *Taking the offensive: Disrupting Cyber Crime*. Haettu 26.8.2016 osoitteesta http://www.resourcesbt.com/resources/files/quicklinks/taking_the_offensive_disrupting_cyber_crime_24802.pdf

KPMG Sweden. (2014). *Unknown threats in Sweden*. Haettu 26.8.2016 osoitteesta https://www.kpmg.com/SE/sv/kunskap-utbildning/nyheter-publikationer/Publikationer-2014/Documents/Study-report-UnknownThreats-in-Sweden.pdf

Krishnamurthy, S. (2003). *An Analysis of Open Source Business Models*. University of Washington, Bothell. Noudettu osoitteesta https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=650001

Ministry of Security and Justice of Netherlands. (2015). *What is the NCSC?* Haettu 24.8.2016 osoitteesta National Cyber Security Centre: https://www.ncsc.nl/english/organisation

MITRE Corporation. (2012). *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™).* Haettu 18.8.2016 osoitteesta Mitre Tenhnical Papers: http://www.standardscoordination.org/sites/default/files/docs/STIX_Whitepaper_v1.1.pdf

National Council of ISACs. (2016). *ABOUT ISACs*. Haettu 9.5.2017 osoitteesta https://www.nationalisacs.org/about-isacs

NIST. (2016). *Guide to Cyber Threat Information Sharing*. U.S. Department of Commerce. doi:10.6028/NIST.SP.800-150

Obrst, L.;Chase, P. & Markeloff, R. (2012). *Developing an Ontology of the Cyber Security Domain*. STIDS, 49–56.

Pfleeger, C. P. & Pfleeger, S. L. (2002). *Security in Computing*. Lebanon, Indiana, U.S.A: Prentince Hall PTR.

Puhakainen, P. & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, 34(4), 757–778.

Quinn, J. B. (1987). Technology in services. *Scientific American*, 257(6), 50–58.

Rohde, F. H. (2004). IS/IT outsourcing practices of small-and medium-sized manufacturers. *International Journal of Accounting Information Systems*, 5(4), 429–451. doi:10.1016/j.accinf.2004.04.006

SANS. (2015). *Automating the Hunt for Hidden Threats*. SANS Instutite. Haettu 17.8.2016 osoitteesta https://www.sans.org/reading-room/whitepapers/analyst/automating-hunt-hidden-threats-36282

SANS. (2016a). *SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing*. SANS org. Haettu 19.8.2016 osoitteesta https://www.sans.org/reading-room/whitepapers/bestprac/state-cyber-threat-intelligence-survey-cti-important-maturing-37177

SANS. (2016b). *The SANS State of Cyber Threat Intelligence*. SANS Institute. Haettu 19.8.2016 osoitteesta https://www.sans.org/reading-room/whitepapers/bestprac/state-cyber-threat-intelligence-survey-cti-important-maturing-37177

SANS. (2016c). *The Who, What, Where, When, Why and How of Effective Threat Hunting*. Haettu 19.8.2016 osoitteesta https://www.sans.org/reading-room/whitepapers/analyst/who-what-where-when-effective-threat-hunting-36785

SANS. (2016d). *2016 State of Application Security: Skills, Configurations and Components*. April. Haettu 19.8.2016 osoitteesta https://www.sans.org/reading-room/whitepapers/application/2016-state-application-security-skills-configurations-components-36917

SANS Infosec Reading Room. (2016). *The Who, What, Where, When, Why and How of Effective Threat Hunting*. Haettu 19.8.2016 osoitteesta https://www.sans.org/reading-room/whitepapers/analyst/who-what-where-when-effective-threat-hunting-36785

SANS Institute. (2013). *SANS Institute*. Haettu 17.8.2016 osoitteesta https://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840

Sääksjärvi, M., Lassila, A. & Nordström, H. (2005). *Evaluating the software as a service business model: From CPU time-sharing to online innovation sharing*. IADIS international conference e-society. Qawra, Malta.

Taleb, N. N. (2007). *The black swan: The impact of the highly improbable*. Random house.

The Bundestag. (2009). *BSI act - BSIG. Act to Strengthen the Security of Federal Information Technology*. Berlin, Germany. Haettu 24.8.2016 osoitteesta https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf;jsessionid=5DE94B7DA732B68960EDB34996F3511B.2_cid359?__blob=publicationFile&v=1

TNS opinion & Social. (2015). *Special Eurobarometer 423 Cyber Security*. European Commission. doi:10.2837/411118

US-CERT. (2011). www.us-cert.gov. Haettu 17.8.2016 osoitteesta https://www.us-cert.gov/ncas/tips/ST06-001

Valtiovarainministeriö. (2008). Vahtiohje.fi. Haettu 15.8.2016 osoitteesta https://www.vahtiohje.fi/c/document_library/get_file?uuid=7e2220f1-cc93-4ba6-8c70-a67869c526cc&groupId=10229

Viestintävirasto. (2015). Haavoittuvuuskoordinointi. Haettu 30.8.2016 osoitteesta https://www.viestintavirasto.fi/kyberturvallisuus/viestintavirastontietoturvapalvelut/haavoittuvuuskoordinointi.html

Viestintävirasto. (2016a). CERT-toiminto. Haettu 5.11.2016 osoitteesta https://www.viestintavirasto.fi/kyberturvallisuus/viestintavirastontietoturvapalvelut/cert-fi.html

Viestintävirasto. (2016b). Yhteistyöryhmien tiedonvaihtokäytäntöjä. Haettu 5.11.2016 osoitteesta https://www.viestintavirasto.fi/attachments/cert/certtiedostot/julkaisu_003_2016_J.pdf

Viestintävirasto. (2016). Postituslistat. Haettu 30.8.2016 osoitteesta https://www.viestintavirasto.fi/kyberturvallisuus/viestintavirastontietoturvapalvelut/cert-fi/postituslista.html.stx

Viestintävirasto. (2017). NCSA-toiminto. Haettu 15.5.2017 osoitteesta https://www.viestintavirasto.fi/kyberturvallisuus/viestintavirastontietoturvapalvelut/ncsa-fi.html

LUKU 8.

Tietoturvapalveluiden kategorisointi

Kulta Lotta

Koskinen Jani

Tämän työpaketin alkuperäisenä tehtävänantona oli: ”*Mitkä ovat sellaisia tietoturvahyödykkeitä, joita käytetään laajasti eri toimialoilla Suomessa toimivissa yrityksissä, ja miten tällaista palveluntarjontaa ja avainosaamista on tarvittaessa mahdollista ankkuroida Suomeen?”* Työpaketin kohdalla kävi kuitenkin ilmi, että alkuperäistä tehtävänantoa ei ollut mahdollista toteuttaa alkuperäisessä muodossaan. Tähän oli kaksi perusteltua syytä. Ensimmäinen oli termin tietoturvahyödyke puuttuminen kirjallisuudesta, mikä aiheutti ongelman rajauksen ja tutkimuksen kohdentamisen osalta. Toinen syy oli kokonaisvaltaisen kuvan puute eri tietoturvapalveluista (hyödykkeen lähin ja paras vastine kirjallisuudessa), asia, joka puoltaa tässä työpaketissa valittua toteutusta ja lähestymistapaa. Tämä työpaketti perustuu systemaattiseen kirjallisuuskatsaukseen eri tietoturvapalveluista ja niiden kategorisoinnista, pohjautuen ISO27002-standardiin ja VAHTI-ohjeeseen. Tämän lisäksi työpaketissa tehtiin kysely, jolla kartoitettiin tietoturvan merkitystä yrityksissä.

8.1. Kirjallisuuskatsaus

Kirjallisuuskatsauksen alkuperäisenä tarkoituksena oli kartoittaa, millaisia tietoturvahyödykkeitä markkinoilla on. Ongelmaksi nousi se, että termi hyödyke (commodity) ei ole yleisesti käytetty. Kirjallisuuskatsauksen tekeminen ja hyödykkeiden luokittelu ei siis onnistunut, koska tuloksia ei termillä hyödyke kirjallisuudesta saatu. Tästä johtuen kirjallisuuskatsauksessa hyödyke-termi korvattiin termillä palvelu, joka taas on kirjallisuudessa yleisesti käytetty tietoturvatuotteiden kohdalla. Kirjallisuuskatsaus toteutettiin systemaattisesti ja se jakautui seitsemään eri vaiheeseen (kuva 9).

Kuva 9: Systemaattisen kirjallisuuskatsauksen toteutus.

Ensimmäisessä vaiheessa tarkennettiin alustavaa tutkimuskysymystä ja luotiin katsauksen protokolla. Protokollassa määriteltiin käytetyt artikkelitietokannat ja alustavat hakusanat. Tässä vaiheessa kävi ilmi, että termi tietoturvahyödyke (information security commodity) ei ole käyttökelpoinen hakusana systemaattiseen kirjallisuuskatsaukseen johtuen termin käyttämättömyydessä kirjallisuudessa. Tämän johdosta hyödyke korvattiin sanalla palvelu (service), joka on kirjallisuudessa yleisesti käytetty termi.

Toisessa vaiheessa tehtiin alustava haku Google Scholarilla, minkä perusteella valittiin lopullisessa haussa käytettävät hakusanat ja tietokannat. Hakusanoina käytettiin seuraavia termejä:

- Information security service(s)
- Infosec service(s)
- Infosecurity service(s)
- IS security service(s)
- IT security service(s).

Haun kattavuuden lisäämiseksi käytettiin myös hakusanojen monikkomuotoja ja hakuun sisällytettiin kaikki lähteet, jotka sisälsivät jonkin edeltävistä hakusanoista (OR-operaattori). Kirjallisuuskatsauksen haku suoritettiin systemaattisesti ja haut tehtiin seuraaviin tietokantoihin:

- IEEE,
- Elsevier Science Direct
- Emerald Insight
- ACM – Association for Computing Machinery
- Proquest
- SpringerLink.
-

Haku toteutettiin 4.9.2016 ja haun tulokseksi saatiin 656 artikkelia. Haussa käytettiin rajoituksia, ja niiden avulla mukaan hakuun sisällytettiin tieteelliset aikakausijulkaisut, konferenssijulkaisut ja kirjat (pelkästään tieteelliseen aikakausijulkaisuhakuun sisältyvät). Systemaattiseen kirjallisuuskatsaukseen sisällytettiin vain ne artikkelit, joihin oli pääsy Turun yliopiston tunnuksilla, ja erillisiä, maksullisia lähteitä ei otettu mukaan katsaukseen.

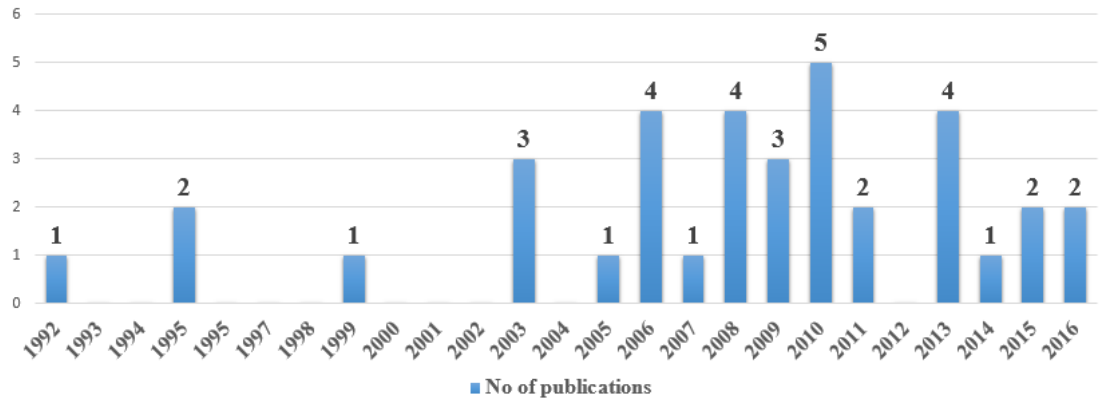
Kolmannessa vaiheessa kirjallisuuskatsausta artikkeleista valittiin mukaan ne, joissa joku termeistä löytyi otsikosta, tiivistelmästä tai johdantoluvusta. Valinnan tarkoituksena oli keskittyä keskeisiin artikkeleihin, ja tämän vaiheen katsauksen jälkeen jäljelle jäi 60 artikkelia. Artikkelien löytyminen tietokannoittain vaiheessa kaksi ja kolme on eritelty taulukossa 13.

Taulukko 13: Artikkelit tietokannoittain.

Step	IEEE	Science-Direct	ACM	Emerald Insight	Proquest	Springer Link	In total
Step 2	167	226	3	20	121	119	**656**
%	25,5%	34,5%	0,5%	3,0%	18,4%	18,1%	**100,0%**
Step 3	35	5	1	2	12	5	**60**
%	58,3%	8,3%	1,7%	3,3%	20,0%	8,3%	**100,0%**

Neljännessä vaiheessa artikkelit käytiin systemaattisesti läpi, ja niistä poistettiin hakutuloksiin tulleet kaksoiskappaleet (9 kpl). Seuraavaan vaiheeseen otettiin mukaan 51 artikkelia.

Viidennessä vaiheessa artikkelit käytiin läpi yksitellen, ja niistä valikoitui mukaan lopulta 36 artikkelia vuosilta 1992–2016 (katso liite 1). Katsauksen ulkopuolelle jätettiin artikkelit, joiden kieli oli muu kuin englanti. Lisäksi pois jätettiin artikkelit, jotka eivät liittyneet aiheeseen tai joiden laatu ei ollut tieteellisellä tasolla. Valitut artikkelit on esitetty julkaisuvuosien mukaan eriteltyinä kuvassa 10.



Kuva 10: Artikkelien julkaisuvuodet.

Kuudennessa vaiheessa saaduista artikkeleista toteutettiin analyysi. Analyysi oli luonteeltaan iteratiivinen ja sisälsi useita syklejä, kun uusia tietoturvapalveluja löytyi artikkeleista ja niitä jouduttiin uudelleen ryhmitelmään ja vertaamaan toisiinsa.

Seitsemännessä vaiheessa analyysin perusteella palveluista muodostettiin kategoriat ja ne visualisoitiin Freemind-ohjelmalla. Myös tämä vaihe oli iteratiivinen ja sisälsi useita syklejä, joiden aikana kategorioita kehitettiin ja muokattiin.

8.2. Palvelujen kategorisointi

Kirjallisuuskatsauksen perusteella tietoturvapalvelut kategorisoitiin kolmella eri tasolla siten, että ensimmäisellä tasolla on yleisin kuvaus (pääluokat) ja kahdella seuraavalla tasolla kategorisointi tarkentuu niin, että kolmannella tasolla yksittäiset tietoturvapalvelut ovat näkyvillä. Kategorisoinnin pohjaksi etsittiin jo olemassa olevia luokitteluja, jotta nähtäisiin, miten tietoturvapalveluita on jaoteltu ja mitä kirjallisuuskatsaus tuo niihin lisää. Kirjallisuuskatsauksen perusteella tehty kategorisointi hyödyntää jo tehtyjä luokitteluja, mutta tuo niihin syvyyttä ja tuo näkyväksi, kuinka laaja tietoturvapalvelujen kenttä on ja kuinka monimuotoisia palveluja on ylipäätään olemassa.

Vahti-ohjeisiin perustuva ylätason kategoria

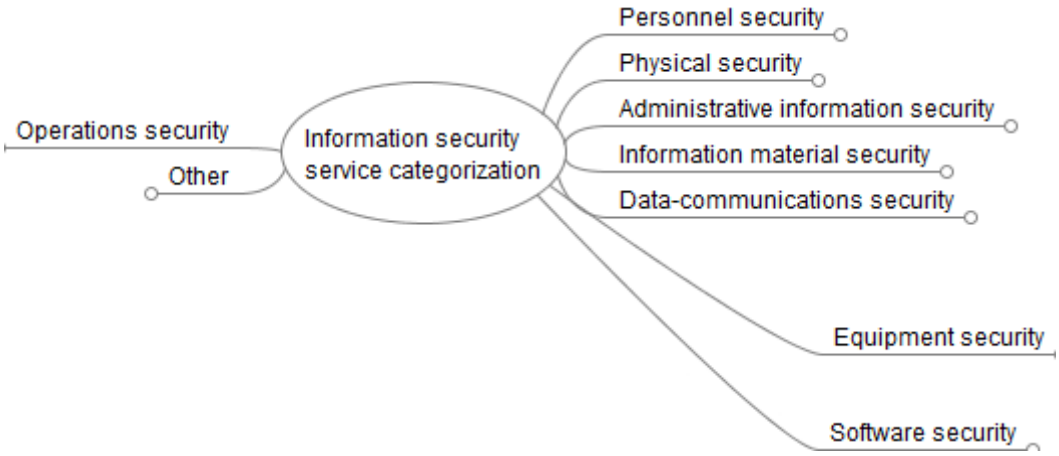
Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on luonut tietoturvaohjeet (Vahti-ohjeen[41]), joita hyödynnetään julkishallinnossa, mutta myös yritysmaailmassa.

Kategorisoinnin pohjana ensimmäisellä tasolla (kuva 11) ovat siis VAHTI-ohjeista otetut tietoturvapalvelujen kategoriat:

- Fyysinen turvallisuus (Physical security)
- Hallinnollinen tietoturvallisuus (Administrative information security)
- Henkilöstöturvallisuus (Personel security)
- Käyttöturvallisuus (Operation security),
- Laitteistoturvallisuus (Equipment security)
- Ohjelmistoturvallisuus (Software security)
- Tietoaineistoturvallisuus (Information material security)
- Tietoliikenneturvallisuus (Data-communications security).

VAHTI-ohjeen tietoturvan osa-alueiden lisäksi kategoriaan liitettiin kohta muut (other), jotta kaikki palvelut saatiin otettua mukaan kategorisointiin, kun kategoriaa laajennetaan seuraavilla tasoilla. Kategorisoinneissa käytetään englanninkielisiä termejä, koska kirjallisuus pääsääntöisesti on englanninkielistä, ja tämän lisäksi kaikille palveluille ei ole yksiselitteistä ja vakiintunutta suomenkielistä termiä.

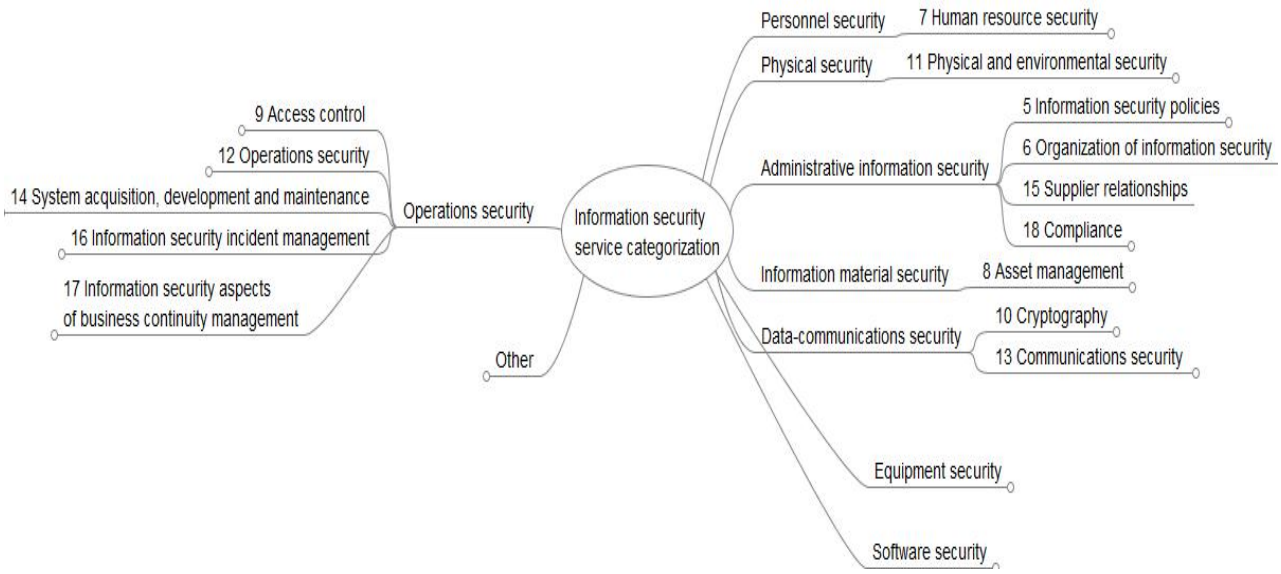
[41] https://www.vahtiohje.fi/web/guest/vahti-ohjeet-by-categoy



Kuva 11: Vahti-palvelujen mukainen ensimmäisen tason kategoria.

ISO 27002 -standardiin perustuva välitason kategoria

Kategorisoinnin toisella tasolla hyödynnettiin ISO 27002 -standardin 14 klausuulia, jotka muodostavan palvelujen kategorisoinnin toisen tason laajentaen Vahti-ohjeistukseen perustuvaa ylimmän tason kategoriaa. Toisen tason kategoria jaottelee osan ylemmän tason kategorioista toisen asteen kategorioiksi (kuva 12). ISO 27002 -standardin mukaista kategorisointia puoltaa myös ISO-standardin asema ja tunnettavuus, joka helpottaa kategorisoinnin omaksumista ja käyttöä organisaatioissa, koska kategoria mukailee jo mahdollisesti käytössä olevaa kuvausta tietoturvapalveluista.



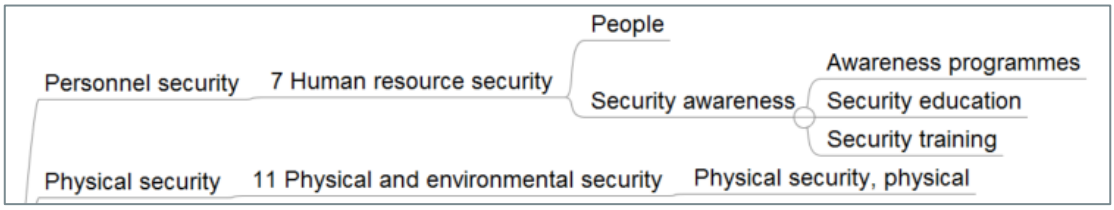
Kuva 12: ISO 27002 -standardin mukaan muodostettu kategorian toinen taso.

Tietoturvapalvelujen kattava kategorisointi

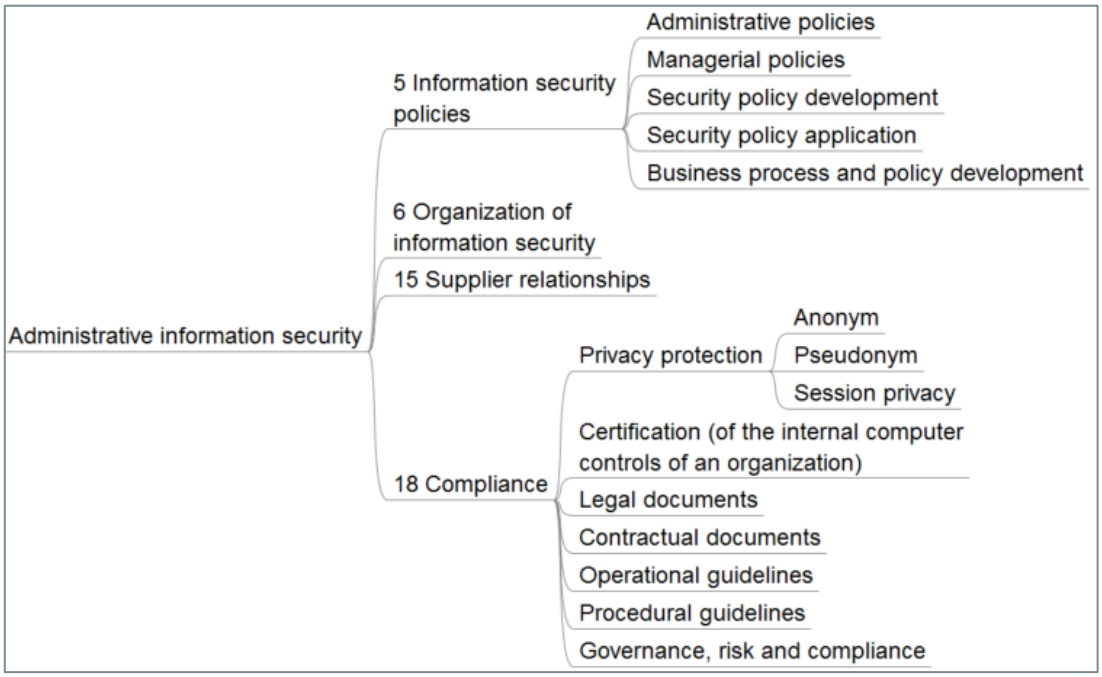
Kategorisointi perustuu kirjallisuuskatsauksen (liite 1) tuottamaan listaan erilaisista tietoturvapalveluista ja niiden eri muodoista. Kategorisointi on yksi vaihtoehto ja keinotekoinen kuvaus palveluista. Palvelun asettamisen eri kategorioihin voisi toteuttaa eri tavalla, koska eri osa-alueet linkittyvät verkostomaisesti toisiinsa ja niiden sijoittuminen eri luokkiin eri tavoin voitaisiin

myös perustellusti toteuttaa. Kyseiseen kategoriaan päädyttiin siis iteratiivisen lähestymistavan avulla, ja nyt esitetty malli perustuu prosessin aikana muodostettuun käsitykseen palveluista ja niiden suhteista.

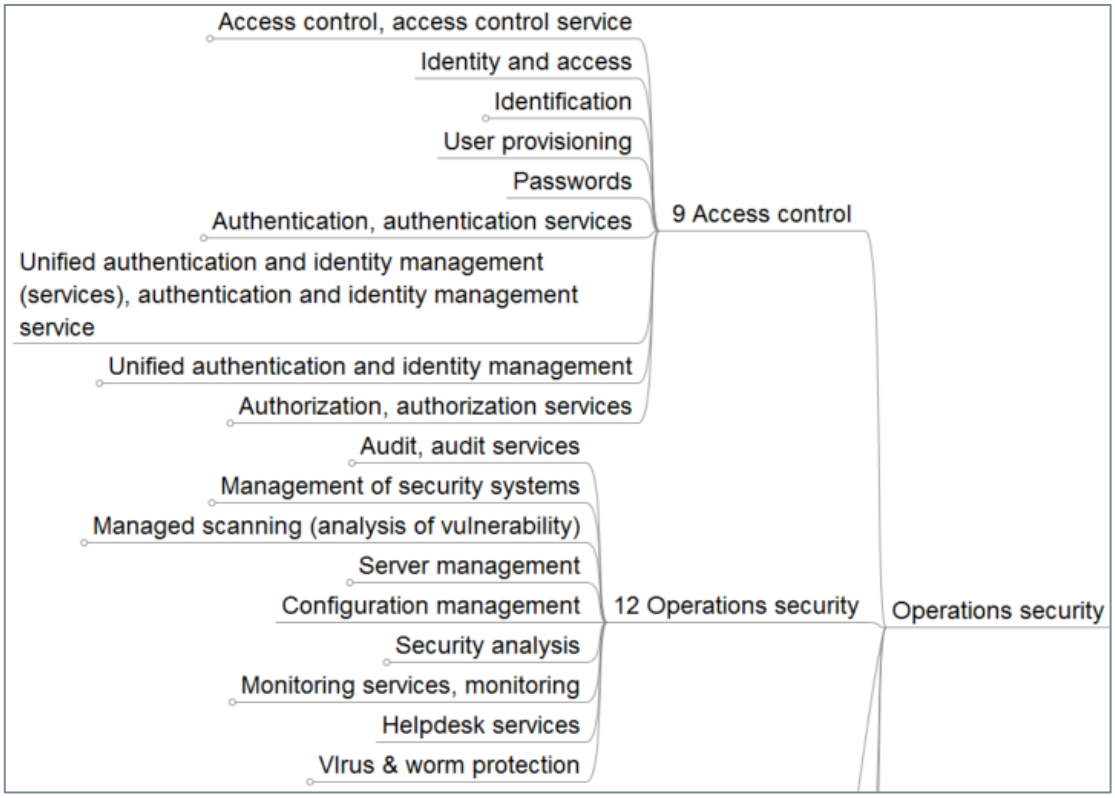
Tässä esitettyä kategorisointia voidaan kritisoida ja sen tilalle voidaan löytää vaihtoehtoisia tapoja palvelujen kategorisointiin. Tästä huolimatta tässä luodun kategorisoinnin etuna on sen tuottama selkeä kuva siitä, millaisia tietoturvapalveluita on olemassa. Kategorisoinnin ryhmittely mahdollistaa erilaisten palvelujen tarkastelun käsiteltävinä ja ymmärrettävinä kokonaisuuksina. Tämä ryhmittely luo paremman kokonaiskuvan kuin pelkkä lista palveluista olisi voinut antaa. VAHTI-ohjeisiin ja ISO 27002 -standardiin perustuva kategorisointi antaa mahdollisuuden analysoida tietoturvapalvelujen käyttöä laaja-alaisesti jo käytössä olevien parhaitten käytäntöjen mukaisesti ja tuo esiin niiden suhteet toisiin palveluihin. Kategorisointi tuo analyysiin tarvittavaa syvyyttä systemaattisella ja samaan aikaan suoraviivaisella, selkeällä esityksellä.



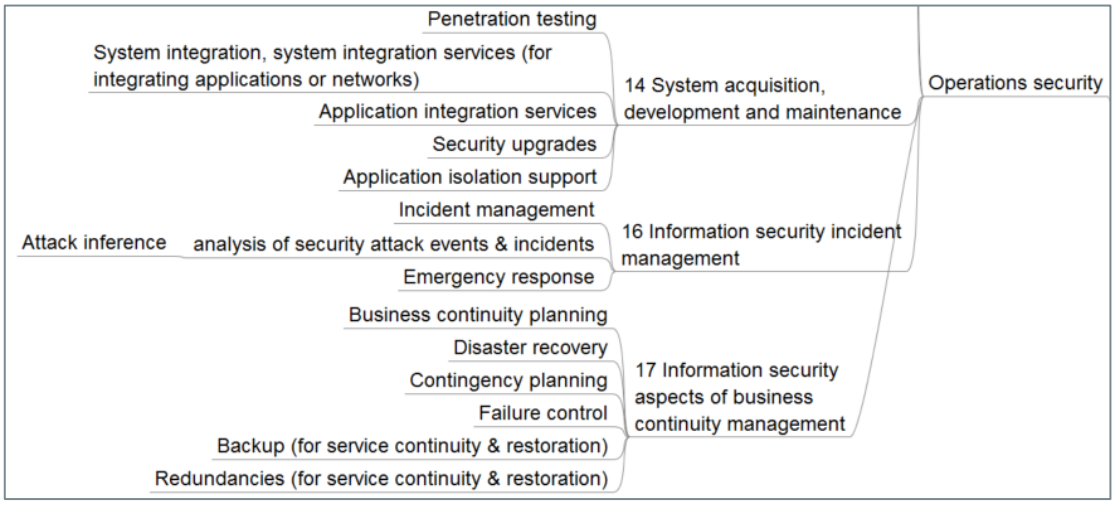
Kuva 13: Kategorisaation palvelujaottelu, osa 1.



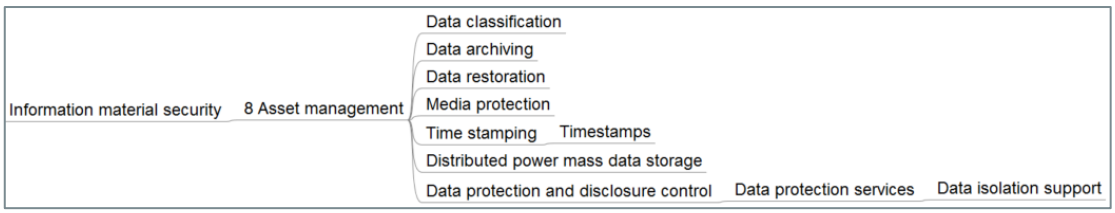
Kuva 14: Kategorisaation palvelujaottelu, osa 2.



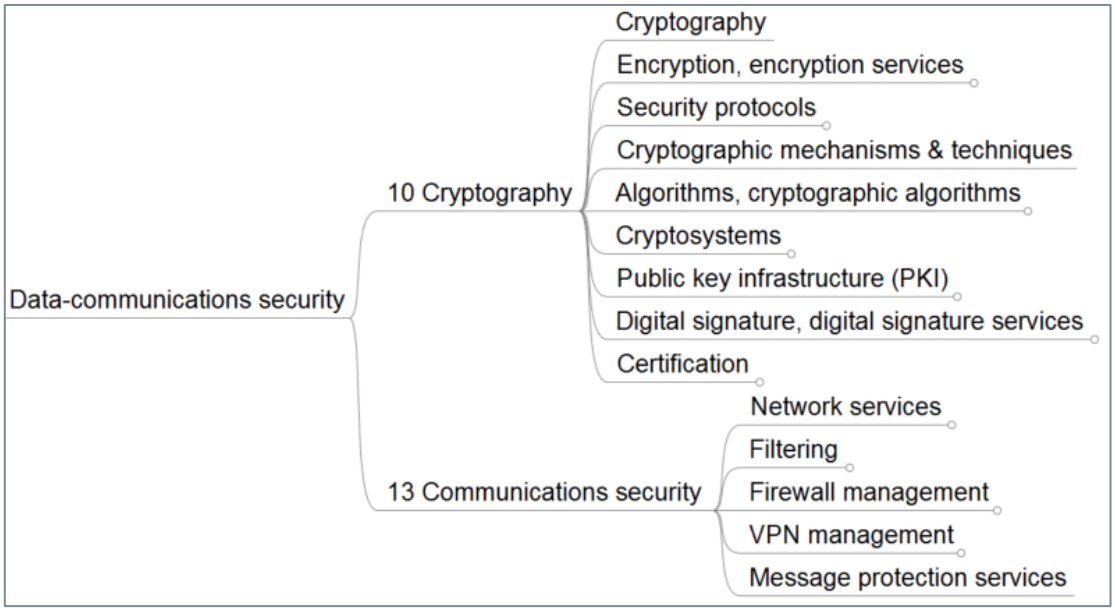
Kuva 15: Kategorisaation palvelujaottelu, osa 3.



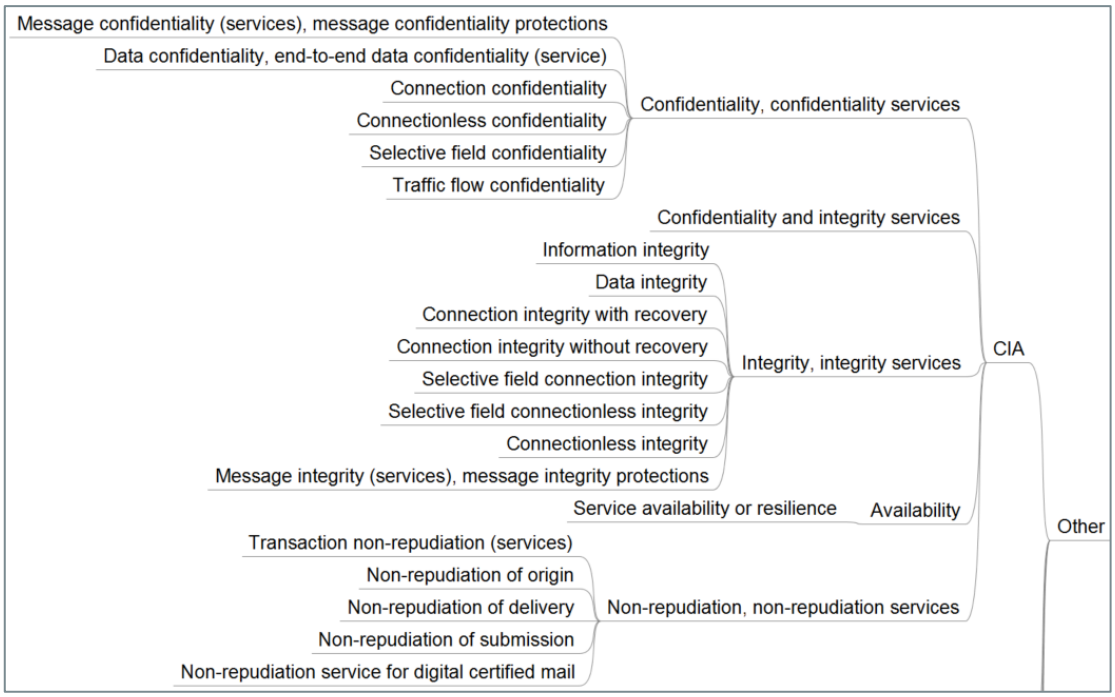
Kuva 16: Kategorisaation palvelujaottelu, osa 4.



Kuva 17: Kategorisaation palvelujaottelu, osa 5.



Kuva 18: Kategorisaation palvelujaottelu, osa 6.



Kuva 19: Kategorisaation palvelujaottelu, osa 7.

8.3. Kyselytutkimus

Kyselytutkimuksen tarkoituksena oli kartoittaa tietoturvapalveluiden käyttöä yrityksissä ja niiden merkitystä yritykselle. Kyselytutkimus suoritettiin ajalla 16.–30.5.2017, ja se toteutettiin Webropol-verkkokyselynä (kysymykset liitteessä 2). Kysely kohdistettiin Turun seudun alueella toimiville yrityksille ja erityisesti tietohallinnossa toimiville henkilöille.

Kyselyä markkinoitiin sosiaalisessa mediassa LinkedIn-palvelussa (LinkedInin kautta kyselyä on katsottu yli 1300 kertaa) ja Facebookin eri sivuilla (ei tarkkaa katsojamäärää tiedossa). Sosiaalisen median lisäksi kyselyä markkinoitiin myös Turun Kauppakamarin ICT-valiokunnassa ja sähköpostitse tutkijoiden sidosryhmille.

Kyselyyn vastasi vain 15 henkilöä (vastaukset liitteessä 3), mutta huomattavaa on, että kysely avattiin lähettämättä vastausta yli 130 kertaa. Yhden uskottavan syyn kyselyyn vastaamatta jättämiselle tarjoavat suorilta kontakteilta saadut vastaukset. Heidän mukaansa kyselyyn ei voitu vastata luottamuksellisten tietojen ja asiakassalaisuuksien vuoksi. Kyselyyn vastaajat olivat myös maininneet samansuuntaisia kommentteja avoimissa kysymyksissä.

Vastauksien vähäisyyden vuoksi kyselyn perusteella ei voida tehdä kovin pitkälle meneviä johtopäätöksiä.

8.4. Johtopäätökset

Tietoturva ja niihin liittyvät palvelut ovat alue, joka kehittyy ja on kehittynyt nopeasti. Osin tästä syystä käsitys siitä, mitä tietoturvapalvelut ovat, on epäselvä. Terminologia on vaikeasti ymmärrettävää ja kirjallisuudesta ei löydy selkeää kategoriaa tai yhtenäistä mutta riittävän yksityiskohtaista kuvausta eri tietoturvapalveluista. Jotta tietoturvapalveluita voidaan kehittää systemaattisesti ja implementoida käyttöön yhteiskunnan eri tasoilla, – mikä on aina vain tärkeämpää – tulee luoda kokonaisvaltainen kuva eri tietoturvapalveluista ja niiden merkityksestä.

Edellä esitettyä kategorisointia voidaan käyttää hyväksi monin eri tavoin. Yksinkertaisimmillaan se voi toimia organisaation tietoturvakarttana, kun halutaan syventää ymmärrystä tietoturvasta ja löytää mahdolliset tietoturvaratkaisut ja palvelut, joilla organisaatio voi vastata jo kohdattuihin tai vasta mahdollisiin tietoturvauhkiin. Sen avulla voidaan tarkastella, mitä tarpeita organisaatiolla on tietoturvaan liittyen, mitkä tietoturvapalvelut ovat käytössä ja mihin mahdollisesti tulisi panostaa.

Laajempana käyttönä voisi olla esim. VAHTI-ohjeiden kehittäminen kategorisoinnin perusteella. Kategorisointi voisi toimia ylätason hierarkiana, jolla VAHTI-ohjeet saatettaisiin syvemmälle tasolle. Koska tässä ehdotettu kategorisointi perustuu osin jo käytössä oleviin tietoturvallisuuden osa-alueisiin, se syventäisi ohjeiden ryhmittelyä ja toisi näin esiin mahdolliset osa-alueet, joihin ohjeissa voisi tulevaisuudessa panostaa.

Kategorisointia voidaan ja sitä tulisi kehittää eteenpäin riskien hallinnan näkökulmasta. Kun nyt kategorisoinnissa vain tarkastellaan eri palveluita, pitäisi tarkastella myös, mitä riskejä eri palvelut torjuvat ja mikä on eri palveluiden suhde eri riskeihin ja toisiin palveluihin. Kuten jo aiemmin on todettu, palvelut liittyvät verkostomaisesti toisiinsa ja vasta kokonaisuus luo turvallisuuden. Kategorisointi tuo näkyväksi, minkälaisia palveluita on olemassa, ja sen avulla voidaan kartoittaa, mitä palvelukombinaatioita eri riskien hallinnassa voidaan käyttää. Esimerkkinä on potilastietojen tietoturva, jossa palomuurit tai ohjelmistot eivät riitä, jos potilastietoja käytetään myös paperimuodossa ja niiden käsittelyä ei ole kontrolloitu. Kategorian avulla voidaan läpikäydä ja varmistaa, onko jokin tietoturvan osa-alue unohtunut kyseisen organisaation tai toiminnan kohdalla.

Tietoturvapalvelujen laajan repertuaarin vuoksi emme myöskään suosittele käyttämään termiä tietoturvahyödyke, koska se lisää vain tulkinnallisuutta terminologisesti jo muutenkin monimutkaisella alalla. Suosittelemme nojautumaan jo olemassa oleviin luokituksiin ja standardeihin sekä niiden tarkennuksiin, jotka tässä raportissa tarjotaan.

Kirjallisuuden ja kyselyn perusteella voidaan myös olettaa, että yksilöiden ja yritysten kokonaiskuva tietoturvapalveluista ei ole kattava terminologian ja palvelujen hajanaisuudesta johtuen. Tässä onkin mahdollisuus edistää tietoturvaa ja siihen liittyvää liiketoimintaa tarjoamalla

VAHTI-ohjeiden lisäksi tarkempaa ja laajempaa ohjeistusta kokonaisvaltaiseen tietoturvakartoitukseen. Tässä Valtionhallinnon tietoturvallisuuden johtoryhmä olisi toimija, joka voisi ottaa edelläkävijän roolin ja tukea tietoturvallisuuden kehittymistä suomalaisessa yhteiskunnassa.

Lähteet

AbdElnapi, N. M. M., Omara, F. A., & Omran, N. F. (2016). A Hybrid Hashing Security Algorithm for Data Storage on Cloud Computing. *International Journal of Computer Science and Information Security*, 14(4), 175.

Asgarnezhad, M., Nasiri, R., & Sahebhonar, S. (2010, 9-15 May 2010). *Analysis and Evaluation of Two Security Services in SOA*. Paper presented at the 2010 Fifth International Conference on Internet and Web Applications and Services.

Bahl, S., & Wali, O. P. (2013). An empirical analysis of perceived significance of information security service quality to predict the organisational performance in software service industry. *CSI transactions on ICT*, 1(3), 221–230.

Bahl, S., & Wali, O. P. (2014). Perceived significance of information security governance to predict the information security service quality in software service industry: An empirical analysis. *Information Management & Computer Security*, 22(1), 2–23.

Bowen, P., Hash, J., & Wilson, M. (2006). *Information security handbook: A guide for managers-Recommendations of the national institute of standards and technology*.

Buecker, A., Ashley, P., Borrett, M., Lu, M., Muppidi, S. & Readshaw, N. (2008). *Understanding SOA Security Design and Implementation*: IBM Redbooks.

Chang, C.-C. & Lee, W.-B. (2003). Taiwan: focus on the information security market. *IT professional*, 5(5), 26–29.

Chappell, B. L., Marlow, D. T., Irey, P. M., & O'Donoghue, K. (1999). IP security impact on system performance in a distributed real-time environment.Teoksessa *Real-Time Systems Symposium, 1999. Proceedings. The 20th IEEE* (218-219). IEEE.

Choi, Y.-s. & Seo, D.-i. (2005, 2005). *An analysis of ISPs' role as managed security service providers (MSSPs)*. Paper presented at the The 7th International Conference on Advanced Communication Technology, ICACT 2005.

Claassen, G. J., Kuhn, G. J. & Penzhorn, W. T. (1992, 1992). *Information security services and standards for telecommunications in Africa.* Paper presented at the 3rd Africon Conference. Africon '92.

Deng, R. H., Bhonsle, S. K., Wang, W., & Lazar, A. A. (1995, 1995). *Integrating security in CORBA based object architectures.* Paper presented at the 1995 IEEE Symposium on Security and Privacy.

Jeong, C. W., Joo, S. C., & Jeong, Y. S. (2010, 2010). *Mobile Collaboration Environment Based on Distributed Object Group Framework for u-Hospital.* Paper presented at the 5th International Conference on Ubiquitous Information Technologies and Applications.

Jin, S., Cho, S., Choi, D., & Ryou, J.-C. (2003, 2003). *New security paradigm for application security infrastructure*. Paper presented at the Information Networking: International Conference, ICOIN 2003.

Karokola, G., Kowalski, S., & Yngstrom, L. (2011, 2011). *Secure e-government services: Towards a framework for integrating it security services into e-government maturity models*. Paper presented at the 2011 Information Security for South Africa.

Karokola, G., Kowalski, S., & Yngström, L. (2013, 2013). *Evaluating a Framework for Securing E-Government Services--A Case of Tanzania.* Paper presented at the 46th Hawaii International Conference on System Sciences.

Katsikas, S. K., Gritzalis, S., Karyda, M., Mitrou, E., & Quirchmayr, G. (2006). A framework for outsourcing IS/IT security services. *Information Management & Computer Security*, 14(5), 403–416.

Keeratiwintakorn, P. & Krishnamurthy, P. (2006, 2006). *Energy efficient security services for limited wireless devices*. Paper presented at the 1st International Symposium on Wireless Pervasive Computing.

Kovač, D. & Trček, D. (2009). Qualitative trust modeling in SOA. *Journal of Systems Architecture*, 55(4), 255–263.

Lee, W., Kim, S. & Kim, B. (2006). Response against hacking and malicious code in P2P. *Computational Science and Its Applications-ICCSA 2006*, 851–857.

Lin, Z. & Zhixin, C. (2010, 2010). *Design and implementation of a E-commerce system based on PKI*. Paper presented at the International Conference on Computer and Communication Technologies in Agriculture Engineering.

Liping, H. & Lei, S. (2011, 2011). *Research on trust model of pki.* Paper presented at the Fourth International Conference on Intelligent Computation Technology and Automation.

Lu, W., Liu, S., Yang, Y., Fu, R., Xiang, X., Qu, Y. & Huang, H. (2015). Design for the Emergency Command Information System Architecture of Ocean Oil Spill. *Aquatic Procedia*, 3, 41–49.

Miguel, J., Caballé, S., Xhafa, F. & Snasel, V. (2015, 2015). *A Data Visualization Approach for Trustworthiness in Social Networks for On-line Learning*. Paper presented at the IEEE 29th International Conference on Advanced Information Networking and Applications.

Moulton, R. & Coles, R. S. (2003). A contest to evaluate IT security services management. *Computers & Security*, 22(3), 204–206.

Mutegi, L., Gichuki, D. & Sevilla, J. (2016, 2016*). IT security service commoditization: The case of financial institutions in Kenya*. Paper presented at the IST-Africa Week Conference.

Oladapo, S., Zavarsky, P., Ruhl, R., Lindskog, D. & Igonor, A. (2009). *Managing risk of IT security outsourcing in the decision-making stage*. Paper presented at the 2009 International Conference on Computational Science and Engineering.

Peiris, H., Soysa, L. & Palliyaguru, R. (2008). *Non-repudiation framework for e-government applications*. Paper presented at the 2008 4th International Conference on Information and Automation for Sustainability.

Priescu, I., Patriciu, V. V. & Nicolaescu, S. (2009). *The Viewpoint of E-Commerce Security in the Digital Economy*. Paper presented at the 2009 International Conference on Future Computer and Communication.

Rachedi, A. & Benslimane, A. (2016). *Multi-objective optimization for Security and QoS adaptation in Wireless Sensor Networks.* Paper presented at the 2016 IEEE International Conference on Communications (ICC).

Ray, P. D., Harnoor, R. & Hentea, M. (2010). *Smart power grid security: A unified risk management approach*. Paper presented at the 44th Annual 2010 IEEE International Carnahan Conference on Security Technology.

Schultz, E. E. (1995). A new perspective on firewalls. *Network Security*, 1995 (10), 13–17.

Shaikh, R. A., Sharif, K., & Ahmed, E. (2005, August). Performance analysis of unified enterprise application security framework. In *Engineering Sciences and Technology, 2005. SCONEST 2005. Student Conference on Engineering Sciences and Technology* (1-7). IEEE.

Sidiroglou, S., Stavrou, A. & Keromytis, A. D. (2007). *Mediated overlay services (MOSES): Network security as a composable servic*e. Paper presented at the 2007 IEEE Sarnoff Symposium.

Sun, J. & Chen, Y. (2008). *Intelligent Enterprise Information Security Architecture Based on Service Oriented Architecture*. Paper presented at the 2008 International Seminar on Future Information Technology and Management Engineering.

Tamilarasan, A., Shankarapani, M. K., Qin, X., Mukkamala, S. & Sung, A. H. (2008, 2008). *Integrating energy efficiency and security for storage systems.* Paper presented at the 2008 IEEE International Conference on Systems, Man and Cybernetics.

Vorakulpipat, C., Siwamogsatham, S. & Kawtrakul, A. (2014). An investigation of information security as a service practice: case study in healthcare. *International Journal of Computer Applications in Technology*, 49(3-4), 365–371.

Wahab, A., Bahaweres, R. B., Alaydrus, M., Muhaemin, & Sarno, R. (2013, 12-14 Feb. 2013). *Performance analysis of VoIP client with integrated encryption module*. Paper presented at the 2013 1st International Conference on Communications, Signal Processing, and their Applications (ICCSPA).

Wang, Y., Deng, S., Lin, W.-M., Zhang, T. & Yu, Y. (2010, 2010). *Research of electric power information security protection on cloud security*. Paper presented at the 2010 International Conference on Power System Technology.

Xia, Z. & Hu, Y. (2006). Extending RSVP for quality of security service. *IEEE Internet Computing*, 10(2), 51–57.

Yamany, H. F. E. L. & Capretz, M. A. M. (2008, 2008). *Use of Data mining to Enhance Security for SOA*. Paper presented at the 2008 Third International Conference on Convergence and Hybrid Information Technology.

LOPPUSANAT

Suomi Reima

Tietosuojan kehittämisessä pitää ottaa huomioon kaikkien sidosryhmien tarpeet. Keskittyminen pelkästään kuluttajien suojaamiseen tekee liiketoiminnan mahdottomaksi, ja keskittyminen pelkästään yritystoiminnan edellytysten parantamiseen puolestaan saa kuluttajat hylkäämään palvelut.

Tietoturvan ja -suojan pitäisi olla luonnollisia kilpailuetuja yrityksille. Pitkällä tähtäimellä yritykset, jotka eivät pysty vastaamaan kuluttajien tarpeisiin, kuihtuvat markkinoilta. Sitä ennen voi kuitenkin tapahtua paljon pahaa.

Tietosuoja ja -turva eivät kehity tyhjiössä, vaan niiden kehittymiseen tarvitaan muutenkin suotuisa ympäristö. Yritystoiminnan ja palveluiden kokonaisvaltainen vastuullinen kehittäminen on keskeistä. Tietosuoja ei voi olla kovin paljon yrityksen muuta toimintatapaa enemmän tai vähemmän kehittynyttä, tai silloin kehityspanoksista ei ainakaan saada kaikkea hyötyä irti.

MyData-tyyppiset ratkaisut, jotka todella voimavaraistavat kuluttajan, ovat tarpeen. Kuluttajat eivät aina myöskään jaksa paneutua ja pysty paneutumaan erilaisten palveluiden ja tuotteiden tietosuojaan ja -turvaan riittävästi. Erilaiset viranomaisten tai hyväksyttyjen sertifiointitahojen tuottamat helppotajuiset – vaikkakin väistämättä myös osin ylimalkaiset – asteikot osoittamassa tietosuojan tasoa voisivat olla hyödyllisiä. Tällaisiahan jo nähdään esim. erilaisten sähkölaitteiden energiatehokkuutta tai ravintoloiden hygieniatasoa määrittämässä. Tällaisten asteikkojen kehittäminen voi perustua vain Euroopan laajuiseen yhteistyöhön.

Helpot keinot, kuten (kaupallisten) kolmansien osapuolten myöntämät sertifikaatit, taikka se, että sivusto käyttää salausta tietoliikenteessä, eivät vielä riitä takaamaan kuluttajan luottamusta. Yrityksen vahva brändi on usein paljon parempi keino saavuttaa kuluttajan luottamus. Pohjoismaissa ja Suomessa julkishallinto onneksi nauttii kansalaisten luottamusta, ja ulkopuolisilla sertifikaateilla ei todennäköisesti saavutettaisi suurta etua. Sertifikaattien merkitys tulee todennäköisesti tulevaisuudessa korostumaan, ja niitä tarvitsevat erityisesti pienet yritykset, joiden brändi ei ole kovin vahva. Mitään suurta hyppäystä sertifikaattikulttuuriin ei kuitenkaan ole näköpiirissä, sillä esim. nuoret kuluttajat eivät näytä luottavan niihin eivätkä vaativan niitä sen enempää kuin vanhemmatkaan.

Kuluttajat eivät myöskään luota mahdollisuuksiinsa säädellä oman tietonsa käyttöä itse. Tämä johtopäätös näyttää vahvistuvan esimerkiksi silloin, kun verkkotoimijan koko ja kansainvälisyys kasvaa. Tutkimuksen tulokset osoittavat, että kuluttajien luottamusta digitaalisiin hyödykkeisiin voidaan lisätä tietojenkäsittelytoimien läpinäkyvyyden lisäksi antamalla heille mahdollisuuksia hallita tietojaan. Nykyisellään rekisteröidyn oikeudet toteutuvat monissa viestintäsovelluksissa ja pilvipalveluissa, mutta tietojen hallintamahdollisuudet ovat usein näennäisiä. Tietosuojakäytännössä tai palvelun käyttöehdoissa tulisi ensinnäkin varmistaa, että suostumuksen laajuus on käyttäjälle selvä. Suostumuksen on oltava myös helposti peruutettavissa. Mikäli suostumuksen peruuttaminen tarkoittaa palvelun poistamista, voidaan sen katsoa aiheuttavan käyttäjälle haittaa, mikä on paitsi tietosuoja-asetuksen vastaista, myös kuluttajan kannalta epäsuotuisa menettely. Käyttäjällä tulisi olla mahdollisuus tarkistaa, mitä tietoja hänestä on kerätty, keillä

on pääsy niihin ja ketkä ovat käsitelleet niitä. Tarkastusoikeuden lisäksi käyttäjällä tulisi olla valintamahdollisuuksia: käyttäjä voisi tehdä valintoja esimerkiksi sen suhteen, mitä tietoja viestintäsovellus kerää ja käyttää.

Terveydenhuolto voisi toimia suunnannäyttäjänä kuluttajien luottamusta rakennettaessa. Toimiala on jo valmiiksi erittäin säädelty ja melko samalla lailla toimiva kaikkialla maailmassa. Kansalaiset eivät tule toimialan asiakkaiksi kokeilunhalusta ja huvikseen, vaan ovat aina vakavasti liikkeellä, kun terveys- tai sosiaalialan palveluita tarvitaan.

Käyttäjän ja palveluntarjoajan arvopohjan yhdensuuntaisuus sekä arvoristiriitojen välttäminen ovat merkittäviä tekijöitä luottamuksen rakentamisessa, ja niitä voidaan hyödyntää kilpailutekijänä. Suomessa julkishallinto onneksi jakaa arvopohjan useimpien kansalaisten kanssa. Tätä yhteistä arvopohjaa on vaalittava ja jalostettava edelleen, esim. Kansallisen Palveluarkkitehtuurin onnistuminen on tässä avainasemassa.

Kansalaiset arvioivat ja tarvitsevat tietosuojaa ja -turvaa eri tavalla eri palveluissa. Taloudellisia transaktioita tehtäessä varovaisuus on huipussaan, mutta esim. sosiaalisessa mediassa vallitsee melko vapaamielinen ilmapiiri.

Pilvipalvelut ovat tulleet yhteiskuntaamme jäädäkseen. Uudenlaisten teknologioiden tuomien mahdollisuuksien lisäksi niihin liittyy merkittäviä riskejä, jotka saattavat vaarantaa käyttäjien yksityisyydensuojan. Palveluita tarjotaan ympäri maailmaa niin kuluttajakäyttäjille kuin yrityskäyttäjille, ja usein perusinfrastruktuuri keskittyy harvojen keskeisten toimijoiden käsiin. Mikäli yritykset informoivat asiakkaidensa henkilötietoihin kohdistuvista tietojenkäsittelytoimista avoimesti, läpinäkyvästi ja ymmärrettävästi, kuluttajien luottamus digitaalisia palveluita kohtaan kasvaa. Luottamuksen on nähty olevan yksi digiyhteiskunnan peruspilareista, joka on edellytys markkinoiden tehokkaalle toiminnalle.

Keskeistä on, että kuluttajien pitäisi päästä nauttimaan palveluista täysimääräisesti ja tasaarvoisesti myös tilanteessa, jossa he eivät halua luovuttaa henkilötietojaan, esim. paikkatietojaan. Toisaalta on ymmärrettävää, että tietojen puuttuessa palveluntarjoajan kyky tarjota parasta palvelua ei välttämättä ole täydellinen.

Avoimet rajapinnat ovat yksi keskeinen keino rakentaa tietojenkäsittelyn ekosysteemejä. Niitä määriteltäessä tehdään myös tärkeitä ja keskeisiä tietoturva ja -suojapäätöksiä. Globaalisti suurimpia menestystarinoita avoimien rajapintojen käytössä ovat sosiaalisen median toimijat (esim. Facebook), jotka tarjoavat rajapinnan tuhansille eri sovelluksille, sekä mobiilipuolen ekosysteemin perustan muodostavat käyttöjärjestelmät Googlen Android ja Applen iOS.

Avoimia rajapintoja tarvitaan paitsi teknisten syiden vuoksi, myös luottamuksen ja sosiaalisen pääoman rakentamiseksi. Erityisesti tämä korostuu asioiden ja esineiden Internetin yleistyessä, missä lähes kaikki toiminta perustuu laajempaan ekosysteemiin. Erityisesti PK-yritysten tulee vastata tähän haasteeseen lisäämällä sosiaalista pääomaansa, verkostoituen eri toimijoiden kanssa.

Julkishallinto nauttii jo suurta sosiaalista pääomaa ja on rakentamassa tietoonsa ja järjestelmiinsä avoimia rajapintoja. Hyvänä esimerkkinä voidaan nostaa esiin Kanta-palvelut, jotka edustavat avoimiin rajapintoihin perustuvaa terveydenhuollon ekosysteemiä. Alussa tarvitaan usein julkisen sektorin vahvaa panosta, jonka jälkeen yksityinen sektori voi alkaa kehittää toimintaa omalta osaltaan.

API-manifestia noudattamalla varmistetaan hyvä palvelu. Jotta tässä onnistutaan, tulee varmistaa että kaikki julkisen sektorin organisaatiot omaksuvat ja toteuttavat API-manifestin ajatuksen. Kaikilta julkisen sektorin organisaatioilta voidaan edellyttää avointa, sitoutunutta ja yhdenmukaista toimintaa niiden avointen rajapintojen ja avoimen datan kautta palvelemisessa.

Avoimet rajapinnat eivät tarkoita julkishallinnon toimintojen ulkoistamista. Varsinkaan vastuuta ei voi koskaan ulkoistaa. Erityisesti perusinfrastuktuurin ulkoistaminen kokonaan on kyseenalaista.

Anonyymit datamassat, big data, sisältävät suuren potentiaalin, myös liiketoiminnalle. Datamassoja liiketoiminnassa hyödyntävät yritykset keskittyä datamassojen myyntiin, jalostamiseen tai analysointiin.

Jotta anonyymien datamassojen liiketoimintamalleja voidaan tutkia, joudutaan luopumaan vaateesta *absoluuttisen* yksityisyyden suojan osalta. Sen sijaan anonyymius tulee nähdä suhteellisena ja täytyy hyväksyä mahdollisuus, että riittävillä resursseilla ja tietotaidolla anonymisoinnin purkaminen on aina mahdollista. On siis aina olemassa mahdollisuus, että yksittäisiä käyttäjiä voidaan tunnistaa datamassasta anonymisointiyrityksistä huolimatta.

Haittaohjelmien päätelaitteiden torjuntaratkaisuissa on ollut jonkin aikaa jo lisääntymässä sovelluskontrollointi (Application Control) ja siihen liittyen sallittujen sovellusten tai tiedostojen listat, sekä torjuntaratkaisut, jotka tunnistavat haittaohjelmille tyypillistä käyttäytymistä ja sitä kautta haittaohjelmia paremmin kuin tunnisteisiin perustuvat ratkaisut. Laitteiden konfiguraatiot ovat avainasemassa: oikein säädetyt laitteet ovat olennainen osa hyvää tietoturvaa.

Pelkillä teknologisilla ratkaisuilla ei kyetä saamaan tehokkainta mahdollista suojausta: Kuluttajilla ja yrityksillä – myös pienyrityksillä – tulisi olla riittävät resurssit, kiinnostus ja kompetenssi laitteiden konfigurointia ja hälytysten analysointia varten. Näin ei useinkaan ole.

Huoltovarmuuskriittisille toimijoille valtiolliset instanssit tarjoavat asiantuntijapalveluita ensisijaisesti poikkeamahavaintojen analysointiin ja ratkaisukeinoja käytettävissä olevien resurssien puitteissa. Lisäksi on käytettävissä kaupallisia tietoturvapalveluita,

Kaupalliset palvelut haitallisten vaikutusten arvioimiseksi koostuvat asiantuntija- ja konsultointipalveluista, kuten riskien vaikutusten arvioimisesta etukäteen (riskienhallinta ja ohjelmistokoodin analysointi), piilevien riskien löytämiseen liittyvistä palveluista sekä toteutuneiden riskien vaikutusten analysointipalveluista.

Tietoturvariskejä koskevien tietojen jakaminen on äärimmäisen keskeistä. Julkiset toimijat jakavat tietoa hallitusti suljettujen toimialakohtaisten ryhmien kesken. Asiantuntijaverkostot ovat myös tärkeitä. Yksittäisten työntekijöiden muodostamat epäviralliset ja viralliset verkostot muodostavat yksityisille toimijoille yhden tärkeimmistä tiedonjakokanavista. Esimerkiksi Viestintäviraston Kyberturvallisuuskeskus ylläpitää viestintäkanavia muun muassa huoltovarmuuskriittisillä toimialoilla. Organisaation tulisi miettiä, mitä tietoa voi itse tuottaa kyseiseen kanavaan ja olla halukas jakamaan muita hyödyttävää tietoa. Tietoa pitäisi myös pystyä jalostamaan liiketoiminnan ymmärtämään muotoon

Hyviä yleisesti tunnettuja käytänteitä tietoturvan ja -suojan kehittämiseen on paljon tarjolla. Käytänteitä tarjoavat muun muassa standardointielimet, tietoturvayhteisöt sekä valtiolliset ja kansainväliset toimijat. Käytänteiden etsijän haasteena on poimia itselle parhaiten sopivat käytänteet runsaasta tarjonnasta.

Yksi ongelma on, että toteutuneista tietoturvariskeistä ei aina haluta jakaa tietoa. Yksi ratkaisu voisi olla Chatham House -sääntö. Sääntöä noudattaessa tieto on riisuttu sen jakaneen tahon tunnistustiedoista, jolloin kynnys tietojen jakamisen laskee.

Jotta tietoturvapalveluita voidaan kehittää systemaattisesti ja implementoida käyttöön yhteiskunnan eri tasoilla, tulee luoda kokonaisvaltainen kuva eri tietoturvapalveluista ja niiden merkityksestä. Palvelut liittyvät verkostomaisesti toisiinsa ja vasta kokonaisuus voi luoda turvallisuuden. Tietoturvapalvelujen kategorisointi tuo näkyväksi, minkälaisia palveluita on olemassa, ja sen avulla voidaan kartoittaa, mitä palvelukombinaatioita voidaan käyttää erilaisten riskien hallinnassa.

Kuluttajien ja yritysten kokonaiskuva tietoturvapalveluista ei ole kattava terminologian ja palvelujen hajanaisuudesta johtuen. Tässä onkin mahdollisuus edistää tietoturvaa ja siihen liittyvää liiketoimintaa tarjoamalla tarkkaa ja laajaa ohjeistusta kokonaisvaltaiseen tietoturvakartoitukseen. Tässä Valtionhallinnon tietoturvallisuuden johtoryhmä on toimija, joka voisi ottaa edelläkävijän roolin ja tukea näin tietoturvallisuuden kehittymistä suomalaisessa yhteiskunnassa.

Liite 1. Verkkokyselyssä esitetyt väittämät ja kysymykset

Väittämät:

1. Tunnistan salausta käyttävän web-sivuston.
2. Koen salausta käyttävällä web-sivustolla asioinnin luotettavaksi.
3. Koen voivani riittävissä määrin vaikuttaa siihen, kuinka palveluntarjoaja käyttää palveluun tallentamiani tietoja.
4. Tiedän, kuinka ja mistä pyytää omien tietojeni poistamista tai tarkistamista sähköisestä palvelusta.
5. Haluan itse määritellä, mihin tarkoitukseen henkilötietojani käytetään.
6. Koen, että sähköisissä palveluissa ilmaistaan selkeästi, millaisia tietosuojakäytänteitä palvelu soveltaa.
7. Koen digitaalisten terveyspalveluiden käytön luotettavaksi.
8. Minulle on merkityksellistä, kuka on palveluntarjoaja.
9. Minulle on tärkeää, että palveluntarjoaja on tunnettu toimija.
10. Tunnen tietosuojalainsäädännön vaikutuksen tietojeni käsittelyyn.

Asteikko:

1: Täysin eri mieltä
2: Jokseenkin eri mieltä
3: En samaa enkä eri mieltä
4: Jokseenkin samaa mieltä
5: Täysin samaa mieltä

Kysymykset:

1. Kuinka paljon kiinnität huomiota tietoturvaan ja tietosuojaan silloin, kun käytät digitaalisen palvelun maksuominaisuuksia tai tunnistaudut verkkopankin kautta Internetissä?
2. Kuinka paljon kiinnität huomiota tietoturvaan ja tietosuojaan silloin, kun luovutat tietojasi verkko- tai sosiaalisen median sivustoille, joissa ei kulje maksuliikennettä?
3. Kiinnitätkö huomiota siihen, onko digitaalisia hyödykkeitä tai niitä tarjoavia organisaatioita arvioitu ulkopuolisen tahon toimesta (arviointilaitoksen myöntämä sertifikaatti hyödykkeen tai organisaation turvallisuudesta, esim. ISO 27001)?
4. Kuinka paljon edellä mainittu ulkopuolisen tahon tekemä arviointi hyödykkeen tai organisaation turvallisuudesta (sertifiointi) vaikuttaa kokemaasi luottamukseen palvelua kohtaan?
5. Kuinka tietoinen olet edellä mainittujen arviointien tai sertifiointien arviointikriteeristöistä ja niihin vaikuttavasta lainsäädännöstä?

Liite 2. Haastattelujen teemat ja haastatellut asiantuntijat

1. Millaisia kaupallisia ja julkisia palveluita tietojärjestelmien ylläpitäjillä sekä käyttäjillä on piilevien tietoturvariskien havainnoimiseksi?

2. Millaisia kaupallisia ja julkisia palveluita tietojärjestelmien ylläpitäjillä sekä käyttäjillä on piilevien tietoturvariskien haitallisten vaikutusten arvioimiseksi?

3. Millaisia kaupallisia ja julkisia palveluita tietojärjestelmien ylläpitäjillä sekä käyttäjillä on piilevien tietoturvariskien pienentämiseksi tietoa jakamalla?

4. Mitkä ovat parhaita käytäntöjä, joiden mukaisesti em. palveluita voidaan toisiaan täydentäen käyttää turvaamaan ohjelmistohaavoittuvuuksia koskevien tietojen jakamiseen sekä tietoturvariskien pienentämiseen?

Henkilö	Organisaatio	Ajankohta	Asema / Rooli
Jari Pitkänen	KPMG Suomi	10.4.2016	Cyber Security Services,Manager
Jeroen de Wit	KPMG Hollanti	17.11.2016	Cyber Security Services, Manager
Tuomas Juntunen	Databasement Oy	25.11.2016	Teknologiajohtaja
Aki Levänen	Telia Company	14.12.2016	Senior Business Manager / Cyberturvallisuus liiketoiminta
Mikko Vatanen	KPMG Suomi	29.12.2016	Cyber Security Services, Manager
Tommi Vänninen	Telia Company	1.5.2017	Offering Lead Managed Security
Tomi Pitkänen	Neste Oyj	9.2.2017	Head of ICT Security

VALTIONEUVOSTON
SELVITYS- JA TUTKIMUSTOIMINTA

tietokayttoon.fi

ISSN 2342-6799 (pdf)
ISBN 978-952-287-524-2 (pdf)