



LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Julkisten lähteiden riskit henkilöturvallisuudessa

Haaranen, Markus

2017 Laurea



Laurea-ammattikorkeakoulu

Julkisten lähteiden riskit henkilöturvallisuudessa

Markus Haaranen
HSA216KA
Opinnäytetyö
Huhtikuu, 2017

Markus Haaranen

Julkisten lähteiden riskit henkilöturvallisuudessa

Vuosi 2017 Sivumäärä 60

Digitalisoituvassa nykyyhteiskunnassa henkilöstä tallentuva tietomäärä on erittäin laaja. Eri-laisiin tietokantoihin päätyy henkilön yksilöiviä tietoja, joista iso osa on julkisia eli kaikkien saatavilla. Tiedot päätyvät rekistereihin, järjestelmiin ja palveluihin hyvin eri tavalla ja henkilön on hyvin vaikea ymmärtää sitä, kuinka kattavan kuvan hänestä saa, kun näitä tietoja yhdistetään. On selvítettävä, miten ja mitä henkilöä yksilöivää tietoa päätyy julkisesti haettavaksi ja miten tätä tietoa voidaan hankkia ulkopuolisen tahon toimesta.

Yksittäiselle henkilölle julkisesti haettavat tiedot muodostavat henkilöturvallisuusrisikin. Tiedonmuruksesta koottu kokonaisuus voi paljastaa erittäin henkilökohtaista tietoa ihmisestä, jota voidaan käyttää hyväksi esimerkiksi henkilöön kohdistuvissa uhkaus- tai painostamistilanteissa. Riski ei rajaudu ainoastaan yksittäiseen henkilöön, vaan julkisesti haettavia tietoja voidaan hankkia myös henkilön lähipiiristä ja näin tehostaa haluttua uhkakuvaa.

Opinnäytetyön aiheena käsitellään julkisten lähteiden aiheuttamia riskejä henkilöturvallisuudelle. Tutkimuksessa otetaan kantaa siihen, kuinka suomalaisesta henkilöstä päätyy tietoja julkisesti haettavaksi ja millaisia mahdollisuuksia henkilöllä on ennaltaehkäistä ja poistaa julkisiksi päätyneitä tietoja. Kyseessä on kehityshanke, jonka avulla pyritään luomaan yksiker-tainen tietoa tiivistävä malli. Mallin avulla on mahdollista saada nopea kokonaiskuva riskeistä ja keinoista ennaltaehkäistä niistä syntyvää uhkaa. Uhkamalli on jaettu kahteen osaan, tarjo-ten näin visuaalisen ja kirjallisen kuvauksen tutkittavasta aiheesta.

Tutkimus on laadullinen eli kvalitatiivinen ja se on laadittu toimintatutkimusmenetelmän avulla. Opinnäytetyö on jaoteltu siten, että julkiset lähteet on jaettu passiivisiin ja aktiivisiin lähteisiin. Tutkimuksessa käsitellään passiivisina lähteinä, suomalaisia julkisia lähinnä valtionhallinnon ylläpitämiä rekistereitä ja niiden tietojärjestelmiä. Aktiivisina julkisina lähteinä on avattu sosiaalisen median mukanaan tuomia uhkia, sekä henkilön yksilöivien tietojen, kuten sähköpostin, hyväksikäyttöä julkisten lähteiden tiedonhankinnassa. Työn teoriapohja perustuu kirjallisuuskatsauksessa hyödynnettyyn tutkimuskirjallisuuteen, artikkeleihin, ohjeistuksiin ja rekisteriselosteisiin.

Tutkimus tuo hyvin kattavasti esille julkisesti haettavien, henkilöä yksilöivien tietojen muodostumisen, sekä antaa yksiselitteisiä neuvoja siitä miten tietoja voidaan hakea ja miten tiedon päätymistä julkiseksi voidaan rajata. Lisäksi työssä huomioidaan henkilön lakisääteisiä oikeuksia koskien hänen yksityisyydensuojaansa. Tutkimuksen tarkoituksena ei kuitenkaan ollut tehdä kaiken tiedon kattavaa kokonaisuutta, vaan antaa työn lukeville yleiskatsaus ilmiöstä ja sen luomista uhista. Tiivistettyjä uhkamalleja voidaan hyväksikäyttää henkilöstön ohjeistuksen perustana.

Asiasanat: Henkilötieto, Henkilötiedustelu, OSINT, Julkiset lähteet

Markus Haaranen

Risks of Public Sources in Personal Security

Year	2017	Pages	60
------	------	-------	----

The amount of data that is stored in the modernizing society today is very large. Various databases are endowed with individual information, most of which are public and accessible to all. The data derives from registers, systems and services in different ways, and it is very difficult for a person to understand how a comprehensive picture of him can be obtained, when this information is combined into a single entity. It is necessary to examine how and by whom the personal data is made public and how this information can be obtained by an outsider.

Information that is publicly available for a person is a personal security risk. A collection of information can reveal highly personal information about a person that can be exploited for example in threatening situations. The risk is not limited to a single person, but publicly available information can also be obtained on a target-related person, thereby enhancing the desired threat.

The topic of the thesis is the risks posed by public sources for personal security. The study focuses on how personal information on a Finnish person, ends up available for outsiders to see and what kind of opportunities a person has to prevent this threat and how he can remove publicly accessible information. The study is a development project that seeks to create a simplistic model. The model allows a quick overview of the risks and means of preventing the threats arising from them. The threat model is divided into two sections, providing a visual and written description of the topic investigated.

The research is qualitative and it is based on a action research method. The subject of the Bachelor's thesis is divided into passive and active open sources. The study examines public, mostly Finnish government-maintained registers and their information systems. As active public sources, the threats posed by social media and the use of personal information, such as e-mail, have been depicted. The thesis is based on research literature, articles, guidelines and registration notes used in the literature review.

The research is comprehensive and it raises awareness of publicly open personal information, as well as provides unambiguous advice on how to retrieve data and how to narrow the information that is public. In addition, the person's statutory rights regarding their privacy are taken into account. However, the purpose of the study is not to establish a comprehensive set of information but to provide an overview of the phenomenon and the threats it created. The summarized threat models can be used as a basis for personnel guidance.

Keywords: HUMINT, Open sources, OSINT, Personal data

Sisällys

1	Johdanto.....	7
	1.1 Opinnäytetyön tarkoitus, tavoite ja rakenne	7
	1.2 Opinnäytetyön käsitteet.....	11
2	Julkiset lähteet osana nyky-yhteiskuntaa	13
	2.1 Sosiaalinen kanssakäyminen	14
	2.2 Internetin kautta tapahtuva henkilötiedustelu ilmiönä ja uhkana	16
3	Passiiviset julkiset lähteet.....	18
	3.1 Väestötietorekisteri ja väestötietojärjestelmä (VTJ).....	19
	3.2 Ajoneuvoliikennerekisteri ja ajoneuvotietojärjestelmä (ATJ)	19
	3.3 Patentti- ja rekisterihallitus (Virre)	22
	3.3.1 Kaupparekisteri	22
	3.3.2 Yhdistysrekisteri	24
	3.4 Oikeusrekisterikeskus.....	25
	3.5 Luottorekisteri	26
	3.6 Ulosottorekisteri.....	26
	3.7 Kiinteistörekisteri ja kiinteistötietojärjestelmä (KTJ).....	26
	3.8 Teleoperaattorit ja numeropalvelut.....	27
	3.9 Julkinen esiintyminen ja harrastukset	28
4	Miten estää henkilötietojen selvittäminen julkisista rekistereistä	29
	4.1 Maistraatista ja väestörekisterikeskuksesta haettavat henkilötietojen luovutuskiellot.....	29
	4.1.1 Suoramarkkinointi-, henkilömatrikkeli- ja sukututkimuskielto	30
	4.1.2 Yhteystietojen luovutuskielto ja asiakasrekisterin päivityskielto	30
	4.1.3 Turvakielto	31
	4.1.4 Väestötietojärjestelmän tietojen hyödyntäminen.....	32
	4.2 Ajoneuvon omistajan tai haltijan tiedot.....	32
	4.3 Salainen numero.....	33
	4.4 Yritystoiminnan piilottaminen.....	33
	4.5 Muut tahot.....	33
5	Aktiiviset julkiset lähteet.....	34
	5.1 Sosiaalinen media	35
	5.2 Kuvien ja videoiden metadata	37
	5.3 Muut verkkoyhteisöt	38
	5.4 Pikaviestisovellukset.....	38
	5.5 Sähköposti	39
6	Miten suojautua aktiivisissa lähteissä ja oikeus omaan yksityisyyden suojaan	40
	6.1 Kertakäyttöinen sähköposti.....	41

6.2	Tiedon näkyvyys internethakukoneissa	42
6.3	Tieto on näkyvillä vaikka se on poistettu varsinaisesta lähteestä	43
7	Opinnäytetyön tulokset	44
	7.1.1 Uhkamallikuvio.....	44
	7.1.2 Uhkamalli	45
8	Johtopäätökset	50
	8.1 Työelämää hyödyntävät vaikutukset	53
	Lähteet	55
	Kuvat:.....	59
	Kuviot.....	60

1 Johdanto

Internet lukeutuu läntisessä maailmassa perusoikeuksiin ja se on osa päivittäistä arkea. Olemme jatkuvasti jonkin tietoverkkoon kytkeytyneen laitteen vaikutuspiirissä ja jos olisi mahdollista päästä käsiksi kaikkeen henkilöstä tietoverkkoihin päätyvään dataan, kattaisi se lähes jokaisen elämässä tapahtuvan asian. Julkisesti tämä kaikki data ei kuitenkaan ole esillä ja vain osaan on helppo päästä käsiksi.

Internetiin kytköksissä olevien laitteiden määrä jatkaa kasvuaan ja jollain tapaa päivitämme itsestämme tietoa tietoverkkoihin jatkuvasti. Tieto voi olla ns. metadataa eli pieniä "yksilöimättömiä" tiedonjyviä, joita isot internetjättiläiset kuten Google tai Microsoft hyödyntävät kohdennetussa mainonnassa. Tieto voi olla myös itsemme jakamaa tietoa, jonka ajattemme jakavamme ainoastaan lähipiirille, kuvan tai tilapäivityksen muodossa. Lisäksi meistä rekisteröidään tarkkoja henkilötietoja viranomaisten käyttämiin väestörekistereihin, joista tietoa myydään eteenpäin kolmansille osapuolille.

Nykyaikana ihmisen jättämä täysin julkinen digitaalinen jalanjälki on kuitenkin massiivinen. Tietoverkkoihin sekä erilaisiin tietokantoihin päätyy henkilöistä tietoa, halusi sitä tai ei. Suuret hakukonepalvelut indeksoivat osan tästä tiedosta hyvinkin helposti haettavaksi tiedoksi, johon kaikilla nettiyhteyden omaavilla on helppo pääsy. Kuka ei ole hakenut omalla nimellään esiin tulevia tietoja hakukonepalveluista tai selvittänyt alustavasti tulevan treffiseuran sosiaalisen median tiliä, ennen ensimmäistä tapaamista?

Tietojen löytämisen helppous aiheuttaa yksilölle turvallisuusongelman. Julkisesti löydettävissä olevat tiedot pystytään helposti kasamaan isommaksi ja tarkemmaksi kokonaisuudeksi, jonka avulla yksittäisestä henkilöstä voidaan luoda kattava profiili. Tätä profiilia voidaan käyttää hyväksi monella tapaa. Se voi olla oikeanlaisen ihmissuhteen löytämistä, yrityksen rekrytointikäytäntöä tai sitä hyödynnetään henkilöön kohdistuvissa uhkaustilanteissa.

1.1 Opinnäytetyön tarkoitus, tavoite ja rakenne

Nykypäivänä tietoturvariskit ja tiedonkeruun vaarat ovat saavuttaneet valtavirran. Tästä on pitänyt huolen Edward Snowdenin paljastukset NSA:n jättimäisestä tiedonkeruusta sekä useat muut tietovuotoskandaalit. Euroopassa tähän on herätty niin kansallisesti kuin EU-tasolla. Euroopan unionin uusi tietosuojalainsäädäntö on jo astunut voimaan ja sen toimeenpanemiseksi ponnistellaan kansallisella tasolla. Silti yksilötasolla käsitys siitä mikä on julkisesti löydettävissä ja kuinka juuri yksittäisen henkilön tiedot saattavat kiinnostaa jotain

tahoa, ovat edelleen huonolla tasolla (Pew Research Center 2016). Ihmiset antavat henkilötietojaan yritykselle ilmaiseksi, jotta saavat käyttöönsä palveluita ja samalla uskovat sokeasti siihen, että vain omaa lähipiiriä saattaa kiinnostaa yksilön julkaisemat mm. perhekuvat.

Julkisten lähteiden ja sen osan sosiaalisen median kautta on pystytty todistamaan esimerkiksi se, että Venäjän sotilashenkilöstöä oli Ukrainassa Krimin valtauksen yhteydessä, vaikka Venäjä kiisti nämä toimet (The Guardian 2015). Artikkelin antaa hyvän kuvan siitä, että kaikki henkilöt ovat jollain tavalla kytköksissä internetiin, vaikka esimerkin henkilöt toimivat kokonaisen valtion salaamassa operaatiossa.

Eräässä valtion virastossa oltiin havahduttu uhkakuvaan siitä, että jokin henkilö pystyy selvittämään helposti toisen henkilön tietoja ja käyttää niitä uhkaavassa tai painostavassa mielessä. Tämä on lisäksi huomattavasti helpompaa tehdä muutamalla haulilla kotikoneelta, kuin lähteä fyysisesti seuraamaan kohdetta. Tämän lisäksi uhkausta voi painottaa liittämällä siihen yksityiskohtaisia tietoja kohteen lähipiiristä.

Opinnäytetyön tarkoituksena on tarkastella julkisia tiedonhakulähteitä ja mahdollisuuksia kerätä tietoa indeksoidusta osasta tietoverkkoa eli periaatteessa siitä osasta internettiä mikä on löydettävissä internethakukonepalveluilla. Tutkimuksessa tarkastellaan asiaa henkilöstöturvallisuuskäytännöstä ja pureudutaan siihen mitä kautta henkilötietoja päätyy julkisesti haettavaksi. Tarkasteltaessa varsinaista tutkintaongelmaa, selvitetään samalla keinoja torjua henkilötietojen päätymistä kaikkien saataville.

Opinnäytetyöhön ei liity varsinaista toimeksiantoa. Tutkimus kuitenkin tehdään erään valtionhallinnon viraston tarpeesta ja sitä tullaan hyväksikäyttämään käytännön työn helpottamiseksi ja tulevan henkilöstön ohjeen pohjana. Opinnäytetyön tuloksena luodaan tietoa tiivistävä malli, jota voidaan käyttää henkilöstöturvallisuuden kehittämisessä ja julkisten lähteiden kokonaisvaltaisen henkilöturvallisuusongelman hahmottamisessa. Opinnäytetyön tuloksi esitetään paremmin luvussa 7.

Opinnäytetyön tavoitteena on pyrkiä luomaan lukijalle tiivistetty näkemys niistä pääpiirteistä, miten tieto Suomessa päätyy julkisesti haettavaksi ja kuinka henkilö voi omilla toimillaan määrittää mitä tietoa hänestä on saatavilla. Tiivistetyn tiedon tueksi ja ymmärtämiseksi opinnäytetyössä tuodaan esille joitain tapoja hakea ja selvittää henkilön tietoja julkisista lähteistä.

Opinnäytetyö on jaoteltu siten, että julkiset lähteet on jaettu passiivisiin ja aktiivisiin lähteisiin. Tutkimuksessa passiivisina julkisina lähteinä käsitellään suomalaisia lähinnä

valtionhallinnon ylläpitämiä, rekistereitä ja niiden tietojärjestelmiä. Aktiivisina julkisina lähteinä on avattu sosiaalisen median mukanaan tuomia uhkia, sekä henkilöä yksilöivien tietojen, kuten sähköpostin, hyväksikäyttöä julkisten lähteiden tiedonhankinnassa.

Lisäksi tutkimuksessa tuodaan esille niitä oikeuksia mitä Suomen kansalaisella lakimääritteisesti on, koskien hänen omia henkilötietojaan ja yksityisyydensuojaa. Yksityisyyden suojalla tarkoitetaan yksilön oikeuksia omaan yksityiselämäänsä ja yksityisyyteensä silloin kun häntä yksilöiviä tietojaan käsitellään (Minilex - 2017).

Opinnäytetyö on rajattu siten, että tutkimuksessa tarkastellaan Suomessa käytössä olevien julkisten rekistereiden tiedonkeruuta ja tämän tiedon hankkimista kolmannen osapuolen toimesta. Opinnäytetyö keskittyy käsittelemään julkisten lähteiden varassa tapahtuvaa henkilötiedustelua enemmänkin normaalin tietokoneen käyttäjän näkökulmasta eli avoimen indeksoidun internetin osalta. Lisäksi tutkimuksessa havainnollistetaan pääpiirteittäin sosiaalisen median ja muiden yksilöivien tietojen, kuten sähköpostin mahdollisuuksia kokonaisvaltaisen henkilöprofiilin selvittämiseksi. Tarkoituksena on luoda karkea kokonaiskuva riskeistä, joita erilaiset julkiset lähteet tuottavat yksittäisen ihmisen henkilöturvallisuudelle.

Tutkimuksen tarkoitus ei ole olla täysin kattava tietopaketti julkisten lähteiden tiedustelusta, vaan enemmänkin antaa lukijalle kokonaiskuva julkisen tiedonkeruun riskeistä. Lisäksi työtä rajataan siten, että tiedonhankintamenetelmät eivät riko Suomen lainsäädäntöä. Kokonaisuutena tutkimuksessa käytettävä aineisto on laaja ja sen rajaaminen hankalaa. Kirjallisuuskatsauksen ja lähdemateriaalin avulla pyritään rajaamaan tutkimuksessa käsiteltäviä keskeisiä aihealueita.

Opinnäytetyön viitekehys pohjautuu yksilön yksittäisten henkilötietojen tiedusteluun julkisista lähteistä. Tiedustelu on erilaisiin tiedon lähteisiin kohdistuvaa tiedonhankintaan, jonka tarkoituksena on tuottaa parempi kokonaiskuva tarkkailtavasta kohteesta (Puolustusministeriö 2015, 20). Tätä tiedustelua tehdään tietoverkon julkisista lähteistä henkilötiedustelun keinoin.



Kuvio 1: Tiedustelusykli (Puolustusministeriö 2015, 15)

Aihetta käsitellään osissa, joiden kautta avataan julkisten lähteiden varassa tapahtuvan henkilötiedustelun keinoja sekä menetelmiä. Lisäksi tutkimuksessa käsitellään yksittäin merkityksettömien tietojen kautta syntyvää uhkaa. Tämä uhka syntyy, kun tiedonpalasia kasataan ja analysoidaan isommaksi kokonaisuudeksi sekä tiedonhankintaa kohdistetaan uudelleen jo hankittujen tietojen perusteella tiedustelusyklin mukaisesti (Kuvio 1). Tietojen alkuperä ei ole sidoksissa henkilön itsensä jakamiin tai hänestä löytyviin muihin julkisiin tietoihin, vaan kokonaisuuteen on myös kytkettävissä henkilöön kontaktissa olevat tahot ja tapahtumat, joiden kautta tarkkailtavan kohteen tietoja voi valua julkisiksi. Ilmiön avaaminen edesauttaa henkilöä siinä, millä tavoin hän voi vaikuttaa omilla toimillaan itsestään löytyvään julkiseen tietoon ja lisäksi tutkimuksessa tuodaan esille, kuinka henkilö voi rajata tietojensa näkyvyyttä julkisissa lähteissä, sekä osittain poistaa niitä.



Kuvio 2: Opinnäytetyön viitekehys

Opinnäytetyön tutkimusmenetelmät. Opinnäytetyö on toimintatutkimus, jonka avulla pyritään etsimään ratkaisu käytännön ongelmaan eli julkisten lähteiden aiheuttaman henkilöturvallisuusriskin kokonaisvaltaisempaan ymmärtämiseen. Toimintatutkimuksen tarkoituksena on selvittää organisaatiossa ilmeneviä tosielämän ongelmia ja luoda uutta tietoa sekä ymmärrystä asiasta. Toimintatutkimuksessa on tärkeää käytännönläheisyys ja ihmisten aktiivinen osallistuminen. Tutkimuksessa tutkimuskysymykset ovat muodostuneet tutkijan työelämässä huomioitujen ongelmakohtien ympärille. Näin tutkimuksessa ihmisten tuomat ongelmat ovat apuna tutkijan teoreettisen pohjan hankinnassa. Vaikka opinnäytetyön lopullisten tiivistettyjen mallien hyödyntäminen jää valtion viraston vastuulle, tullaan mallit arvioimaan kyseisen organisaation toimesta. (Ojasalo, Moilanen & Ritalahti 2015, 58)

Opinnäytetyö on laadullinen eli kvalitatiivinen, ja sen tarkoituksena on todellisen elämän ja tapahtumien kuvaaminen. Kvalitatiivisessa tutkimuksessa pyritään tutkimaan aihetta mahdollisimman kokonaisvaltaisesti (Hirsjärvi, Remes & Sarjavaara 2001, 152).

Opinnäytetyön teoreettisena perustana käytetään kirjallisuuskatsausta, joka keskittyy tutkimusongelman kannalta tarpeelliseen kirjallisuuteen, lakiteksteihin, ohjeistukseen ja internetlähteisiin. Tutkimuksen tarkoituksena on tuoda lukijalle esille aiheeseen liittyvää tietoa ja kartuttaa myös tutkimuksen tekijän tietoutta aihepiiristä. (Hirsjärvi, Remes & Sarjavaara 2001, 108-109)

Koottu tutkimustieto tiivistetään uhkamalliksi ja visuaalisesti havainnollistavaksi uhkamallikuviksi dokumenttianalyysin avulla. Dokumenttianalyysi on menetelmä, jonka avulla tehdään päätelmiä mm. erilaisen kirjallisen materiaalin esim. lehtileikkeiden ta www-sivujen avulla. Aineistolähtöiseen sisältöanalyysiin kuuluu aineiston pelkistäminen, jonka tarkoituksena on parantaa aineiston ymmärrettävyyttä. Uhkamallin ja uhkamallikuvion tarkoituksena on tuottaa selkeä kokonaiskuva julkisten lähteiden pääpiirteistä ja niiden luomista uhista. Uhkamalliin liitetään ennaltaestävien ja takautuvien torjuntatoimien mahdollisuudet ja niiden kytkeytyminen julkisten lähteiden tietojen hankintaan. (Hirsjärvi, Remes & Sarjavaara 2001, 136-140)

1.2 Opinnäytetyön käsitteet

Tässä luvussa tuodaan esille opinnäytetyön käsitteet tiivistetysti. Näiden käsitteiden merkitystä tutkimuksessa tarkastellaan tutkimuksen aikana eri näkökulmista.

Aktiiviset julkiset lähteet ovat julkisesti löydettäviä tietoja joita henkilö itse itsestään julkaisee tai antaa aktiivisesti julkaistavaksi. Aktiivisten julkisten lähteiden suurin osa-alue on sosiaalisen median palvelut. Aktiiviset julkisille lähteille on myös tunnusomaista se, että niitä

ei kosketa lain määrittämät laadulliset edellytykset, eikä tietojen ylläpitäjällä ole välttämättä lakimääritteistä vastuuta henkilötietojen käsittelystä. Henkilön on vaikea ymmärtää mitä tietoa hänestä on julkisesti haettavissa näiden lähteiden kautta.

Avointen lähteiden tiedustelu eli Open Source Intelligence (OSINT) on julkisiin lähteisiin, kuten kirjallisuuteen, karttoihin, lehtiin ja julkisiin asiakirjoihin sekä Internet-sivustoihin kohdistuvaa tiedonhankintaa (Puolustusministeriö 2015, 16).

Henkilötiedoilla tarkoitetaan luonnollista henkilöä koskettavia kaikenlaisia yksilöiviä tietoja. Nämä tiedot voivat kuvata henkilön ominaisuuksia tai elinolosuhteita ja ne kattavat hänen perheensä tai samassa taloudessa asuvat henkilöt (Henkilötietolaki 22.4.1999/523).

Henkilötiedustelu eli Human Intelligence (HUMINT) on henkilön kanssakäymisen tai kohteen havainnointiin perustuvaa tiedustelua. Tiedustelu voi tapahtua monin eri keinoin kuten suullisesti lähestyen henkilöä, mutta sitä voidaan suorittaa myös tietoverkkojen kautta (Puolustusministeriö 2015, 16).

Julkisilla lähteillä tarkoitetaan sellaisia tietoja, jotka ovat julkisia ja avoimia kanavia pitkin saatavilla. Tiedot päätyvät joko lakisääteisesti viranomaisten rekistereihin, henkilö itse julkaisee tiedon tai joku muu henkilöön kytköksissä oleva taho julkaisee tiedon siten, että tieto on avoimesti kaikkien löydettävissä. (CIA 2010)

Passiiviset julkiset lähteet ovat sellaisia, joita henkilö ei itse tuo julki ja jossain tapauksessa edes tiedosta, että sellaisia tietoa hänestä on haettavissa. Ne pitävät sisällään niitä tietoja jotka päätyvät tietokantoihin julkisuuslain ja henkilötietolain nojalla. Tätä varten on määritelty laki viranomaisten toiminnan julkisuudesta eli ns. julkisuuslaki ja henkilön yksityisyydensuojaa turvaava henkilötietolaki. Lisäksi henkilöstä valuu passiivisesti tietoja julkisiin kantoihin esimerkiksi harrastustoiminnan tai vastuutehtävän vuoksi.

Tiedustelu on erilaisiin lähteisiin perustuvaa tiedonhankintaa. Tietolähteet voivat olla julkisia tai ei-julkisia. Tiedustelun tarkoituksena on kartoittaa ja lisätä ymmärrystä tarkkailtavasta kohteesta tai ilmiöstä. Tiedustelun tarkoituksena on tuottaa varhaisvaiheen tietoa, jota voidaan käyttää hyväksi siinä tarkoituksessa mitä varten tietoa ollaan kasaamassa. Tiedustelun yhtenä osana on tiedon analysointi, jonka avulla kerätty tieto jäsenellään ja näin tiedonhankintaan voidaan jatkaa ja tehostaa. (Puolustusministeriö 2015, 15)

Yksityisyyden suoja on luonnollisen henkilön oikeus suojautua ulkopuolisen tahon, kuten valtion, puuttumiselta. Yksityisyyden suojalla tarkoitetaan yksilön oikeuksia omaan yksityiselä-

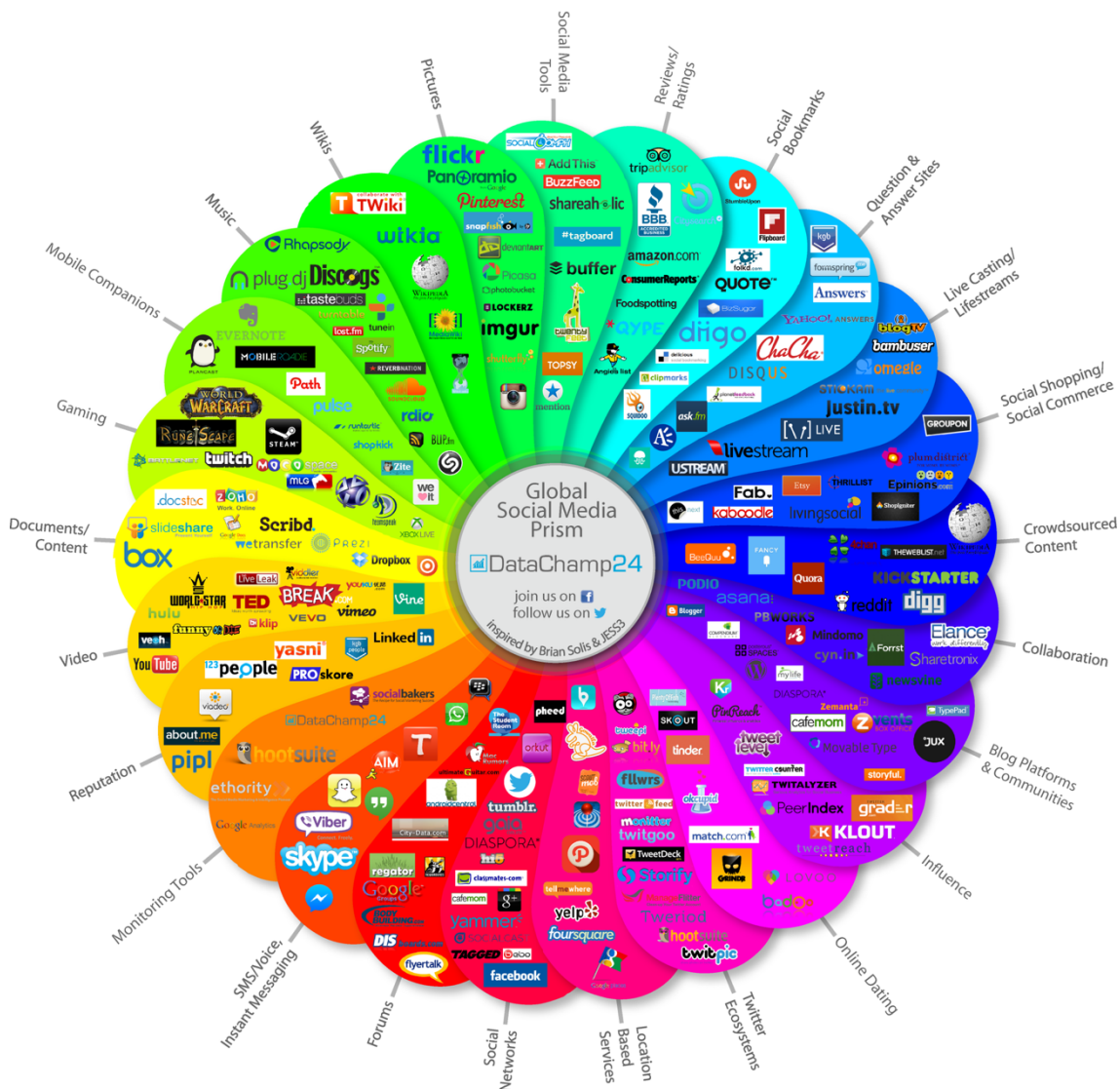
määnsä ja yksityisyyteensä silloin kun häntä yksilöiviä tietojaan käsitellään. Yksityisyyden suojaan kuuluu perusoikeus yksityisen elämän suojasta.

2 Julkiset lähteet osana nyky-yhteiskuntaa

Nyky-yhteiskunnassa lähes kaikesta jää jonkinlainen sähköinen jälki. Puhelin hakee tauotta sijaintitietoa liikkeistä ja tarkentaa tätä tietoa yhdistelmällä langattomien verkkojen vierailutietoja. Isot tietoliikenneyritykset kuten Google, tallentaa kaikki suoritettut haut, verkkovierailut ja jopa yksityiset sähköpostit jättimäisiin palvelinkeskuksiinsa ja internetselaimet seuraavat käyttäjän toimintaa ja klikkauksia verkossa. Mikäli tähän kaikkeen tietoon pääsisi käsiksi, kertoisi se tarkemman kuvan henkilöstä kuin mitä hän itse pystyisi tuomaan esille (Järvinen 2010, 9). Tästä hyvänä esimerkkinä on Target yrityksen tapaus, jossa tyttären isä oli rynnännyt vihaisena kauppaan vaatien yritykseltä anteeksipyyntöä sen vuoksi, että hänen tyttärelleen tulee raskauteen liittyviä alekuponkeja postitse. Target oli pystynyt päättämään tyttären olevan raskaana, seuraamalla tyttären käyttäytymistä internetissä yrityksen omilla sivustoilla. Isä joutui pyytämään anteeksi käytöstään (Techland 2012). Suurvallat satsaavat tiedon keräämiseen ja kehittävät järjestelmiä ja menetelmiä suodattaa ja analysoida tätä laajaa alati kasvavaa datamäärää.

Yksityisyys on siinä määrin menettänyt muotonsa verrattuna aikaan ennen tietokoneita ja tietoverkkoja. Nyky-yhteiskunnassa on mahdollista tietää tarkasti mitä jokin yksilö tekee, eikä se enää välttämättä vaadi isoa tiedusteluorganisaatiota ja runsaasti resursseja. Henkilötiedustelua ja vakoilua on tehty auvoisista ajoista asti. Se muutos mitä sosiaalinen media ja muut julkiset lähteet ovat tehneet on se, että nyt yksittäinen henkilö pääsee omalta kotikoneelta selvittämään toisen henkilön jopa hyvinkin yksityisen elämän tietoja helposti ja vaivattomasti.

Suurimmalla osalla ihmisistä on jonkinlainen näkyvyys internetissä, joka on voimistunut entisestään viimeisten vuosien aikana. Keskiarvallisesti henkilöllä on Facebookissa noin 100 ystävää ja joka kuukausi noin 1.2 miljardia ihmistä vierailee erilaisilla blogeilla, foorumeilla ja muilla sivustoilla, lisäten niihin materiaalia ja tarkastelemalla niitä. Avointen lähteiden tiedustelu eli OSINT ja ylipäätään henkilöihin kohdistuva tiedustelu sekä yksityisyydensuoja on herättänyt paljon keskustelua aivan valtamedioissa ja kahvipöytäkeskusteluissa asti. OSINT ei ole uusi asia vaan se on saanut alkunsa toisen maailmansodan jälkeen, lehtileikkeiden leikkaamisella ja nyt siitä on kehittynyt paljon puhuttu ja laajalti tiedossa oleva käsite. Julkisten lähteiden tiedustelusta löytyy läjäpäin kirjoja ja se on tehty helpoksi jopa sellaisille ihmisille, jotka eivät ole kovin valveutuneita tietokoneiden käyttäjiä (Layton & Watters 2016, 5).



Global Social Media Prism by ethority | <http://www.facebook.com/SocialMediaPrism> | <https://www.twitter.com/SoMePrism> | <http://pinterest.com/someprism> | Contact us for updates: prism@ethority.net



Kuva 1: Sosiaalisen median prisma (Ethority 2017)

Sosiaalisen median prisma kautta havainnollistuu tiedon suuri määrä. Lisäksi se visualisoi sen, mitä kautta henkilöstä voi valua yksittäisiä tiedon osia internetiin. Prisma ei kuitenkaan ole täysin kattava havainnollistus, vaan ainoastaan suuntaa antava visualisointi joukosta palveluita. Erilaisia sosiaalisia palveluita ja yhteisöjä muodostuu jatkuvasti lisää ja keinot tämän tiedon löytymiseksi ja kehittelemiseksi muuttuvat tekniikan ja lähteiden muuttuessa.

2.1 Sosiaalinen kanssakäyminen

Sosiaalinen media perustuu luottamukseen. Ihminen on sosiaalinen olento ja kaipaa muiden ihmisten palautetta omasta toiminnastaan. Sosiaalisten medioiden yleistyttyä koko kansan käyttöön, sosiaalinen kanssakäyminen siirtyi myös osaksi tietoverkkoja. The New York Times lehden teettämän tutkimuksen mukaan ihmisen tarve jakaa tietoa perustuu viiteen

pääteemaan, jotka näkyvät kuvassa 2. Kaikissa pääteemoissa korostuu sosiaalisen kanssakäymisen tarve henkilön omakohtaisen kokemuksen tukemiseksi. (The psychology of sharing 2011)



Kuva 2: Isoimmat syyt tietojen jakamiseen verkossa (Avidian 2017)

Olemme siinä pisteessä teknologista kehitystä, että rajat fyysisen ja virtuaalisen maailman välillä alkavat hämärtyä. Kuten yllä olevan kuvan perusteella voidaan huomioda, ihmiset haluavat puhua itsestään ja tuoda esille sen, että he välittävät myös muista. Olemme sosiaalisia olentoja, joiden syvin olemus kumpuaa tarpeesta olla vuorovaikutuksessa muiden kanssa. Jokaisella ihmisellä on omat tarpeensa ja syynsä täyttää tätä tarvetta, mutta se mikä on ihmiselle ominaista ei muutu, vaikka se viedään virtuaaliseen maailmaan.

Ihminen ei kohdistu toimintaansa tietoverkoissa ainoastaan yksittäisiin ihmisiin. Hänen halunsa ja tarpeensa perustuvat laajempaan kokonaisuuteen ja muodostavat henkilöstä kokonaiskuvan. Sosiaalisten verkostojen kautta yksittäisestä ihmisestä on näin selvitettävissä paljon enemmän kuin yksittäinen henkilötieto, koska toiminnallaan tietoverkoissa käyttäjä luo yhteyden myös sisältöön, yhteisöihin ja erilaisiin sovelluksiin. Tietoja kokoamalla ja yhdistelemällä henkilöstä rakentuu kokonaisvaltainen kuva, jonka kautta voi rakentaa varsin kattavan profiilin henkilöstä ja hänen elämänsä tärkeimmistä yhteyksistä. (Moyer & Hamiel 2008)

Sosiaalisella verkostolla on myös kääntöpuoli. Henkilöön linkittyvät tahot voivat olla niitä heikkouksia, joita tarkastelemalla saadaan tarkkailtavasta kohteesta parempi kuva. Vaikka henkilö olisi itse osannut turvata oman, esimerkiksi sosiaalisen median palvelun käyttäjätilinsä kattavasti, voi hänen läheisessä tuttavapiirissään oleva henkilö vuotaa yksilökohtaisia tietoja henkilöstä tämän tietämättä (VAHTI 4/2010, 20). Kohteen tiedostamatta kaikille julkiseksi tullut tieto voi olla peräisin esimerkiksi perheenjäsenen avoimen Facebook-profiilin kautta tapahtuneesta tykkäyksestä, jolloin alun perin suljetussa profiilisissa julkaistu kuva on näkyvissä perheenjäsenen avoimella aikajanalla.

Kaikesta tiedosta ei kuitenkaan tarvitse olla ns. fyysisesti liitoksissa tarkkailtavan kohteen jakamaan tietoon. Pelkästään se tieto, että tarkkailtava kohde on joidenkin ihmisten lähipiirissä antaa paljon tietoa sitä etsivälle. Mikäli julkisten lähteiden kautta on saatu selvitettyä henki-

lön lähipiiri, voidaan tarkastella niitä tapahtumia mitä lähipiirissä tapahtuu ja näin saada jonkinasteinen kuva siitä missä tarkkailtava kohde voi olla tai mistä toiminnasta hän voisi tykätä. Näillä tiedolla voidaan jälleen kerran kohdistaa tarkkailua niihin alueisiin, josta sitä suuremmalla todennäköisyydellä on saatavissa, ellei jo esimerkiksi kohteen lapsen jalkapalloharrastus ja löytyvät otteluohjelmat vielä riitä. Suhteet ja linkit henkilöiden sekä yhteisöjen välillä ovat niitä tietoja, jotka rikastavat sekä kirkastavat kokonaiskuvan ja näin ollen luovat rakenteen sille, miten ja mitä tietoa henkilöstä tulee julkiseksi. (Moyer & Hamiel 2008)

Ihmisen sosiaalisen kanssakäymisen tarpeen ovat huomanneet myös palveluntarjoajat, jotka ovat kasvattaneet asiakasmääriään luomalla palveluihinsa sosiaalisen aspektin. Tästä hyvänä esimerkkinä toimivat palveluihin kytketyt keskustelumahdollisuudet, kuten monien internetlehtien kommenttipalstat. Näiden avulla ihmiset saadaan kytkettyä henkilökohtaisella tasolla palveluun ja samalla tuottamaan sille lisää sisältöä ja näkyvyyttä. Huomioitavaa kommenttipalstoilla on se, että niiden käyttöä on jopa jouduttu rajoittamaan siten, ettei kommentointia voi tehdä anonymisti, vaan henkilöt toimivat siellä omilla sosiaalisen median profiileillaan. Ulkopuolisen tarkkailijalle tästä muodostuu isompi kuva, kuin mitä yksi tykkäys tai lause itsessään antaisi. Esimerkiksi poliittisesti suunnatun artikkelin kommentointi voi paljastaa hyvinkin paljon, varsinkin kun tästä kommentista on tykännyt lukuisat henkilön kaveripiirissä olevat henkilöt.

Koska ihminen on sosiaalinen olento, on yhteisöllisyys ja kanssa käyminen muiden ihmisten kanssa sille ominaista. Muiden mielipiteet merkitsevät ja oman minän tuominen esille, on meille luontainen tapa hakea hyväksyntää ja kuulua joukkoon. Tämä on myös tärkeä seikka huomioida, kun tarkastellaan asiaa oman henkilöturvallisuuden näkökannalta tai silloin kun näitä tietoja pyritään etsimään.

2.2 Internetin kautta tapahtuva henkilötiedustelu ilmiönä ja uhkana

Ennen internetin läpimurtoa henkilötiedustelua ja etenkin julkisten lähteiden tiedustelua tehtiin paperipohjalta. Henkilöstä kerättiin tietoa lehtien ja yritysjulkaisujen sekä muiden kanavien kautta. Tiedustelu perustui siihen, että se mitä näit oli se mitä sait. Internet teki tähän muutoksen ja sosiaaliset mediat räjäyttivät pankin 2000-luvulla. Tuoreimpien tutkimusten perusteella vuonna 2020 neljällä ihmisellä viidestä on Facebook-tili. Mahdollisuus päästä internetiin laajenee kun suuryritykset satsaavat miljoonia kehittyviin maihin ja uusiin asiakkaisiin. Internetyhteyksiä tarjotaan sääpallojen ja muiden uusien tapojen välityksellä. Tämä tarkoittaa sitä, että tietomäärä ja mahdollisuudet henkilötiedusteluun internetin kautta jatkavat nousuaan. (Bertram 2015, 2-5)

Suomen Puolustusministeriön (2015, 16) mukaan henkilötiedustelulla tarkoitetaan henkilön sosiaalisen kanssakäymisen tai muun toiminnan seuraamista. Tiedustelua voi tehdä myös

tietoverkkojen kautta. Sotilaallisessa ja siviilitiedustelussa on käytössä termit HUMINT (Human Intelligence) ja OSINT. Nämä ovat osa-alueita tiedustelussa, jotka linkittyvät hyvin vahvasti toisiinsa. Nyky-yhteiskunnassa julkisten lähteiden tarjoamia mahdollisuuksia ei voida unohtaa, puhuttaessa henkilötiedustelussa kokonaisuutena.

OSINT on tiedustelumuoto jossa yhdistetään useita eri osa-alueita, tarkoituksena koota kokonaiskuva tiedusteltavasta kohteesta. Nämä osa-alueet ovat tekninen osaaminen, verkkotunnustietämys ja tiedustelutaito. Teknisesti pätevä henkilö pystyy hyväksikäyttämään verkkoon luotuja työkaluja omiin tarkoituksiinsa, vaikka niitä ei ole luotu sinne tiedustelutarkoituksessa. Tällä tarkoitetaan sitä miten tietomassaa ja käytäntöjä internetissä käytetään ja kuinka tieto on löydettävissä kun sitä osaa etsiä oikeasta paikasta (Bertram 2015, 4-5).

Jotta pystytään ymmärtämään kokonaisvaltaisesti julkisten lähteiden varassa tapahtuvaa tiedustelua, tulee ymmärtää tiedustelumallin neljä peruspilaria:

1. Internet on monikerroksinen tarkoittaen sitä, että siitä vain osa on indeksoitu ja näkyvillä mm. hakukoneilla. Internet koostuu kolmesta kerroksesta, jotka ovat niin sanotusti avoin, syvä ja tumma internet eli surface web, deep web ja dark web. Nämä käsitteet ovat yleisesti ottaen väärin ymmärrettyjä ja hankalia käsittää.

Avoin internet eli surface web on kaikille näkyvä osio. Täällä tietomassa on indeksoitu ja sitä voi selata käyttäen erilaisia hakukoneita. Pääosa tästä materiaalista on laitettu sinne esimerkiksi Facebook-käyttäjän toimesta. Syvä internet eli deep web on osa verkkoa, jossa data ei ole indeksoitu tukemaan normaaleja hakukonepalveluita. Tämä johtuu siitä, että teknologia millä tavoin esimerkiksi Facebook tai Twitter julkaisee alustalle dataa, ei ole tarkoitettu luettavaksi tai julkiseksi. Tämä on kuitenkin yleisesti ottaen henkilötiedustelua suorittavalle henkilölle tärkein paikka löytää henkilöä koskevia tietoja. Ongelmana on se miten syvästä internetistä löytää pääsyn juuri haluttuun dataan. Tumma internet eli dark web on internetin osa johon pääsee käsiksi ainoastaan erityisten ohjelmien kautta, jotka anonysoivat nettiliikenteen. Tällaisia ovat esimerkiksi The Onion Router eli TOR. Tumman internetin tarkoitus on palvella niitä henkilöitä, jotka haluavat pysyä piilossa, kuten rikolliset ja anonymitietämiään huolehtivat ihmiset (Bertram 2015, 6).

2. Cyber-geografia on hyvin samantyylinen kuin normaali maantieto. Sillä tarkoitetaan sitä, että internet on jaettu eri osa-alueisiin liittyen kielelliseen kontekstiin. Pääosa internetistä löytyvästä materiaalista on englanniksi, mutta monet palvelut julkaisevat uutta sisältöä internetiin eri kielillä. Cyber-geografia tulee ottaa huomioon suorittaessa tiedustelua, koska muuten tutkijalta voi jäädä osa olemassa olevasta tiedosta huomioimatta (Bertram 2015, 7).

3. Kaiken keskiarvo eli mixed medium on ymmärrys siitä, että internet on kaikkien eri kerrostensa sekoitus, joka yhdistyy käyttäjäkohtaisena kokemuksena. Jotta voidaan ymmärtää internetissä tehtävän tiedustelun kokonaiskuva on ymmärrettävä, että jokaisella tekniikalla ja käytänteellä on oma tarkka toimintamallinsa ja tekniikkansa. Jotta päästään käsiksi kaikkeen tietoon, on pystyttävä ymmärtämään moninaiset lähestymistavat ja teknologiat isona kokonaisuutena (Bertram 2015, 8).

4. Aineellisuudella tai ymmärrettävyydellä tarkoitetaan sitä, että on pystyttävä käsittelemään internetiä samana asiana kuin muutakin elämää. Internetistä on tullut yksi osa ihmisten elämää, eikä niitä voida enää erottaa toisistaan. Etenkin läntisen maailmankatsomuksen maissa internetiä pidetään yhtenä perustarpeena puhtaan veden ja sähkön lisäksi (Bertram 2015, 8).

Vain osa julkisten lähteiden tiedoista on löydettävissä strukturoidun internetin puolelta. Hakukonepalveluilla on kuitenkin helppo löytää syvemmin tietoa OSINT-tiedustelusta ja erilaisia ohjelmistoja sekä sovelluksia tähän tarkoitukseen löytyy lukuisia. Lisäksi palvelut, kuten pipl.com, ovat sellaisia, että ne osaavat käsitellä palveluissaan tietoa myös indeksoimattomasta osasta internetiä ja näin tuovat tiedot helposti löydettäviksi. Tämän vuoksi onkin tärkeää ymmärtää kokonaisuutena ilmiötä, jotta sen luomat uhat ovat paremmin ymmärrettävissä ja sudenkuopat vältettävissä.

Lisäksi on tärkeää tiedostaa se, että kerättävän tiedon kasvaessa ja välineistön kehittyessä, julkisina lähteinä olevan tiedon automaattinen käsittely jatkaa voimakasta kasvua. Tätä vauhdittavat markkinatalouden paine kohdistaa palveluitaan vielä henkilökohtaisimmiksi, sekä tiedustelupalveluiden massiivinen tiedonkeruu ja tiedon analysoiminen. Suurten datamäärien eli ns. big datan käsittelyn koetaan olevan seuraava iso trendi ja askel markkinataloudessa, joten siihen investoidaan valtavia määriä rahaa. Big datalla tarkoitetaan strukturoitujen ja strukturoitumattomien tietomassojen keräämistä, säilyttämistä sekä analysointia ja tällaisia tietomassoja voivat olla esimerkiksi sivustojen lokitiedot tai sosiaalisen median sisältö (IBM 2017). Tutkimuksissa käytettävät algoritmit, joilla isoja määriä tietoa pystytään käsittelemään sujuvasti ja helposti, tulevat muuttamaan myös julkisista lähteistä saatavan tiedon käytettävyyttä ja hyödyllisyyttä. Tekniikan kehittyessä, tällä hetkellä vasta isojen yritysten ja tahojen käyttämät ohjelmistot ja sovellukset tulevat kotikäyttäjän saataville. (Layton & Watters 2016, 7-8)

3 Passiiviset julkiset lähteet

Iso osa passiivisista julkisista lähteistä koostuu perusrekistereistä joille tunnusomaista on se, että niitä säädellään lakien tai asetusten mukaisesti. Perusrekistereille on määritetty

kriteeristöt, joita ovat luotettavuus, kattavuus, monikäyttöisyys ja tietojen suojaus. Luotettavuudella tarkoitetaan sitä, että rekistereitä ylläpitää jokin viromainen virkavastuullaan. Lisäksi syötetyille tiedoille on oikaisumahdollisuus. Kattavuudella tarkoitetaan rekistereihin syötetyn tiedon määrämuotoisuutta, joilla on virallinen tunnus. Monikäyttöisyydellä tarkoitetaan sitä, että yksi viranomaistaho kerää tiedon, jonka jälkeen tieto on käytettävissä muilla sitä tarvitsevilla viranomaisilla. Tietojen suojaus taataan tietojen saannin ja luovutuksen tarkalla säätelyllä. (Korhonen 2003, 175)

Muita passiivisia julkisia lähteitä voivat olla esimerkiksi harrastustoiminnan tai koulutuksen kautta selvitettävät henkilötiedot. Yleisesti ottaen tämän tyyppiset tahot pitävät yllä jäsenrekisteriä palvelunsa toiminnan ylläpitämiseksi. Henkilötiedot päätyvät rekistereihin henkilön suostumuksella ja toimintaan osallistumisen kautta tietoja voi päätyä julkiseksi henkilön tietämättä. Henkilötietoja voi esiintyä vaikka seuran nettisivuilla.

3.1 Väestötietorekisteri ja väestötietojärjestelmä (VTJ)

Väestötietojärjestelmää voisi kuvailla jopa merkittävämmäksi yhteiskunnan perusrekisteriksi. Sitä ylläpitää väestörekisterikeskus ja maistraatit. Väestötietojärjestelmä juontaa juurensa väestötietokirjanpitoon, jota on ylläpidetty Suomessa yli 400 vuotta (Korhonen 2003, 177). Väestötietojärjestelmässä on Suomen kansalaisten ja Suomessa vakinaisesti asuvien ulkomaalaisten perustiedot. Lisäksi järjestelmään päivitetään tietoja rakennuksista, huoneistoista, rakennushankkeista ja kiinteistöistä. Tiedot rekisteröidään järjestelmään lakisääteisten ilmoitusten perusteella. Väestötietojärjestelmässä olevat tiedot eivät ole julkisia, mutta järjestelmän avulla eri tahot pitävät yllä ja päivittävät omien rekisteriensä tietoja. Väestötietojärjestelmän tietojen käyttäminen vaatii aina tietojenluovuttajan myöntämää tietolupaa. Luvassa määritetään käytettävien tietojen ehdot. (VTJ 2016).

Väestötietojärjestelmästä vastaa väestörekisterikeskus. Järjestelmä tuottaa palveluja rekisterinsä pohjalta kansalaisille, julkishallinnolle ja yrityksille. Se on tehty palvelemaan suurimmaksi osaksi julkishallintoa, jonka kautta viranomaiset saavat päivitettyt ja ajantasaiset henkilöä koskevat perustiedot. Rekisteriin kirjattavia tietoja ovat mm. henkilö-, osoite-, perhesuhde- ja ammattitiedot sekä rakennusten ja kiinteistöjen tietoja. (Korhonen 2003, 182 - 186).

3.2 Ajoneuvoliikennerekisteri ja ajoneuvotietojärjestelmä (ATJ)

Laki ajoneuvoliikennerekisteristä (13.6.2003/541) määrittelee itsensä siten, että: "Ajoneuvoliikennerekisteri on ajoneuvoista sekä niiden verotuksesta ja kiinnityksestä, ajoneuvoa kuljetavista, maakuljetusten turvallisuusneuvonantajista, tieliikenteen valvontalaitteissa käytettävistä korteista, lupaa edellyttävää kuljetustoimintaa varten järjestettävistä kokeista ja

myönnettävistä todistuksista pidettävä rekisteri.” Rekisterin tarkoitus on mm. parantaa liikenneturvallisuutta. Rekisteri on valtakunnallinen ja siitä vastaa Liikenteen turvallisuusvirasto eli Trafi (Trafi 2016).

Ajoneuvotietojärjestelmä eli ATJ on Trafin ylläpitämä järjestelmä jonka kautta viranomaiset, yritykset ja yksityiset henkilöt voivat selvittää ajoneuvoliikennerekisteriin talletettuja tietoja. Tietojen luovuttaminen perustuu siitä erikseen laadittuun lakiin ajoneuvoliikennerekisteristä 541/2003 (Trafi 2016).

Yksityiset henkilöt voivat saada ajoneuvotietojärjestelmästä tietoja ajoneuvon rekisteritunnuksen tai valmistenumeron perusteella, joko sähköisesti, puhelimella tai tekstiviestillä. Tiedot voidaan tilata ilman tunnistautumista. Kysyjä saa kattavat tiedot ajoneuvosta. Näitä tietoja ovat mm. omistajan ja haltijan nimi- ja osoitetiedot, määräaikaikatsastuksen suorittamisen tiedot ja millä katsastusasemalla viimeinen määräaikaikatsastus on suoritettu (Trafi 2016). Kysyjä voi siis saada tiedot siten, ettei hänen henkilöllisyyttään pystytä selvittämään, esimerkiksi tilaamalla tiedot prepaid-liittymän kautta.


Ajoneuvon MVI-825 perus- ja historiatiedot
 Haettu 08.01.2013

Ajoneuvo

Punainen M1/Henkilöauto Volkswagen NEW BEETLE

 Valmistenumero VVVWZZZ9CZ8M553648
 Määräaikaikatsastus Suorittamatta

Rajoitustiedot

Rajoituslaji	Rajoituksen alalaji	Voimassaolo
Määräaikaikatsastus suorittamatta		

Tietoa ajoneuvosta

Käyttöönottettu	02.01.2008
Ensirekisteröity	02.01.2008
Käyttö	Yksityinen
Vakuutusyhtiö	Pohjola (36), alkaen: 16.02.2009

Tietoja katsastuksista

Seuraava katsastus	02.09.2012-02.01.2013
Määräaikaikatsastettu	09.12.2010

Omistajat ja haltijat

Omistajatyyppi	Alkaen	Nimi	Osoite
1.omistaja	16.02.2009	Oksaharju, Terhi Kristiina	Jyränmaankatu 8, 37140 NOKIA

Moottori

Moottorin iskutilavuus (cm³)	1890
Käyttövoima	Dieselöljy

Kulutus (l/100 km)

Dieselöljy	
Kulutus maantieajossa	4,6
Kulutus kaupunkiajossa	6,8
Yhdistetty kulutus	5,4
CO2 Yhdistetty	143

Pakokaasu-arvot

Dieselöljy [g/km]	
CO	0,12
NO _x	0,206
Hiukkaset	0,021
HC/THC+NO _x	0,224

Turvavarusteet (penkkirivi: sijainti)

Eturvatyyyny (1: Oikea)
 Eturvatyyyny (1: Vasen)
 Turvavyön kiristin (1: Oikea)
 Turvavyön kiristin (1: Vasen)

Kilometrilukemat (km)
Omistushistoria

Omistusaika	Asiakaslaji/nimi ja osoite	Omistajuustyyppi
16.02.2009-	Oksaharju, Terhi Kristiina Jyränmaankatu 8, 37140 NOKIA	1.omistaja
23.10.2008-16.02.2009	INCHCAPE MOTORS FINLAND OY Niittymaantie 8, 02200 ESPOO	1.omistaja
19.03.2008-23.10.2008	Korhonen, Antti Mikael Pahkalaukkaantie 102, 21350 ILMARINEN	1.omistaja
02.01.2008-19.03.2008	Yksityinen	1.haltija
02.01.2008-19.03.2008	Yksityinen	1.omistaja

Katsastushistoria

Pvm	Katsastuslaji	Tila
21.07.2011	Muutuskatsastus	hyväksytty
09.12.2010	Määräaikaikatsastus	hyväksytty
10.02.2010	Muutuskatsastus	hyväksytty

Tunnushistoria

Tunnus	Alkuvp	Loppupv
MVI-825	02.01.2008	

Vakuutushistoria

Yhtiö	Alkuvp	Loppupv
Pohjola	16.02.2009	
Fennia	23.10.2008	16.02.2009
Pohjola	02.01.2008	19.03.2008
Pohjola	02.01.2008	23.10.2008

Käyttöhistoria

Käyttö	Alkuvp	Loppupv
Yksityinen	19.02.2009	
Myyntivarasto	23.10.2008	18.02.2009
Yksityinen	02.01.2008	22.10.2008

Poistohistoria

Lähde: Ajoneuvoliikennerekisteri

 Jos haluat nämä tiedot talteen, tulosta tai tallenna tämä sivu.
 (Tämän voit tehdä selaimesi Tallenna ja Tulosta -toiminnoilla.)
 Copyright © 2012 Trafi

Kuva 3: ATJ:sta tilattavat ajoneuvon perus- ja historiatiedot (Trafi 2016).



Ajoneuvon MVI-825 tekniset tiedot
Haettu 08.01.2013

Ajoneuvo

Rekisteritunnus	MVI-825
M1/Henkilöauto	Volkswagen NEW BEETLE
Valmistenumero	WVWZZZ9CZ8M553648

Tietoa ajoneuvosta

Käyttöönottettu	02.01.2008
Käyttö	Yksityinen
Seuraava katsastus	02.09.2012-02.01.2013
Vaihdettujen osien kokonaisprosentti	
Tyypinimi	5267371331
Tyypinhyväksyntänumero	e1*01/116*0106*22
Variantti	ABB5WX01
Versio	FM5FM5A40091N10GG

Katsastushistoria (hyväksytyt katsastukset)

Pvm	Katsastuslaji	Paikka
21.07.2011	Muutuskatsastus	A-Katsastus Järvenpää
09.12.2010	Määräaikauskatsastus	K1-Katsastajat Oy Vuosaari
10.02.2010	Muutuskatsastus	A-Katsastus Aleksis Kiven katu

Kuva 4: ATJ:sta tilattavat ajoneuvon tekniset tiedot (Trafi 2016).

3.3 Patentti- ja rekisterihallitus (Virre)

Patentti- ja rekisterihallitus eli PRH ylläpitää ja valvoo kaupparekisteriä, yhdistysrekisteriä, säätiörekisteriä, tilintarkastajarekisteriä sekä tietoja yritysikiinnityksistä, mallioikeuksista, patenteista ja hyödyllisyysmalleista. PRH:n ylläpitämän Virre-tietopalvelun kautta voi tehdä sähköisesti hakuja ja ostoja liittyen PRH:n hallinointiin rekistereihin ja tietokantoihin (PRH 2017).

3.3.1 Kaupparekisteri

Kaupparekisteri on PRH:n ylläpitämä virallinen ja julkinen rekisteri, joka ylläpitää tietoa yrityksistä, asunto-osakeyhtiöistä ja asumisoikeusyhtiöistä. Osakeyhtiöiden, kommandiittiyhtiöiden, avoimien yhtiöiden ja osuuskuntien velvollisuus on tehdä ilmoitus toiminnastaan kaupparekisteriin. Lisäksi yksityisten elinkeinonharjoittajien on useimmiten tehtävä perustamisilmoitus kaupparekisteriin (PRH - kaupparekisteri 2017).

Kaupparekisteriotteella on luonnollisen henkilön täydellinen nimi, syntymäaika, kansalaisuus ja kotikunta. Ainoastaan yritykselle rekisteröidyn ilmoituksen perusteella lähetetyssä kaupparekisteriotteessa on näkyvissä kaikki yrityksen ilmoittamat henkilötiedot kokonaisuudessaan, jotka kattavat myös henkilötunnuksen (PRH - kaupparekisteri 2017).

Patentti- ja rekisterihallituksen ylläpitämästä rekisteristä on myös haettavissa asunto-osakeyhtiön hallituksen, isännöitsijän tai muiden vastuuhenkilöiden tietoja. Suomessa asuvan henkilön kotiosoitetta ei ilmoiteta rekisteriin ja luonnollisten henkilöiden yksilöintitiedot ilmoitetaan erillisellä lomakkeella. Henkilön nimitieto on kuitenkin saatavissa ja näin ollen yhdistettävissä taloyhtiöön, jos henkilö kuuluu taloyhtiön hallitukseen tai hänellä on jotain muuta ilmoitettuja vastuutehtäviä taloyhtiössä (PRH - tiedot 2017).

Kaupparekisteristä saa tietoa monella eri tavalla. PRH:n ylläpitämän Virre-tietopalvelun kautta voi hankkia sähköisesti kaupparekisteriotteen, yhteisösäännökset, tilinpäätökset, kaupparekisteri-ilmoituksen asiakirjat ja erilaiset yrityspoiminnat. Tietoja voi myös tilata puhelimitse ja postitse. Virre-palvelun kautta voi myös hakea tietoa säätiöistä ja yrityskiinnityksistä. Haku tapahtuu yrityksen tietojen tai henkilön tietojen (nimi, henkilötunnus tai syntymäaika) avulla.

Virre > Yrityshaku

Yrityshaulla voit etsiä kaupparekisteriin merkittyjä tai lakaneita yrityksiä sekä yrityksiä, joiden ilmoitus on vireillä. Yrityshaku tuottaa listauksen yrityksistä, joihin valitut hakukriteerit soveltuvat. Listauksesta pääset etenemään yrityksen perustietoihin ilmaiseksi, tarkemmat tiedot ovat maksullisia. [Katso tarkemmat ohjeet](#)

Yrityshaku

Yrityksen nimi:

Y-tunnus:

Rekisterinumero:

Kotipaikka:

Yrityksen tila:

Yritysmuoto:

Nimen tila:

Tarkka haku

Hae

Kuva 5: Yritysten haku Virre-palvelun avulla (PRH - kaupparekisteri 2016)

Yritysten tietoja voi myös etsiä muiden palveluiden avulla, joita ovat mm. Fonectan tarjoama Finder yrityshaku ja Kauppalehden yrityshaku. Tietoja voi hakea yrittäjän nimellä tai yrityksen nimellä. Palveluista tulee tarkempaa tietoa rekisteröitymällä palveluun. Tällöin on mahdollista saada selville mm. yrittäjän käyttämä puhelinnumero tai osoite.

The screenshot shows the FINDER service interface. At the top, the word 'Finder' is displayed in white on a blue background. Below it, a search bar contains the text 'Pakilan Isännöinti Oy'. Underneath the search bar, there are three tabs: 'KAIKKI (5)', 'YRITYKSET (2)', and 'HENKILÖT (3)'. The 'YRITYKSET (2)' tab is selected. The main content area displays a list of search results. Each result includes a company or person icon, their name, contact information (phone number), and location (address and city). The results are as follows:

Company/Person	Contact Information	Location
Pakilan Isännöinti Oy 0998885-2	050 590 NÄYTÄ NUMERO	Taulutie 12 B/Siven, 00680 Helsinki
As. Oy Rapakivenkuja 3-4-5 Asunto-Oy Rapakivenkuja 3-4-5 0121503-8	09 477 NÄYTÄ NUMERO	Taulutie 14 A, 00680 Helsinki
Anna-Kaisa Siven Pakilan Isännöinti Oy, hallituksen varajäsen		Taulutie 12 B/Siven, 00680 Helsinki
Hannu Erkki Juhani Siven Pakilan Isännöinti Oy, hallituksen puheenjohtaja		Taulutie 12 B/Siven, 00680 Helsinki
Satu Kristiina Siven Pakilan Isännöinti Oy, hallituksen jäsen, toimitusjohtaja		Taulutie 12 B/Siven, 00680 Helsinki

Kuva 6: Esimerkki yrityshausta Fonectan Finder palvelusta (Fonecta 2016)

3.3.2 Yhdistysrekisteri

Yhdistysrekisteri on myös Patentti- ja rekisterihallituksen ylläpitämä rekisteri, johon on talletettu mm. yhdistyksen rekisterinumero, nimi, kotipaikka ja ensirekisteröinnin päivä sekä yhdistyksen nimenkirjoittajat. Yhdistysrekisterin kautta voi hakea kaikkiaan noin 130 000 suomalaisen rekisteröityneen yhdistyksen tietoja. Yhdistysrekisterin tiedot ja sen ilmoitukset liitteineen ovat yleisesti ottaen julkisia. Lisäksi yhdistysrekisteri tarjoaa tiedonhakuotteita, jotka ovat jaettu maksuttomiin ja maksullisiin (PRH - yhdistysrekisteri 2017).

Yhdistysrekisterin tietojen ajantasaisuus on riippuvaista siitä miten yhdistys niitä itse päivittää rekisteriin. Huomioitavaa on kuitenkin se, että yhdistyksen nimenkirjoittajien henkilötietoja päivitetään väestötietojärjestelmästä henkilötunnuksen avulla, jolloin ne ovat ajantasaisia. Yhdistysrekisterin tietojen katsotaan olevan julkisesti luotettavia (Korhonen 2003, 198).

Yhdistyslain 11§:n mukaan yhdistyksen jäsenistä on pidettävä luetteloa, joka kattaa jäsenen täydellisen nimen ja kotipaikan. Yhdistyksen jäsentietojen luovuttamisen lähtökohtana on asianomaisen suostumus. Yhdistyksen säännöissä voi kuitenkin olla kirjattu säädös

jäsenluettelon julkisuudesta. Yhdistyksen olisi kuntien tuotava tietojen julkisuus esille kerätessään jäsenluetteloja tai lisätessään uusia jäseniä. Näin toimimalla voidaan varmistua siitä, ettei yhdistyksen jäsenten tietoja luovuteta henkilötietolain vastaisesti (Tietosuojavaltuutetun toimisto 2010).

PATENTTI- JA REKISTERIHALLITUS

Yhdistysnetti

[Svenska](#)
[English](#)

Yhdistyshaku

- Hae yhdistysten, kauppakamareiden ja uskonnollisten yhdyskuntien tietoja nimellä, kotipaikalla tai muilla hakutekijöillä. Vaihtoehtoisesti voit hakea tietoja yhdistyksen rekisterinumerolla.
- Tästä hausta löydät voimassaolevat tiedot. Jos tarvitset tietoja vireillä olevista tai purkautuneista yhdistyksistä, [siirry nimihakuun](#).
- Klikkaamalla hakutuloksesta rekisterinumeroa pääset perustietoihin. Maksuttomia perustietoja ovat: rekisterinumero, nimi, kotipaikka, ensirekisteröinnin päivä ja viimeisen rekisteröinnin päivä sekä tiedot ilmoitusten käsittelyvaiheista.
- Voit ostaa sähköisen otteen. Otteen hinta on 4,34 €/kpl (sis. alv 24%). Otteelta löydät esim. yhdistyksen nimenkirjoittajat.
- Voit ostaa myös yhdistyksen säännöt, jos ne on rekisteröity 2011 tai myöhemmin. Sääntöjen hinta on 4,34 €/kpl (sis. alv 24%).
- Hakuohjeita löydät kysymysmerkkien alta ja [kootuista ohjeista](#).

Hae: vain yhdistyksiä vain kauppakamareita vain uskonnollisia yhdyskuntia kaikkia

Yhdistyksen nimi ?

Kotipaikka ?

Rekisteröintipäivä ?

Viimeisin rekisteröintipäivä ?

Postinumero (ja/tai toimipaikan nimi) ?

Maakunta ?

Vaalipiiri ?

Vapaa tekstihaku ?

Haku rekisterinumerolla ?

Kuva 7: Haku yhdistysrekisteristä (PRH - yhdistysrekisteri 2017)

3.4 Oikeusrekisterikeskus

Oikeusrekisterikeskus (2017) ylläpitää konkurssi- ja yrityssaneerausrekisteriä, velkajärjestelyrekisteriä ja liiketoimintakieltorekisteriä, joista kuka tahansa voi tilata maksullisia otteita. Lisäksi se ylläpitää eläintenpitorekisteriä joka on salassa pidettävä rekisteri. Eläintenpitorekisteristä saa tilattua otteen ainoastaan jos sen saaminen on perustelua eläinsuojelun toteuttamiseksi. Rekisterit pitävät sisällään tietoja konkurseista ja yrityssaneerauksista sekä niihin kohdistuvista päätöksistä, yksityishenkilöiden velkajärjestelyistä ja niiden hakemuksista sekä päätöksistä, tietoja liiketoimintakielloista. Eläintenpitorekisteri pitää sisällään tietoja tuomituista eläintenpitokielloista. Tietoja tilattaessa on oltava tiedossa yhtiön tai henkilön nimi, y-tunnus tai sosiaaliturvatunnus ja tilaajan nimi sekä osoitetieto. Tietoja voi tilata sähköpostitse lukuun ottamatta eläintenpitorekisteriä, jonne tarvitsee lähettää kirjallinen anomus perusteluineen.

3.5 Luottorekisteri

Suomen Asiakastieto Oy (2017) pitää yllä luottorekisteriä, joka sisältää tiedot ja maksuhäiriömerkinnät väestötietorekisteriin merkityistä henkilöstä, sekä kaupparekisteriin merkityistä yrityksistä. Tiedot on tarkastettavissa yrityksen sivustojen kautta ja ne ovat maksullisia. Suomen Asiakastieto Oy kerää tietonsa rahoitusyhtiöiden, oikeushallinnon, väestörekisterikeskuksen, ulosottoviranomaisten, käräjäoikeuksien ja kaupparekisterin kautta.

Luottorekisterin sisältämistä tiedoista on säädetty Luottotietolaissa (527/2007). Suomen Asiakastieto Oy:n (2017) mukaan sähköisesti voi tiedustella toisen henkilön tietoja maksua vastaan. Kysyttäessä henkilöstä saa tietää perustiedot eli nimen ja syntymäajan, henkilön oikeustoimikelpoisuuden ja siinä olevat mahdolliset rajoitukset, henkilön mahdolliset maksuhäiriöt ja muut luottotietomerkinnät sekä niiden vanhenemisajat. Vuokranantaja voi kysyä vuokralaisesta perustiedot eli luottorekisteristä löytyvät tiedot, vuokalaisen luottotiedot ja päätösehdotuksen. Päätösehdotuksella tarkoitetaan Suomen Asiakastieto Oy:n keräämistä tiedosta pohjautuvaa ehdotusta, jossa on huomioitu henkilön luottotiedot, yritysytteudet ja työsuhteen laatu.

3.6 Ulosottorekisteri

Ulosoton tietojärjestelmä on luotu ulosottoviranomaisille kuuluvien tehtävien hoitamista varten. Rekisteriin merkitään ulosoton hallintaan varten asiaosaisten ja heidän edustajien henkilötietoja sekä velkaan liittyviä tietoja. Yksityisellä henkilöllä on mahdollisuus tiedustella rekisteriin merkittyjä tietoja paikalliselta ulosottoviranomaiselta. Kyselyn voi tehdä nimeämästään henkilöstä, jolloin vastauksena saa kahden vuoden aikana tallennetut rekisteriin merkityt tiedot. Nämä tiedot pitävät sisällään hakijan ja vastaajan nimet, sekä vastaajan syntymäajan ja kotikunnan, tarkemmat tiedot ulosottoasiasta ja velan määrästä, sekä estetodistuksen. Todistus annetaan tulosteena ulosoton tietojärjestelmästä (Laki ulosottokaaresta 15.6.2007/705).

3.7 Kiinteistörekisteri ja kiinteistötietojärjestelmä (KTJ)

Kiinteistörekisterilain mukaan kiinteistörekisteri sisältää tietoja kiinteistöistä ja niiden sijainneista, sekä muita lain määrittämiä tietoja. Kiinteistörekisteri on osa kiinteistötietojärjestelmää (Kiinteistörekisterilaki 16.5.1985/392).

Kiinteistötietojärjestelmään sisältyy kiinteistörekisteri sekä lainhuuto- ja kiinnitysrekisteri. Näitä rekistereitä ylläpitää Maanmittauslaitos. Lisäksi Maanmittauslaitos pitää yllä kauppahintarekisteriä. Kiinteistötietojärjestelmän kautta voi selvittää kiinteistörekisteriin merkittyjä tietoja kuten: kiinteistön tunnuksen, nimen, pinta-alan, sijainnin ja osuudet

yhteisiin alueisiin. KTJ:n kautta voi etsiä myös lainhuuto- ja kiinnitysrekisteriin merkittyjä tietoja, kuten kiinteistön omistajan tiedot sekä kiinteistöön kohdistuvat kiinnitykset ja vuokra-oikeudet. KTJ:n tiedot ovat julkisia ja ne kattavat koko Suomen (Maanmittauslaitos - kiinteistö 2017).

Yksityiset henkilöt voivat tilata KTJ:n tietoja otteina. Tämä tapahtuu Maanmittauslaitoksen, maistraattien tai kuntien asiakaspalveluista. Otteet ovat maksullisia, mutta niistä saa tietoa ilmaiseksi asiakaspalvelusta. Selvitettäessä kuka omistaa kiinteistön on selvittävää ns. lainhuuto, mikä tarkoittaa kiinteistön yms. omistusoikeuden kirjaamista rekisteriin. Lainhuutotodistuksessa käy ilmi rekisteriin merkitty viimeksi myönnetty lainhuuto. Lainhuutotiedot pitävät sisällään mm. tapahtumapäivän, omistusosuuden, lainhuudon saajan tiedot sekä saantotiedot esim. perintö tai kauppa. Lainhuutotodistuksen saamiseksi tulee selvittää kiinteistön tunnus, jonka saa selvitettyä mm. Maanmittauslaitoksen tarjoaman karttapalvelun kautta (Maanmittauslaitos - lainhuuto 2017).

3.8 Teleoperaattorit ja numeropalvelut

Teleoperaattorit säilövät henkilötietoja omiin asiakasrekistereihinsä. Rekistereitä päivitetään ja pidetään yllä mm. palveluiden tarjoamiseksi asiakkaalle sekä laskutuksen hoitamiseksi. Rekisterin tietoja hyödynnetään myös asiakkaaseen kohdennettuun mainontaan. Rekistereihin merkitään henkilöstä kattavat henkilötiedot sekä asiakkaan itsensä antamat tiedot, kuten sähköposti, asiakashistoriatiedot ja lukuisia muita markkinointiin ja liittymän sekä puhelimen käyttöön liittyviä tietoja. Rekisterin tietojenluovutusta määrittää mm. henkilötietolaki (Elisa - asiakasrekisteri 2017).

Teleoperaattorilta hankittu liittymä sisältää yksilöivän puhelinnumeron. Yksittäisen henkilön käytössä olevaa numeroa voi selvittää nimellä erilaisista numeropalveluista, kuten Fonecta henkilöhaku tai 118-numeropalvelu. Haun voi suorittaa myös pelkällä puhelinnumerolla, jolloin saa selville numeron omistajan henkilötietoja. Näitä tietoja ovat nimi- ja osoitetiedot, sekä henkilön itsensä määrittämät tiedot. Henkilö voi lisätä itsestään julkisiksi tiedoiksi esimerkiksi sähköpostiosoitteen, ammatin tai jopa kasvokuvan. Numeropalvelut keräävät ja päivittävät tietojaan mm. väestötietojärjestelmästä, kaupparekisteristä ja luottorekisteristä sekä Trafista (Fonecta 2017).

Finder

Markus Haapanen

KAIKKI (8) YRITYKSET (0) HENKILÖT (8)

	Markus Haapanen Kouvolan Putkityö Oy Kouvola, Toimitusjohtaja	Korjalankatu 5, 45130 Kouvola 040 592 NÄYTÄ NUMERO	
	Markus Haapanen Jetpak Finland Oy, country manager	Rahtitie 1, 01530 Vantaa	
	Markus Juhani Haapanen Hämeenkyrön Sanomat Oy, hallituksen jäsen	Nujamiestentie 1, 39100 Hämeenkyrö	
	Markus Juhani Haapanen Kouvolan Putkityö Oy Kouvola, hallituksen jäsen, toimitusjohtaja	Korjalankatu 5, 45130 Kouvola	

Kuva 8: Esimerkki henkilöhausta Fonectan Finder palvelussa (Fonecta 2016).

3.9 Julkinen esiintyminen ja harrastukset

Pääosin kaikki kirjoitettu tai julkaistu tieto päätyy myös internetiin ja on haettavissa hakukonepalveluilla. Lisäksi eri tahot, kuten lehtitalot, digitalisoivat arkistojaan säilytettävyyden helpottamiseksi. Tämä tarkoittaa sitä, että lehtiartikkeliä varten tehty haastattelu tai yleisessä tapahtumassa otettu kuva päätyy aina myös julkisesti haettavaksi. Kuvien ja videoiden hakua on kuvattu tarkemmin kohdassa 5.2.

Harrastustoiminnan kautta henkilön seuraaminen tai henkilötietojen selvittäminen on hyvin helppoa. Lisäksi toimintamalleja henkilötietojen käsittelylle on lähes yhtä monta kuin erilaisia harrastuksia tai seuroja on olemassa. Harrastus- tai seuratoimintaan osallistuminen yleisesti vaatii jonkinlaisen jäsenmaksun maksamisen. Jäsenmaksuja varten seurassa on käytössä jäsenrekisteri, jonne talletetaan henkilötietoja.

Esimerkiksi Palloliiton jäsenrekisteriin rekisteröidään henkilö kilpailumääräysten mukaisesti ja vakuutusturvan välittämiseksi vakuutusyhtiölle. Rekisteriin syötetään tarkat henkilötiedot sisältäen yhteys- ja henkilötiedot sekä piirin ja urheiluseuran tiedot. Tiedot ovat käyttäjän itsensä luovuttamia, kilpailujärjestäjän luomia sekä Suomen Palloliiton ja sen alaisten piirien ja seurojen lisäämiä. Tietoja voidaan käyttää palvelun kehittämiseksi. Tietoja ei luovuteta markkinointitarkoituksiin kolmansille osapuolille, mutta tietoja voidaan luovuttaa ei-markkinoinnillisiin tarkoituksiin, lukuun ottamatta arkaluonteisia tietoja ja henkilötunnuksia.

Jotta kilpailutoimintaa Palloliiton alaisissa turnauksissa ja toiminnassa voi suorittaa, tulee harrastajan rekisteröidä itsensä Palloliiton rekisteriin nimeltä Pelipaikka (Palloliitto 2017).

Palloliiton nettisivujen kautta voi selvittää kussakin joukkueessa pelaavat henkilöt ja heidän etu- ja sukunimensä. Lisäksi sivujen kautta saa tietoa tulevista otteluista ja niiden pelipaikoista. Lisäksi seuran omien nettisivujen kautta voi henkilöstä selvittää vielä tarkempaa tietoa, esimerkiksi seuran järjestämistä muista tapahtumista aina valokuviiin asti. Henkilön yksilöivien tietojen kuten valokuvan ja nimen esittäminen seuran sivuilla voi tapahtua henkilön tietämättä. Esimerkiksi seuran tekemän reportaasin tiimoilta voidaan henkilön nimitietoja julkaista myös eri lehtien jutuissa, joissa peliä tai seuran järjestämää tapahtumaa on käsitelty.

4 Miten estää henkilötietojen selvittäminen julkisista rekistereistä

Tässä kappaleessa käydään läpi niitä keinoja miten yksittäinen henkilö voi torjua hänen tietojensa päätymistä julkiseksi erilaisten rekisterien kautta. Lisäksi kappaleessa tuodaan esille yksittäisen henkilön lakisääteisiä oikeuksia hänen yksityisyyteensä.

4.1 Maistraatista ja väestörekisterikeskuksesta haettavat henkilötietojen luovutuskiellot

“Rekisteröidyllä on oikeus kieltää rekisterinpitäjää käsittelemästä häntä itseään koskevia tietoja suoramainontaa, etämyyntiä ja muuta suoramarkkinointia sekä markkina- ja mielipidetutkimusta samoin kuin henkilömatrikkelia ja sukututkimusta varten.” (Henkilötietolaki 22.4.1999/523).

Henkilöllä on myös oikeus kieltää omansa, samassa taloudessa asuvan puolisonsa ja huollosaan olevan lapsensa osoitteen ja muun yhteystiedon luovuttaminen. Kielto ei kuitenkaan koske sellaisia tapauksia, joissa tiedot luovutetaan käytettäväksi henkilön, yrityksen tai yhteisön oikeuksien tai velvollisuuksien toteuttamiseksi. Kieltoa koskeva ilmoitus tulee toimittaa Väestörekisterikeskukselle tai maistraatille lähinnä kirjallisesti. (Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista 21.8.2009/661)

Väestörekisterikeskuksen omien tietojen tarkastuspalvelun kautta voi tarkastaa itseään koskevat henkilötiedot, nimihistoriatiedot sekä mahdolliset kiinteistö- ja rakennusomistustiedot. Palveluun kirjaututaan omilla verkkopankkitunnuksilla, mobiilivarmenteella tai henkilökortilla. Palvelun kautta voi myös ilmoittaa ja päivittää omia tietoja, koskien esimerkiksi sähköpostiosoitetta tai kutsumanimeä. Palvelun kautta voi lisäksi määrittää tietojenluovutuskieltoja. Tietoja ja tietojenluovutuskieltoja voi myös selvittää asioimalla henkilökohtaisesti maistraatissa tai pyytää niitä sieltä kirjallisesti. (Väestörekisterikeskus 2016).

4.1.1 Suoramarkkinointi-, henkilömatrikkeli- ja sukututkimuskielto

Suoramarkkinointikielto tarkoittaa sitä, että henkilön nimi- ja osoitetietoja ei luovututa suoramarkkinointiin. Kyseisiä tietoja ei myöskään käytetä markkina- tai mielipidemittauksissa poislukien tieteellinen kyselytutkimus. Kielto estää ainoastaan postitse saapuvan mainonnan (Väestörekisterikeskus - tiedot 2016).

Henkilötietolain 17§:n mukaan henkilömatrikkeli on julkaisu, jossa henkilöitä yhdistää tietty spesifi toimi. Tällainen toimi voi olla esimerkiksi kuuluminen urheiluseuraan, yhteisöön, koululaitokseen, kulttuurilliseen toimeen tai muuhun rinnastettavaan seikkaan.

Henkilömatrikkeli eli julkaisu voi olla vaikka koulusta valmistuneiden opiskelijoiden kirja tai jonkin urheiluseuran jäsenien saavutusten listaaminen. Koululla tai urheiluseuralla on omissa rekistereissään perustietoja henkilöstä, jotka ovat nimi- ja syntymäaikatietoja. Näitä vähäisiä tietoja voidaan luovuttaa henkilömatrikkelin tekijälle, jolla niiden keräämiseen on oikeus henkilötietolain 17§:n nojalla (Hetil 17 §; Vehkamäki & Tamminen-Dahlman 2006, 72.).

Henkilömatrikkelikielto tarkoittaa sitä, ettei henkilön nimi- ja osoitetietoja luovuteta väestötietorekisteristä, esimerkiksi oppilaitoksen entisistä oppilaista tai jonkun spesifin tutkinnon suorittaneista, tehtävää matrikkelia varten (Väestörekisterikeskus 2016).

Sukututkimuskiellolla tarkoitetaan sellaista kieltoa, joka estää henkilötietojen luovuttamisen sukututkimusta tekevän tahon tietoon (Väestörekisterikeskus 2016). Sukututkimusta varten kerättävät tiedot pitävät henkilötietolain 18§:n mukaan sisällään yksilöityyn sukuun kuuluvan henkilön ja tämän aviopuolison tarpeelliset yksilöinti- henkilö- ja yhteystiedot yhteydenottoa varten.

Kirkonkirjat ovat avoimesti nähtävissä digitaalisessa muodossa arkistolaitoksen kuvatietokannassa Digitaalikirjastossa. Useimmat evankelis-luterilaiset seurakunnat ovat kuitenkin päättäneet olla antamatta 100 vuotta ja sitä nuorempia kirkonkirjoja nähtäväksi avoimesti (Geneologia 2017).

4.1.2 Yhteystietojen luovutuskielto ja asiakasrekisterin päivityskielto

Yhteystietojen luovutuskielto tarkoittaa sitä, että henkilön väestötietorekisteriin merkittyjä yhteystietoja ei luovuteta Väestörekisterikeskuksen osoitepalvelussa, eikä muissakaan palveluissa, jotka hyödyntävät väestötietojärjestelmään merkittyjä tietoja (Väestörekisterikeskus - tiedot 2016).

Asiakasrekisterin päivityskielto tarkoittaa sitä, etteivät yritykset pysty päivittämään asiakasrekistereitään väestötietorekisteriin merkittyjen tietojen perusteella. Tällaisia

yrityksiä ovat esimerkiksi lehtitalot. Henkilön muuttaessa, uudet osoitetiedot eivät myöskään välity yrityksille pois lukien pankit, vakuutusyhtiöt, Veikkaus Oy, Raha-automaattiyhdistys sekä Fintoto Oy (Väestörekisterikeskus - tiedot 2016).

Yhteystietojen luovutuskielto on vuonna 2013 korvannut aiemmin käytössä olleen osoitepalvelukiellon. Osoitepalvelukiellon aikanaan hankkineet ovat automaattisesti rekisteröity yhteystietojen luovutuskiellon ja asiakasrekisterin päivityskiellon alaisiksi (Väestörekisterikeskus 2016).

4.1.3 Turvakielto

“Jos henkilöllä on perusteltu ja ilmeinen syy epäillä itsensä tai perheensä terveyden tai turvallisuuden tulevan uhatuksi, väestötietojärjestelmään voidaan hakemuksesta tallettaa turvakielto. Sen henkilön, jota asia koskee, tai hänen laillisen edustajansa tulee hakea turvakieltoa maistraatilta kirjallisesti tai muulla todistettavalla tavalla.” (Henkilötietolaki 22.4.1999/523).

Turvakielto määrittää henkilön kotikunnan, asuinpaikan, osoitteen ja muut yhteystiedot salaisiksi. Turvakielto koskee myös henkilön omistuksessa tai hallinnassa olevan kiinteistön, rakennuksen ja huoneiston yksilöinti- ja sijaintitietoja. Tiedot voi ainoastaan luovuttaa sellaiselle viranomaiselle, jolla on lakimääritteinen oikeus nähdä tietoja ja kyseisten tietojen etsimiseen perusteltu virkatehtävä (Henkilötietolaki 22.4.1999/523).

Turvakieltoa voidaan poikkeuksellisissa tilanteissa määrätä toistaiseksi voimassaolevaksi. Normaaleissa tapauksissa se myönnetään kriteerit täyttävälle henkilölle viideksi vuodeksi kerrallaan, minkä jälkeen se tarvitsee uusia joka toinen vuosi. Turvakieltoa haetaan maistraatista kirjallisella, perustellulla selvityksellä tai käynnillä maistraatissa (Väestörekisterikeskus - turvakielto 2016).

Turvakiellon saanut henkilö voi halutessaan määrittää maistraattiin yhteysosoitteen, joka ei ole salassapidon alaisena. Tämän osoitteeseen avulla voi ulkopuolinen henkilö ottaa yhteyttä turvakieltoon määrättyyn henkilöön. Yhteysosoite ei kuitenkaan näy väestötietorekisterin kautta tietoja päivittäville tahoille, joten yrityksillä yleisesti käytössä olevat järjestelmät eivät tunnista henkilöä Suomessa asuvaksi henkilöksi (Väestörekisterikeskus - turvakielto 2016).

Turvakielto rajoittaa henkilön elämää ja hänen käyttämiään palveluita. Koska osa viranomaisistakaan ei saa henkilön osoitetietoja, eivät kaikki tahot voi varmistua henkilön kotipaikasta. Tämä tarkoittaa sitä, että automaattiset henkilöllisyyden tarkastustoimet kuten luoton myöntö voi estyä, koska järjestelmä ei pysty todentamaan henkilön asuvan Suomessa.

4.1.4 Väestötietojärjestelmän tietojen hyödyntäminen

Yksinkertaisimmillaan väestötietojärjestelmän tietoja voi etsiä internetistä. Useat verkko- ja puhelinpalvelut saavat ja välittävät tietoja mm. väestötietojärjestelmästä. Näihin palveluihin päätyvät henkilön nimi- ja osoitetiedot. Halutun henkilön tietoja voi selvittää soittamalla palveluntarjoajan palvelunumeroon tai käyttämällä palveluntarjoajan verkkosivustoa. Tällaisia henkilötietojen hakupalveluita ovat mm. Fonecta, Osoitepalvelu ja Bisnode.

Henkilötietolain (199/523 19§:n) nojalla yritys saa tallettaa tietoja suoramarkkinointirekisteriinsä, mikäli henkilö ei ole sitä erikseen kieltänyt. Fonectan palvelun ehdoissa mainitaan, että tallennetut tiedot päätyvät pysyväan suoramarkkinointirekisteriin, jossa niitä käsitellään rekisteriselosteen mukaisesti (Fonecta 2016). Väestötietorekisteriin talletettuja tietoja käytetään hyväksi lukuisten yritysten ja virastojen taholta. Väestörekisterikeskus on erikseen listannut kaikki tahot jotka sen rekisterissä olleita tietoja pyytävät ja näin ollen omia rekistereitään päivittävät (Väestörekisterikeskus 2017).

4.2 Ajoneuvon omistajan tai haltijan tiedot

Ajoneuvoliikennerekisteri on pääosin julkinen, mutta luonnollinen henkilö voi rajoittaa itseään koskevien henkilötietojen siirtymistä joidenkin tahojen näkyville. Trafi on yhtenäistänyt tietojenluovutusta maistraatin kanssa ja 1.1.2017 alkaen se on luopunut myöntämästä omaa erillistä turvakieltoa. Tämän vuoksi turvakieltoa ei tarvitse enää erikseen hakea Trafilta, vaan turvakielto haetaan kokonaisuutena maistraatista. Lisäksi maistraatteihin tehtävät osoitteenluovutus- ja markkinointikiellot kattavat myös Trafian palvelun automaattisesti. Yhtenäistäminen helpottaa turvakieltoasiakkaan henkilötietojen suojaamista (Trafi 2017).

Mikäli henkilöllä ei ole maistraatin myöntämää turvakieltoa, osoitteenluovutus- ja markkinointikieltoa, voi henkilö tehdä Trafille oman osoitteenluovutuskiellon. Osoitteenluovutuskielto estää osoitetietojen luovuttamisen ajoneuvotietojärjestelmästä, poislukien viranomaisten tekemät kyselyt. Tämä tarkoittaa sitä, että yksityinen henkilö ei pysty selvittämään ajoneuvon rekisterinumeron perusteella sen omistajan tai haltijan osoitetietoja, vaan ainoastaan nimitiedot (Trafi 2017).

Trafiin voi myös määrittää markkinointikiellon, joka estää nimi- ja osoitetietojen luovuttamisen suoramainontaa, etämyyntiä ja markkina- sekä mielipidetutkimusta varten. Markkinointikielto estää myös tietojen luovuttamisen henkilömatrikkelia ja sukututkimusta varten (Trafi 2017).

Haettavat tietojenluovutuskiellot ovat henkilökohtaisia. Mikäli henkilö on hakenut em. tietojenluovutustietoja Trafilta ennen vuotta 2017 käsitellään ne aiemman tavan mukaisesti erillisesti Trafissa ja ne astuvat voimaan normaalisti (Trafi 2017).

4.3 Salainen numero

Puhelinnumero on mahdollista määrittää salaiseksi, jolloin se ei näy esimerkiksi numeropalveluissa. Puhelinnumero ei pääsääntöisesti ole salattu, vaan se pitää erikseen salata teleoperaattorin asiakaspalvelun tai nettisivujen kautta. Esimerkiksi Elisa tarjoaa numeron salaamiselle kolme eri vaihtoehtoa. Numero voi olla julkinen, jolloin sen käyttäjän tiedot näkyvät numeropalveluissa. Tiedot pitävät sisällään liittymänumeron ja sen omistajan nimitiedot. Lisäksi palvelun kautta voi näkyä henkilön itse lisäämiä tietoja kuten sähköposti, osoite tai jopa kasvokuva. Numero voidaan määrittää myös salaiseksi, jolloin sitä ei löydy numeropalveluiden kautta. Numerolle voidaan tehdä myös osittainen salaaminen, jolloin numeroon on ainoastaan liitetty sen omistajan nimitiedot ja paikkakunta. Numeron salaaminen rekisteröity numeropalveluihin muutamien päivien viiveellä (Elisa - salainen numero 2017).

Lisäksi liittymän käyttäjän on mahdollista salata numero soittaessaan puheluita. Näin ollen puhelun vastaanottaja ei pysty selvittämään soittajan puhelinnumeroa. Numeron salaamisen voi laittaa päälle automaattisesti, jolloin kaikki soitetut puhelut ovat sellaisia ettei vastaanottaja näe numeroa. Tämä tapahtuu puhelimen asetuksista. Toinen tapa salata numero on lisätä numeron eteen koodi #31#, jolloin puhelinnumero ei näy vastaanottajalle. Lähetettäessä viestejä tai multimediatekstejä numeroa ei voi salata. Liittymänumerot muodostuvat myös liikkuvien laajakaistojen käyttäjille, joilla on erillinen oma sim-kortti ja täten yksilöivä puhelinnumero. Tällaisia liikkuvia laajakaistoja käytetään nettitikuissa ja sim-kortillissa kannettavissa tietokoneissa (Sonera 2017).

4.4 Yritystoiminnan piilottaminen

Kaupparekisteri on julkinen ja yleiseen käyttöön tehty rekisteri. Yritys- ja yhteisölaki määrittelee rekisteriin rekisteröivät tahot. Yritys voi kuitenkin itse määrittellä mitä tietoja siitä on julkisesti löydettävissä. Kaupparekisteriin on ilmoitettava ainakin yksi yrityksen käyttämä osoite, mikä voi kuitenkin olla postilokero-osoite. Muuta julkiseksi tulevaa tietoa kaupparekisteriin ei tarvitse ilmoittaa (PRH 2017).

4.5 Muut tahot

Henkilötietolaki määrittelee henkilötietoja keräävän ja käsittelevän tahon yleiset periaatteet siitä miten henkilötiedoista tulee huolehtia, miten niiden käsittelyä tulee suunnitella, mitkä ovat henkilötietojen käsittelyn yleiset edellytykset ja käyttötarkoitussidonnaisuus. Lisäksi

henkilötietolaissa määritellään henkilötietojen laatua koskevat määräykset sekä siitä luotavan rekisteriselosteen edellytykset (Henkilötietolaki 22.4.1999/523).

Jokainen rekisterinpitäjä, esim. koulut ja urheiluseurat, määrittelee rekisteröitävien tietojen tarpeellisuuden. Mitkä tiedot ovat tarpeellista tietojä rekisteröidä ja mitkä tiedot eivät kuulu rekisteröitäväksi. Esimerkiksi urheiluseuran toimintaa osallistuvien henkilöiden nimitiedot voivat olla rekisterissä, mutta jäsenlistalla olevan ammatin, ei katsota olevan sellainen tieto, mikä objektiivisesti tarkastellen liittyy urheiluseuran toimintaan. (Tietosuoja 2013).

Jokaisella henkilöllä on henkilötietolain mukaan tarkastusoikeus omiin tietoihinsa, jotka on talletettuna rekisteriin tai saada tieto siitä, ettei hänestä ole rekisterissä tietoja. Rekisterin ylläpitäjän on samalla ilmoitettava rekisteröidylle ne lähteet, josta rekisteröidyn tietoja on hankittu ja mihin rekisteröityjä tietoja luovutetaan. Poikkeuksina tarkastusoikeuteen on lähinnä valtion kohdistuvat uhat (Henkilötietolaki 22.4.1999/523).

Henkilön itse pitää olla tietoinen ja valveutunut siitä missä toiminnassa hän tai hänen lähiomaisensa ovat ja voiko tieto mahdollisesti päätyä nettisivuille, julkiseen jäsenrekisteriin tai henkilömatrikkeleihin. Perustuslain 10§:n mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu (Suomen perustuslaki 11.6.1999/731). Lisäksi henkilötietolain 29§:n nojalla rekisterin pitäjän on oikaistava tai poistettava sellainen tieto mikä voi loukata rekisteröidyn yksityisyyden suojaa tai oikeuksia (Henkilötietolaki 22.4.1999/523). Näiden lakien pohjalta rekisteröity voi vaatia rekisterin pitäjältä toimia liittyen omien henkilötietojen julkisuuteen tai saatavuuteen. Tämä kuitenkin vaatii henkilöltä itseltään toimenpiteitä ja valveutuneisuutta, jotta luovutetut tiedot eivät ole julkisesti löydettävissä. Lisäksi toimet pitää suorittaa erikseen jokaiseen mahdolliseen tahoon missä henkilö on henkilötietojaan luovuttanut tai niitä on julkaistu.

5 Aktiiviset julkiset lähteet

Aktiiviset julkiset lähteet koostuvat sellaisista henkilön tiedoista jotka henkilö itse julkaisee. Aktiivisten julkisten lähteiden suurin osa-alue on sosiaalisen median palvelut, jonne henkilö päivittää itsestään tietoa. Tämän tiedon näkyvyys voi olla osittain henkilön itsensä rajaama. Tiedon rajaaminen yhdelle taholle on kuitenkin periaatteellisesti mahdotonta ja pääsääntönä voidaankin pitää sitä, että mitä itsestään on mm. sosiaaliseen mediaan laittanut, on se siellä ikuisesti ja siihen on mahdollisesti pääsy kaikilla. Tämä perustuu siihen, että vaikka henkilö omasta mielestään toimii kaikkien tietoturvasäännösten mukaisesti ja määrittelee myös omat yksityisyysasetuksensa parhaiden käytäntöjen mukaan, mikään ei varmista sitä, että joku toinen hänen piirissä oleva henkilö aiheuta toimillaan jopa tahattomasti tietojen leviämistä (VAHTI 4/2010, 21).

5.1 Sosiaalinen media

Nykyisessä tietoverkkoyhteiskunnassa on lähes mahdotonta toimia ilman internetiä ja sen mukanaan tuomia lukuisia tietoa kerääviä ja tuottavia palveluita. Internetistä onkin tullut tärkeä osa jokaisen ihmisen arkea ja se on Suomessa määritelty ihmisen yleismaalliseksi oikeudeksi (Ulkoasianministeriö 2011). Myös sosiaalinen kanssakäyminen on siirtynyt internetiin ja siitä on muodostunut ihmisten persoonallisuuden ja omakuvan jatke. Sosiaalisen median vaikutus yksilölle on iso ja ilman sitä voi henkilö jopa jäädä yhteisöistä ulkopuolelle.

Yleistyksenä sosiaalisesti mediaksi katsotaan palvelu, jossa henkilöt jakavat tuottamaansa tietoa muille tahoille. Tarkoituksena on olla vuorovaikutuksessa toisten ihmisten tai tahojen kanssa. Erilaisia keskustelufoorumeita ja yhteisöjä on internetissä lukemattomia ja niissä jaettava tiedon määrä on moninainen ja massiivinen. Sosiaalisen median perustana on tiedon jakaminen. Jaettava tieto ei ole määritelty, vaan se kattaa kaiken mahdollisen viestinnän kuvista videoihin ja twiiteistä blogeihin jne. NykYTEKNIKALLA on myös mahdollista jakaa sijaintitietoja tai vaikkapa juoksulenkin reitti ja mitatut sydämen sykkeen arvot (Järvinen, P. 2012, S. 290).

Sosiaalisten medioiden liiketoimintamalli perustuu käyttäjätietojen julkisuuteen. Lisäksi iso osa sosiaalisen median palveluista ovat rakennettu siten, että hakukoneet kuten Google, pystyvät hakemaan henkilöön liittyviä tietoja tietokantoihinsa. Tietokannoista tiedot ovat haettavissa jopa sen jälkeen kun ne on poistettu varsinaisesta lähteestä. Lisäksi tietokannat voivat olla julkisia ja kaikkien nähtävissä. Lisäksi sosiaalisten medioiden kautta voidaan selvittää henkilön sosiaalinen verkosto ja sen tuottama data (VAHTI 4/2010, 21).

Käyttäjä ei välttämättä ole tietoinen käyttämänsä sosiaalisen median palvelun käyttöehdoista ja tietojen julkisuudesta. Palvelun epäselvät tai muuttuvat sopimusehdot ovat iso haaste palvelun käyttäjälle. Ulkomailla sijaitsevat palvelut eivät ole Suomen lainsäädännön piirissä ja tämän vuoksi niiden sopimusehdot voivat poiketa huomattavasti suomalaisista palveluista (VAHTI 4/2010, 19).

Kirjautuminen erilaisiin sosiaalisiin medioihin tapahtuu sähköpostivarmistuksen kautta. Lisäksi palveluun syötetään paljon muita henkilötietoja, kuten nimi- ja syntymäaikatietoja. Sosiaalisessa mediassa esiinnyttään usein omalla nimellä, joihin pääosin on vielä liitetty henkilön oma kuva. Sosiaalinen media on tehnyt omien tietojen käyttämisen hyödylliseksi käyttäjälle itselleen. Palvelun käyttämisen helpottamiseksi henkilö suostuu vapaaehtoisesti ilmoittamaan oikeita henkilötietoja itsestään.

Tietoja kertyy palveluihin vuosien ajalta ja tulevaisuudessa henkilön koko elämän kattava aikajana on mahdollista selvittää. Tietojen päätyminen internetiin alkaa vanhempien

jakamista vauvakuvista ja loppuu ulkopuolisen tahon tekemään kuolleen henkilön muistoprofiiliin. Verkkoon muodostuu kokonaan uudenlainen verkkoidentiteetti, jonka tiedonmurusia yhdistelemällä ja analysoimalla voidaan saada hyvin tarkkoja tietoja, esimerkiksi siitä missä ja kenen kanssa henkilö viettää aikaa (VAHTI 4/2010, 21).

Internetiin on myös perustettu lukuisia erilaisia palveluita joiden kautta voi seurata aktiivisesti henkilön toimia sosiaalisissa medioissa. Esimerkiksi Social Searcher palvelun avulla voi kartoittaa henkilön käyttämiä sosiaalisia medioita ja valvoa aktiivisesti näiden palveluiden julkistamaa materiaalia. Palvelun voi laittaa ilmoittamaan uusista tapahtumista välittömästi sähköpostitse. Lisäksi palvelun avulla voi kartoittaa pelkän nimitiedon tai jonkin muun specifin tiedon esiintymistä sosiaalisen median palveluissa. Palvelun avulla voi siis linkittää kaikki yksittäisen henkilön käyttämät tilit yhteen ja valvoa kootusti niiden julkaisuja (Social-Searcher 2017).

Osa palveluista on maksullisia ja osaa pystyy käyttämään osittain maksuttomasti. Esimerkiksi Pipl (2017) sivuston kautta pystyy yhdistämään lähes kaiken henkilöön liittyvän tiedon yhdeksi kokonaisuudeksi, josta palvelu luo hakijalleen vielä lyhyen tiivistelmän haun kohteesta. Palvelu ei tyydy ainoastaan hakemaan tietoa avoimen internetin puolelta, vaan se osaa myös tulkita tietoja syvän internetin indeksoimattomasta datamassasta. Näin ollen se tuo normaalille käyttäjälle hyvin vaikeasti löydettävän tiedon esille vain yhdellä haulla. Hakuja voi suorittaa nimitiedoilla, sähköpostilla, puhelinnumerolla, sosiaalisen median käyttäjäprofiililla tai millä tahansa henkilöä yksilöivällä tiedolla.

Facebook GraphAPI on palvelun osa joka on tarkoitettu sovelluskehittäjille. Tämän avulla eri palveluntarjoajat voivat luoda palveluita Facebookiin tai tarjota Facebook-ominaisuuksia omilla sivuillaan. Facebook GraphAPI:n johdosta myös yksittäinen käyttäjä voi etsiä suoraan Facebookin hakupalvelusta tietoa Googlen hakupalvelun tapaan. Tällöin voidaan hakuja kohdistaa henkilöihin, tykkäyksiin, kuviin, vierailtuihin paikkoihin ja mihin tahansa tietoon mitä henkilö on mahdollisesti syöttänyt palveluun. Mikäli henkilö on osannut turvata sivunsa siten, ettei näitä tietoja voida etsiä, voidaan tietoa kuitenkin löytää kuvasta tykänneen henkilön kautta (Facebook Developers 2017). Tämän vuoksi sosiaalisen verkoston ja läheisten tai ystävien merkitys korostuu suoritettaessa henkilötiedustelua.

Internetistä on myös suoraan löydettävissä palveluita joiden kautta voi suorittaa henkilötiedustelua yksilöidystä Facebook-käyttäjistä. Haku tapahtuu suoraan henkilön yksilöivän Facebook-numeron perusteella, joka myös on selvitettävissä esimerkiksi sivuston (IntelTechniques - Facebook 2017) kautta.

Custom Facebook Tools

Search Target Profile:

Email Address (Account by Email)

+ 1 10 Digit Cell (Account by Cell)

FB User Name (Displays User Number)

Facebook User Number (Populate All)

Facebook User Number (Places Visited)

Facebook User Number (Recent Places Visited)

Facebook User Number (Places Checked-In)

Facebook User Number (Places Liked)

Facebook User Number (Pages Liked)

Facebook User Number (Photos By User)

Facebook User Number (Photos Liked)

Facebook User Number (Photos Of -Tagged)

Facebook User Number (Photo Comments)

Facebook User Number (Apps Used)

Facebook User Number (Videos)

Facebook User Number (Videos Of User)

Facebook User Number (Videos By User)

Facebook User Number (Videos Liked)

Facebook User Number (Video Comments)

Facebook User Number (Future Event Invitations)

Facebook User Number Year (Events Invited)

Facebook User Number Year (Events Attended)

Locate Target Profile:

People named....

People who work at....

People who worked at....

People who live in....

People who lived in....

School attended....

People who visited....

People who live in.... birth year....

People who live in.... and work at....

People who live in.... and worked at....

People named.... who live in....

People named.... who lived in....

People named.... birth year....

People named.... between age... and....

People named.... who work at....

People named.... who worked at....

Multiple Variables:

Name

Kuva 9: Kuvakaappaus IntelTechniquesin Facebook-hausta (Inteltechniques 2017)

5.2 Kuvien ja videoiden metadata

Internetistä löytyy kuvia ja videoita varten erillisiä hakukoneita, joilla haun voi suorittaa kuvan tai videon perusteella (Tineye 2017). Tällaisia ovat mm: TinYey tai Googlen Images palvelut. Näin yksittäisen tiedon perusteella voi löytää paljon muita tietoja aiheen ympäriltä tai kokonaan uusia tietolähteitä. Jälleen kerran tietoja yhdistelemällä voidaan luoda pienistä vähäpätöisistä tiedoista suuria kokonaisuuksia, joiden kautta käyttäjästä mallintuu kokonaisvaltainen kuva. Esimerkiksi sosiaalisessa mediassa julkaistu kuva kodin läheisyydestä voidaan paikantaa käyttämällä kuvahakua, joka löytää samanlaisia kuvia laajasta tietokannastaan. Näin toimimalla voidaan selvittää missä kuva on otettu ja paikallistaa henkilön sijainti (Fotoforensics 2017).

Internetselaimiin on myös ladattavissa lisäosia, jotka automaattisesti selvittävät kuvaan tai videoon liitettäviä metadatatietoja. Tällaisia metadatatietoja ovat mm. Exif-tiedot eli Exchangeable Image File format, jotka ovat kuvaa yksilöiviä tietoja, kuten käytetyn kameran tiedot ja kuvausolosuhteet. Matkapuhelimilla otetut kuvat sisältävät hyvin usein myös paikkatietoja, ellei tätä ominaisuutta ole erikseen kytketty pois käytöstä. Näin ollen julkisesti haettavaan kuvaan on saattanut jäädä tarkka tieto missä ja milloin kuva on otettu. Vaikka itse kuvaan ei välttämättä tallentuisi metadatatietoja, voi sovellukset kuten Instagram tai VKontakte lisätä julkaisuun automaattisesti paikkatiedon. Sovellusta asennettaessa käyttäjä hyväksyy, pääsääntöisesti lukematta, sovelluksen käyttöehdot. Näissä ehdoissa tuodaan

esille se, että sovellus kerää paikkatietoja jokaisesta siinä jaetussa kuvassa tai päivityksessä. Vaikka puhelimesta kytkisi sijaintitiedon pois päältä, voi sovellus hakea sijaintitiedon esimerkiksi läheisyydessä olevien langattomien verkkojen avulla. Internetistä on löydettävissä erilaisia ohjelmia joilla voi hakea julkaisuja sijainnin mukaan. Esimerkiksi Yomapic ohjelma tarjoaa ilmaiseksi mahdollisuuden selvittää tietyllä alueella tehdyt Instagram ja VKontakte julkaisut. Ohjelman avulla voidaan siis kartoittaa valikoidusta sijainnista tehdyt julkaisut ja näin selvittää vaikka talon tai viraston sisältä tulevia päivityksiä. Tarkkailua tekevä henkilö voi näin saada selville tarkkailtavan kohteen tai hänen läheisten käytössä olevia profiileja sekä tehtyjä päivityksiä (First Draft News 2016).

5.3 Muut verkkoyhteisöt

Internetissä on myös muunlaisia yhteisöjä kuin tavanomaiset isot sosiaalisen median palvelut kuten Facebook, Twitter tai Instagram. Erilaiset blogit tai myyntipaikat on isoja julkisen tiedon lähteitä, jonne henkilöt syöttävät hyvinkin yksilöiviä tietoja itsestään. Monet tällaiset palvelut eivät ole indeksoituja ja näin ne eivät ole samalla tavalla löydettävissä hakukoneilla. Osa erilaisista verkkoyhteisöistä vaatii sisäjäsenkirjautumisen, jotta palvelun tiedon saa näkyväksi, mutta yleisesti ottaen rekisteröityminen on ilmaista. Rekisteröitymistä ei kuitenkaan aina tarvitse sillä, tietoa voi löytyä myös sivustojen välimuistiversioista (joista tarkemmin kohdassa 6.3). Verkkoyhteisöihin kohdistuvia hakuja voi kohdistaa erilaisin hakutermein, esimerkiksi nimimerkin, puhelinliittymän tai sähköpostin avulla. Googlea tai Bingiä käytettäessä voidaan rajata hakutermejä siten, että haku kohdistetaan ainoastaan yhteen sivustoon, kuten huuto.net. Tällöin voidaan saada näkyviin jopa poistettuja ilmoituksia. Ilmoituksissa voi olla kuvia henkilön kotoa tai pihalta, tarkempia kaupunginosatietoja tai muuta hyvinkin yksilöiviä tietoja (Bazzel 2014, 157-163).

5.4 Pikaviestisovellukset

Nopean ja halvan internetin myötä useat erilaiset pikaviestisovellukset ovat laajentuneet normaaleille puhelinliikennemarkkinoille. Tällaisia sovelluksia ovat mm. Whatsapp ja Skype. Sovellusten kautta henkilö pystyy lähettämään viestejä ja soittamaan puheluita siten, että liikenne kulkee täysin digitaalisesti internetin kautta. Whatsapp-palveluun kirjaututaan pääsääntöisesti oman puhelinnumeron avulla, jolloin varmentaminen palveluun tapahtuu varsinaisen liittymän avulla (Whatsapp 2017). Palvelu ei kuitenkaan käytä varsinaisesti numeroa palvelun käyttöön yksilöivänä tunnuksena. Tämä tarkoittaa sitä, että henkilö voi kirjautua palveluun myös ilman puhelinnumeroa (Techbout 2015).

Tietoturvaongelmaksi pikaviestipalvelut muodostavat sen takia, että henkilöt käyttävät pääosin palvelussa omaa puhelinnumeroaan ja lisäävät palveluun muita tunnistetietoja kuten oman kuvansa. Esimerkiksi Whatsapp-sovelluksessa käytetyt profiilikuvat ovat täysin julkisia

ja ne näkyvät kaikille käyttäjillä. Profiilikuvan saa näkyviin lisätessään henkilön käyttämän numeron omaan puhelimeensa, jolloin se näkyy puhelimen osoitekirjassa tai profiilikuvia voi etsiä erilaisista avoimista palveluista kuten Wassame.com (Wassame 2017).

Pikaviestisovelluksiin lisätyt kuvat ovat kuitenkin vain yksi puoli siitä, miten puhelinnumeroa voidaan käyttää hakukeinona. Mikäli käyttäjä tallentaa saamansa puhelinnumeron omaan puhelimeensa ja käyttää sillä puhelimeen kytkettyjä ja rekisteröityjä palveluita kuten Instagram tai Facebook Messenger, voi puhelin automaattisesti linkittää puhelinnumeron siihen kuuluvaan käyttäjään ja tiliin. Tämä linkitys syntyy, vaikka henkilön profiilissa ei olisi julkisesti esillä numeroa, eikä sitä löytyisi edes numerolla sivustoilta haettaessa.

5.5 Sähköposti

Sähköposti on painotetuim tietoturvaohjeistuksissa. Sen kautta levitettävät haittaohjelmat ja tietojenkalastelu on iso ongelma yrityksille ja yksityishenkilöille. Ihmisten tapa käyttää ja luoda sähköpostitilejä on syy miksi se on myös ongelma julkisen tiedonhankinnan välineenä ja näin uhka henkilöturvallisuudelle.

Ihmiset yleisesti ottaen luovat sähköpostitilin samalla tavalla kuin sosiaalisen median tilin eli käyttävät siinä omaa nimeään. Lisäksi yleisenä olettamana on, että sähköpostiosoite luovutetaan sen enempää miettimättä, koska pääosin postilaatikkoon tulee muutenkin niin paljon roskapostia, että sitä ei ymmärretä kovin yksilöiväksi tiedoksi.

Sähköpostia voidaan kuitenkin käyttää hakusanana mm. hakukonepalveluissa. Hakukoneet tuovat näin esille eri palveluita joissa sähköpostia on käytetty ja joissa se on näkyvillä. Näin voidaan helposti selvittää henkilön käyttämiä sosiaalisen median tilejä sekä muita palveluita joita yksittäinen henkilö käyttää (Inteltechniques 2017).

Lisäksi internetistä on löydettävissä palveluita joiden kautta voi selvittää eri sähköpostipalveluiden automaattisesti suosittelimia sähköpostiosoitteita. Sähköpostipalvelut generoivat nimitiedot syöttämällä mahdollisia käytettävissä olevia sähköpostiosoitteita. Näitä hyväksikäyttämällä henkilö voi yrittää arvata haluamansa käyttäjän sähköpostiosoitteen ja päästä käsiksi sosiaalisen median tarjoamiin julkisiin tietoihin.

Yhtenä ongelmana sähköpostissa on sosiaalisten medioiden tarjoama kadonneen salasanan palautuspalvelu. Esimerkiksi Facebookissa kadonneen salasanan voi tilauttaa käyttäjän rekisteröimään sähköpostiosoitteeseen. Syötettäessä hakukenttään sähköpostiosoitteen, antaa palvelu näkyville siihen rekisteröidyn käyttäjätilin, osan linkitetystä puhelinnumerosta ja tilin profiilikuvan. Tämä palvelu on käytössä monissa sosiaalisen median palveluissa. Em.

selvittelyn avulla saadaan yksilöityä muuten täysin suojattu sosiaalisen median tili, joka ei edes näy hakukonepalveluissa (Facebook 2017).

Etsi käyttäjätilisi

Sähköposti, puhelin, käyttäjänimi tai koko nimi



En pysty tunnistamaan käyttäjätiliäni

Haku

Peruuta

Kuva 10: Facebookin käyttäjätilin tunnistaminen (Facebook 2017)

Vaihda salasanasi

Miten haluat vaihtaa salasanasi?

-  **Käytä tiliäni palvelussa Google**
Kirjaudu sisään palveluun Google (jos et ole jo) ja vaihda salasanasi nopeasti.
-  **Lähetä minulle sähköpostilla linkki, jonka kautta voin vaihtaa salasanani**
ville.virtanen@gmail.com



Ville Virtanen

Facebook-käyttäjä

Etkö voi enää käyttää näitä?

Jatka

Et sinä?

Kuva 11: Facebookin käyttäjätilin tunnistamisen esimerkkihaku ja tulokset (Facebook 2017)

6 Miten suojautua aktiivisissa lähteissä ja oikeus omaan yksityisyyden suojaan

Suomen kansalaisten yksityisyyden suojasta on säädetty henkilötietolaissa (523/1999), jossa saatettiin voimaan myös Euroopan unionin henkilödirektiivien määräykset.

Yksityisyydensuojasta on myös säädetty Suomen perustuslaissa (731/1999), joka toteutettiin säätämällä henkilötietolaki 1.6.1999. Henkilötietolain säätämisen tarkoituksena on ollut puuttua tietotekniikan mukanaan tuomiin tietosuojariskeihin. Tietosuojalakeihin voidaan lukea myös laki yksityisyyden suojasta työelämässä (759/2004) ja laki sähköisen viestinnän tietosuojasta (516/2004). Viranomaisten toiminnan julkisuudesta annettua lakia sovelletaan silloin, kun henkilötietoja käsitellään ja luovutetaan viranomaisten henkilörekistereissä.

Henkilötietolain (532/199) mukaan henkilötiedoilla tarkoitetaan kaikenlaisia henkilöön liittyviä merkintöjä, jotka kuvaavat häntä itseään, hänen elinolosuhteitaan tai ominaisuuksia. Tällaisia tietoja ovat henkilön perustiedot, kuten sosiaaliturvatunnus, nimi ja puhelinnumero. Lisäksi henkilötiedoiksi luetaan myös sellaiset tiedot joista henkilön voi tunnistaa epäsuorasti johonkin toiseen tietoon yhdistämällä. Tällaisia tietoja voivat olla vaikka henkilön pysyvästi käyttämä IP-osoite ja joissakin tapauksissa jopa henkilön omistaman auton rekisterinumero.

Henkilötietolain (523/199 §4) mukaan suomalaisen on kuitenkin tärkeää huomioida, että henkilötietolakia sovelletaan sellaisten henkilötietojen käsittelyyn, jossa henkilörekisteriä ylläpitävän tahon toimipaikka on Suomen alueella tai muuten Suomen oikeudenkäytön piirissä. Henkilötietolakia sovelletaan myös silloin kun rekisterinpitäjällä ei ole toimipaikkaa edes Euroopan Unionin jäsenvaltioiden alueella. Tällöin on kuitenkin huomioitava se, että rekisterinpitäjä käyttää henkilötietojen käsittelyssä Suomessa sijaitsevia laitteita muuhunkin tarkoitukseen kuin vain tietojen siirtoon alueen kautta, jolloin rekisterinpitäjällä on Suomessa nimetty edustaja. Pääsääntönä voi siis pitää sitä, että jos henkilö käyttää ulkomaille rekisteröityä palvelua, on hyvin todennäköistä ettei Suomen tai Euroopan Union henkilötietoja koskevia määräyksiä tarvitse noudattaa.

Suomessa henkilötietolain (523/199) mukaan henkilön on mahdollista ainoastaan kieltää henkilötietojensa käsittely suoramarkkinointi, etämyynti, markkina- ja mielipidetutkimuksissa sekä matrikkeleita ja sukututkimusta koskevissa asioissa. Mikäli tietoja haluaa poistaa muilla kuin tietojen virheellisyyden, puutteellisuuden tai vanhentuneisuuden vuoksi, voi se olla hyvin vaikeaa.

Euroopan unionin tietosuojalainsäädäntö on kuitenkin uudistunut ja uusi yleinen tietosuojasetus on tullut voimaan 24.5.2016. Asetuksella on kuitenkin kahden vuoden siirtymäaika, jonka puitteissa jäsenvaltioiden on saatava henkilötietojen käsittelyä koskevat tietosuojasetukset valmiiksi. Tämän asetuksen tarkoitus on lisätä henkilötietojen käsittelyn avoimuutta ja antaa rekisteröidylle enemmän oikeuksia omien henkilötietojensa käsittelyyn ja poistamiseen. Tällöin rekisteröity voi pyytää henkilötietoihinsa liittyvien linkkien, jäljennösten sekä kopioiden poistamista. Rekisterinpitäjällä on myös oikeus ilmoittaa asiasta niille tahoille, joille rekisterinpitäjä on henkilötietoja levittänyt (Tietosuojavaltuutetun toimisto 2017).

6.1 Kertakäyttöinen sähköposti

Ihmiset ovat laiskoja ja koska yhdellä henkilöllä on useita erilaisia tilejä ja profiileja internetissä, on yleistä, että kirjaututtaessa palveluun käytetään samaa sähköpostiosoitetta. Kirjaututtaessa uuteen palveluun pääsääntöisesti palvelu lähettää annettuun

sähköpostiosoitteeseen tunnistautumislinkin, jonka kautta varmennetaan käyttäjän olevan oikea ihminen. Kertakäyttöisen sähköpostin avulla henkilö voi luoda itselleen väliaikaisen sähköpostiosoitteeseen, jonne palvelun varmennussähköposti lähetetään. Tällä tavalla henkilö välttää eri palveluiden roskapostin, eikä hän yksilöi käyttämäänsä varsinaista sähköpostia eri tileihin ja näin mahdollista henkilötiedustelua suorittavalle henkilölle lisää mahdollisuuksia, joista tietoa voisi löytyä (Lifewire - email 2016).

Ilmaisia kertakäyttösähköpostipalveluita on useita erilaisia. Hyvin suosittu on esimerkiksi 10minutemail.com, joka antaa nimensä mukaisesti automaattisen sähköpostiosoitteen 10 minuutiksi. Palvelun avulla voi näin ollen hoitaa sisäänkirjautumisproseduurin (10minutemail 2017).

6.2 Tiedon näkyvyys internethakukoneissa

Julkisen sanan neuvosto on tehnyt periaatepäätöksen (4069/SL/09), missä henkilöllä ei ole oikeutta vaatia nimeensä liittyviä juttuja poistettavaksi tiedotusvälineiden ja lehtien verkkoarkistoista. Tietosuojadirektiivin rekisterinpitäjän velvollisuudet eivät siis koske tiedotusvälineitä ja näin ollen heidän ylläpitämänsä juttuarkistot eivät ole henkilörekistereitä.

Euroopan unionin tuomion C-131/12 mukaisesti internethakukoneen ylläpitäjä on vastuussa henkilötiedoista joita se on käsitellyt tuottaessaan hakutuloksia. Henkilötiedot voivat siis sijaita fyysisesti toisen palvelutarjoajan sivuilla, mutta hakukonepalvelun ylläpitäjän on poistettava tiedot omista kannoistaan jolloin tietoja ei voi hakea hakukonepalvelun kautta. Mikäli henkilö haluaa tietojensa poistettavan hakukonepalvelusta on asianomistajan itse tehtävä pyyntö suoraan hakukonepalvelun ylläpitäjälle tietojen poistamiseksi. Mikäli ylläpitäjä ei poista tietoja, voi asianomainen kääntyä toimivaltaisen viranomaisen puoleen. Asianomaisen on syytä huomioida se, ettei tiedot poistu internetistä kokonaisuudessaan, vaan niiden hakeminen ei ole enää mahdollista kyseisellä hakukonepalvelulla. Pyyntönsä jälkeen asianomaisen on huolehdittava myös siitä, että tieto poistetaan siitä lähteestä missä tieto on alunperin julkaistu. Tämäkään ei kuitenkaan vielä varmista, että tieto on täysin hävinnyt internetistä, koska joku muu taho on voinut taltioida tiedon ja julkaista sen toisen väylän kautta uudestaan tai säilöä sen omiin tarpeisiinsa.

Tuomion myötä Google on avannut tietojen poistamista varten oman palvelun, jossa henkilö voi pyytää Googlelta tietojensa poistamista hakukonepalvelusta. Poistamisen pyytäminen ei kuitenkaan takaa, että Google päätyy tiedon poistamaan, vaan pyynnön tarvitsee kattaa kriteerit:

1. Henkilö haluaa tehdä eurooppalaisten tietosuojalakien eli oikeus tulla unohdetuksi mukaisen poistopyynnön.
2. Hakutuloksissa on henkilökohtaisia tietoja kuten sosiaaliturvatunnus, pankkitilin tai luottokortin numero, käsikirjoitettu allekirjoitus tai henkilökohtainen seksuaalinen kuva tai video mitä jaetaan ilman lupaa.
3. Henkilöstä on virheellistä tietoa sisältävä sivu ja se halutaan poistaa Googlen hakutuloksista.
4. Henkilön nimi tai yrityksen nimi esiintyy aikuisviihdesivustossa, mikä esiintyy Googlen hakutuloksissa roskatuloksena
5. Googlen hakutuloksissa löytyy asiaomaisen kunniaa loukkaavaa sisältöä.

Henkilö voi eritellä sen mistä hän haluaa tietonsa poistettavan. Onko kyseessä ainoastaan Google-haussa esiintyvät tiedot vai tietojen estämisen näkymästä kokonaisuudessaan Googlen hakutuloksissa (Google 2017).

6.3 Tieto on näkyvillä vaikka se on poistettu varsinaisesta lähteestä

Vaikka tieto poistetaan näkyviltä tai kokonaisuudessaan sivustolta, tieto ei poistu internetistä. Vaikka 13% internetin tieteellisistä artikkeleista katoaa näkyvistä 27 kuukauden päästä tai tieto ei näytä samalta, muuttuvien sivustojen tai ohjelmien takia, tieto on silti löydettävissä (Meyer & Schroeder 2015). Tietojen tallennus ei ainoastaan tapahdu jonkun yksittäisen henkilön kautta. Internettiin laitettua materiaalia säilötään automaattisesti monen eri palvelun kautta ja se päättyy esimerkiksi Googlen cache-palveluun. Tällä tavoin Google pystyy tarjoamaan parempia hakukonepalveluita, koska poistettu tieto on mahdollisesti tallessa sen omilla palvelimilla ja näkyy suoraan varsinaisen haun alapuolella erillisenä linkkinä (Lifewire 2016).

Jopa internetselaimiin kuten Firefox on asennettavissa lisäosia, joiden kautta käyttäjä voi suoraan tarkastella sivua pääpiirteittäin sen koko olemassaolon ajalta. Tällöin esimerkiksi käyttäjän henkilökohtaisille sivuille laitettut perhekuvat tai urheiluseuran vuosi sitten virheellisesti julkaistu henkilötietoja sisältävä artikkeli on löydettävissä, vaikka ne olisi poistettu varsinaisilta sivuilta. Näitä tietoa voi myös etsitä esim The Wayback Machinen avulla, johon on tallennettuna 279 miljardia internetsivua (Internet Archive).

Tiedon poistaminen esimerkiksi Internet Archive:sta voi olla haasteellista. Pääsääntönä henkilön on lähetettävä palveluntarjoajalle pyyntö poistaa henkilötieto näkyvistä, mutta tässä saattaa mennä aikaa tai se jää kokonaan tekemättä. Jos henkilö itse hallinoi sivuja joiden kautta tieto on välittynyt Internet Archiven tietokantaan, voi henkilö laittaa sivustonsa kantaan erikseen määritellyn "robots.txt" tekstitiedoston. Tällöin esimerkiksi Internet Archive:n tietojenkerääjä tunnistaa sivuston sellaiseksi, ettei sen julkisia halua tietojään

ladattavan palveluun. Samalla aiemmin kerätyt tiedot poistetaan Internet Archive:sta ja näin ollen ne eivät ole näkyvillä The Wayback Machine:ssa (Harvard 2015).

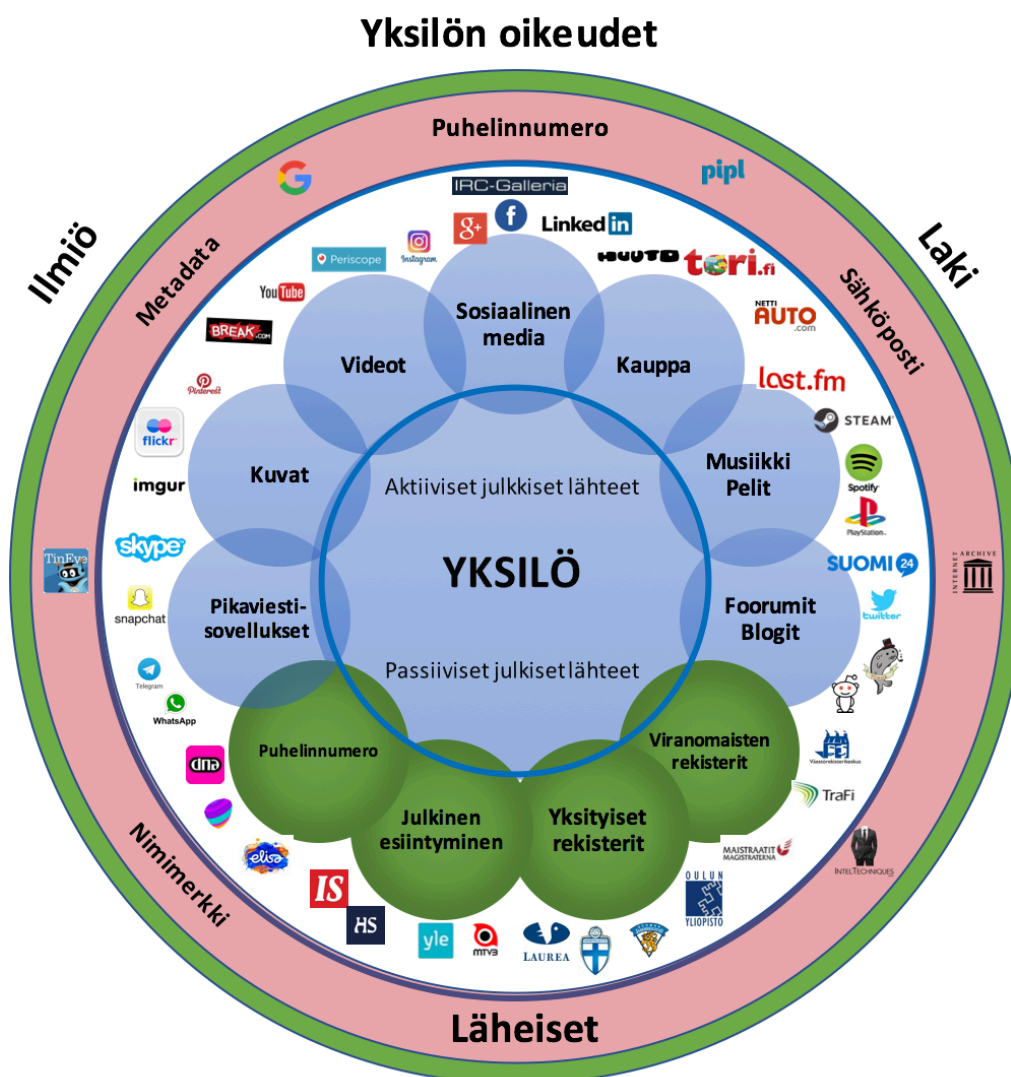
7 Opinnäytetyön tulokset

Opinnäytetyön tuloksena luotiin laajasta kokonaisuudesta tietoa tiivistävä ja selkeyttävä uhkamallikuvio ja uhkamalli. Näitä voidaan hyväksikäyttää työelämässä ja apuna mahdollisessa henkilöturvallisuusohjeessa. Lisäksi mallin tarkoitus on demonstroida julkisten lähteiden henkilöturvallisuusuhan laajuutta ilmiönä ja siinä olevia kytköksiä sekä suojautumiskeinoja.

7.1.1 Uhkamallikuvio

Uhkamallikuvion pääasiallisena tarkoituksena on visualisoida lukijalle julkisten lähteiden aiheuttama kokonaisvaltainen uhka. Jokainen henkilö muodostaa itsestään jonkinasteisen näkymän avoimiin lähteisiin ja tältä on miltei mahdotonta välttyä. Kuvion myötä lukijalle havainnollistuu tiedonjyvistä muodostuva laaja kokonaisuus ja tiedon järjestelmällisen keräämisen mahdollisuudet.

Kehän sisälle on kuvattu yksilö, josta tietoa valuu julkisesti saataville aktiivisten ja passiivisten julkisten lähteiden kautta. Ryhmäjako on eritelty kuviossa eri värein siten, että vihreät pallot kuvastavat passiivisia julkisia lähteitä ja siniset pallot aktiivisia julkisia lähteitä. Eri yritysten ja palveluiden logoilla on tuotu visuaalisesti esille esimerkinomaisesti internetissä olevien tahojen kirjoja. Uhkamallikuvion ei kuitenkaan ole tarkoitus olla täysin kattava kokonaisuus, vaan se on kuvattu suomalaisesta näkökulmasta tarkastellen. Lukijalle logojen esittäminen pyrkii herättelemään käsitystä siitä, mitä kaikkia palveluita hän itse käyttää ja näin ollen niiden kautta luovuttaa tietojaan mahdollisesti muiden saataville. Punainen rengas kuvastaa julkisten lähteiden tiedonhakuja ja sen hakumahdollisuuksia. Sitä millä tavoin julkisia lähteitä läpikäyvä henkilö pyrkii löytämään ja yhdistämään tietoa. Hakumahdollisuudet ja palvelut ovat pääpiirteittäin kuvattuna punaisen rengaan sisälle. Kuvion ulkoreunoja kierää vihreä rengas, jonka tarkoituksena on tuoda esille julkisten lähteiden tiedonkeruun suojaavat tekijät. Yksilön oikeudet ja sitä määrittävät lait turvaavat henkilöä ja kokonaisvaltainen ilmiön ymmärtäminen edesauttaa yksilöä rajoittamaan hänestä löytyvää tietoa. Tietojenluovutuskielloilla yksilö voi myös osittain pyrkiä estämään tiedon päätymistä julkiseksi.



Kuvio 3: Uhkamallikuvio

7.1.2 Uhkamalli

Uhkamallin tarkoituksena on tiivistää tutkimuksessa kerätty ja analysoitu tieto, helposti luettavaan ja yksinkertaiseen pohjaan. Uhkamallissa tuodaan kirjallisesti selitettynä tarkemmin esiin uhkamallikuviossa visualisoidut teemat. Malli on jaoteltu uhkamallikuvion ja tutkimuksen rakenteen mukaisesti siten, että passiiviset ja aktiiviset julkiset lähteet on jaettu erikseen.

Passiivisten julkisten lähteiden tietojen sijainti on tarkennettu erillisellä web-osoitteella, mikä mahdollistaa mallin käyttäjälle omien tietojen tarkastamisen. Lisäksi palvelun maksullisuus on eritelty. Punaisella eriteltyt riskit kuvastavat niitä tietoja, mitä palveluiden kautta on mahdollista päätyä julkiseksi. Vihreällä on kuvattu ne suojatumiskeinot, millä

tavoin tietojen luovutusta voi rajoittaa. Suojautumiskeinot on selvitetty tarkemmin mallin kolmannessa osassa.

Aktiivisten julkisten lähteiden tietojen sijainnista on mallin toisessa osassa annettu esimerkkejä. Punaisella värillä on tuotu esille ne riskit, joita aktiivisten julkisten lähteiden osa-alueet tuottavat. Vihreällä värillä on tuotu esille suojautumiskeinoja, jotka sopivat kokonaisuudessaan kaikkiin aktiivisten julkisten lähteiden osa-alueisiin.

Uhkamallin kolmannessa osassa on selvennetty maistraatista haettavia tietojenluovutuskieltoa. Punaiselle värillä on tuotu esille kiellon haittavaikutukset arkielämään ja vihreällä värillä kiellosta aiheutuvat positiiviset vaikutukset henkilöturvallisuudelle. Lisäksi kolmannessa mallin osassa on tuotu esille henkilön oikeuksia ja niihin liittyviä lakipykälä. Myös näiden osalta on otettu huomioon eri väreihin laeista ja oikeusasteiden tuomioista syntyneet positiiviset ja negatiiviset vaikutukset henkilöturvallisuudelle. Henkilön oikeuksien tuominen esille mallissa, helpottaa lukijaa vaatimaan palveluntarjoajalta omien tietojen poistamista esimerkiksi internethakunoiden tuloksissa.

Passiiviset julkiset lähteet			
Julkisten tietojen sijainti	Kustannus	Riski	Suojautuminen
Väestötietorekisteri (VTJ) https://www.osoitpalvelu.net/	Maksuton	<ul style="list-style-type: none"> · Luovuttaa henkilötietoja oman osoitepalvelunsa kautta ja myy ajantasaisia rekisteritietoja muille yksityisille yrityksille · Suomen kansalaisen kaikki henkilötiedot · Suomessa asuvan kaikki henkilötiedot 	Maistraatin tietojenluovutuskielet
Ajoneuvotietorekisteri (ATJ) https://asiointi.trafi.fi/	Maksullinen	<ul style="list-style-type: none"> · Ajoneuvon omistajan ja haltijan nimi ja osoitetiedot · Katsastus päivät ja paikat · Vakuutusyhtiö 	Maistraatin tietojenluovutuskielet
Kaupparekisteri (Virre) https://virre.prh.fi/	Maksullinen / Maksuton	<ul style="list-style-type: none"> · Palvelun kautta hankittavissa yrittäjän ja eri vastuutehtävissä olevien nimi-, osoite- ja puhelinnumero yms. tietoja. · Asunto-osakeyhtiön tiedot · Kommandiittiyhtiöiden tiedot · Avointen yhtiöiden ja osuuskuntien tiedot · Elinkeinoharjoittajien (toiminimien) tiedot 	Maistraatin tietojenluovutuskielet
Yhdistysrekisteri (Virre) http://yhdistysrekisteri.prh.fi/	Maksullinen / Maksuton	<ul style="list-style-type: none"> · Yhdistysten ja niiden vastuuhenkilöiden nimitiedot ja kotipaikkakunnan · Yhdistyksen jäsenluettelo (mahdollisuus 	Tiedot julkisia, harkittava miten tietoja päivitetään

		salata) · Tulevat kokoukset	
Oikeusrekisterikeskus http://www.oikeusrekisterikeskus.fi/fi/index/rekisterit/muutrekisterit.html	Maksullinen	· Keskuksen kautta sähköpostitse tai puhelimitse hankittavissa henkilötietoja sekä muita yksilöiviä tietoja · Konkurssi- ja yrityssaneeraustiedot · Velkajärjestelytiedot · Liiketoimintakiellot · Eläintenpitorekisteri (salainen) · Rikosrekisteri (salainen)	Haasteellista suojautua. Tiedot ovat julkisia
Luottorekisteri https://asiakastieto.fi/omatieto/fi	Maksullinen	· Palvelun kautta hankittavissa nimitiedot ja syntymäaika sekä oikeustoimikelpoisuus ja maksuhäiriömerkinnät · Maksuhäiriömerkinnät yksityisestä henkilöistä ja yrityksistä	Haasteellista suojautua. Tiedot ovat julkisia
Ulosottorekisteri https://asiointi.oikeus.fi/ulosotto-todistukset	Maksullinen	· Palvelun kautta hankittavissa tarkempia yksilöiviä tietoja henkilöstä. Tiedot ovat viimeisen kahden vuoden ajalta · Rekisteriin merkityn nimi-, osoite ja kotikuntatiedot sekä syntymäajan ja maksuhäiriömerkinnät	Haasteellista suojautua. Tiedot ovat julkisia, tosin hyvin rajatusti
Kiinteistörekisteri (KTJ) https://tiedostopalvelu.maanmittauslaitos.fi/tp/kartta	Maksullinen / Maksuton	· Kiinteistön tietoja (kiinteistönumero, sijainti- ja omistustietoja) · KTJ rekisteri on varsinaisesti viranomaisille tarkoitettu, mutta sillä on myös julkinen puoli	Haasteellista suojautua. Tiedot ovat julkisia
Teleoperaattorit http://www.siirretytnumerot.fi/ http://fonecta.fi/	Maksuton	· Luovuttavat henkilöiden nimi- ja osoitetietoja · Henkilön hallitsemien liittymien numeroita	Salainen numero
Julkinen esiintyminen · Lehdet · Muut arkistot · Tapahtumat	Maksuton	· Digitalisoiduissa arkistoissa henkilöiden nimi- ja olinpaikkatietoja · Kuvia, videoita ja muita yksilöiviä tietoja	Oltava yhteydessä tietojen julkaisijaan (ks. henkilön oikeudet)

Aktiiviset julkiset lähteet

Julkisten tietojen sijainti	Riski	Suojautumiskeinot
Sosiaalinen media · Facebook · Instagram · IRC-Galleria · yms.	· Yksilöiviä tietoja · Tulevat tapahtumat · Menneet tapahtumat · Kuvia ja videoita	· Selvitä profiilin turvallisuus ja yksityisyysasetukset, tarkastamalla profiilin näkyvyys, joko toisen profiilin avulla tai yksityisyysasetusten kautta.

Kauppa · Huuto.net · Nettiauto · Tori.fi, yms.	· Yksilöiviä tietoja · Olinpaikka · Käytetyt kulkuneuvot · Puhelin ja sähköposti	· Harkitse millä nimellä tai nimimerkillä esiinnyt internetissä. Älä käytä samoja tietoja eri palveluissa.
Musiikki ja pelit · Spotify · Last.fm · Steam community · Playstation community · yms.	· Tapahtumat · Mieltymyksen aiheet · Puhelin ja sähköposti · Nimi- ja henkilötiedot	· Älä käytä palveluissa samaa sähköposti-osoitetta. · Tutustu kertakäyttösähköpostipalveluihin.
Foorumit ja blogit · Suomi24 · Twitter · Ylilauta · Reddit, yms. · yms.	· Mielenpisteet · Tulevat tapahtumat · Menneet tapahtumat · Kuvia ja videoita · Olinpaikka · Puhelin ja sähköposti	· Älä jaa itsestäsi tarpeetonta tietoa. Jokainen kuva, tykkäys tai jopa läsnäolo palvelussa, paljastaa sinusta aina jotain. · Harkitse puhelinnumeron liittämistä nettiprofiiliin. Numeron avulla on mahdollista selvittää käytössä oleva profiilitili, vaikka numero ei ole näkyvillä.
Pikaviestisovellukset · Whatsapp · Skype · Telegram · Snapchat, yms.	· Some-profiilien linkitys · Profiilikuvat · Tilapäivitykset	· Huomioi myös pikaviestisovelluksesi julkisuus.
Kuvat · Pinterest · Imgur · Flickr, yms.	· Metadata · Yksilöiviä tietoja · Paikkatietoja · Reverse image search	· Huomioi kuvien ja videoiden metadata. Mitä paljastat tietämättäsi. · Kuvahakupalveluilla voidaan verrata otamaasi kuvaa ja näin selvittää kuvaan liittyvä profiili tai missä kuva on otettu.
Videot · Youtube · Periscope · Break.com, yms.	· Metadata · Yksilöiviä tietoja · Paikkatietoja	· Huomioi paikkatietoon perustuvat hakupalvelut, joilla voidaan selvittää yksilöidystä sijainnista tehdyt sosiaalisen median päivitykset (esim. Yomapic). · Ota huomioon myös läheistesi toimet internetissä.

Maistraatista haettavat tietojenluovutuskiellot

Turvakielto

- Määrittää henkilön kotikunnan, asuinpaikan, osoitteen ja muun yhteystiedon salaisiksi.
- Koskee myös henkilön omistuksessa tai hallinnassa olevan kiinteistön, rakennuksen ja huoneiston yksilöinti- ja sijaintitietoja.
- Tiedot voi ainoastaan luovuttaa sellaiselle viranomaiselle, jolla on lakimääritteinen oikeus nähdä tietoja ja kyseisten tietojen etsimiseen perusteltu virkatehtävä
- Haetaan perustellulla kirjallisella hakemuksella maistraatista
- Turvakiellon hakemisen jälkeen periaatteessa mikään taho ei voi saada VTJ:stä henkilötietoja
- Antaa kattavan eston henkilötietojen leviämiselle
- Kattaa nykyään myös ajoneuvot
- Voi määrittää postilokero-osoitteen mikä on julkinen
- Vaikeuttaa merkittävästi normaalia asioimista esim. luottokauppasopimuksia, muuttotilanteita, asiakkuusrekisterien osoitteiden päivittymistä, postin kulkua
- Jos henkilöllä muita vastuutehtäviä yrityksissä, taloyhtiöissä voivat henkilötiedot olla turvakiellosta huolimatta julkisesti saatavissa

Yhteystietojen luovutuskielto ja asiakasrekisterin päivityskielto

- Henkilön väestötietorekisteriin merkityjä yhteystietoja ei luovuteta sellaisille tahoille, jotka hyödyntävät VTJ:n tietoja.
- Yritykset eivät pysty päivittämään asiakasrekistereitään väestötietorekisteriin merkityjen tietojen perusteella
- Voidaan hakea sähköisesti Suomi.fi palvelusta
- Osoitetietoja ei luovuteta ulkopuolisille
- Ei vaikeuta normaalia asioimista niin paljon kuin turvakielto
- Kattaa ajoneuvot
- Asiakkuusrekisterit eivät päivity ja vaikeuttaa postin kulkua
- Jos henkilöllä muita vastuutehtäviä yrityksissä, taloyhtiöissä voivat henkilötiedot olla kiellosta huolimatta julkisesti saatavissa

Suoramarkkinointi-, henkilömatrikkeli- ja sukututkimuskielto

- Henkilön nimi- ja osoitetietoja ei luovuteta suoramarkkinointiin. Kyseisiä tietoja ei myöskään käytetä markkinatai mielipidemittauksissa pois lukien tieteellinen kyselytutkimus. Eikä niitä lähetetä henkilömatrikkeleita varten
- Voidaan hakea sähköisesti Suomi.fi palvelusta
- Henkilömatrikkeli-kielto tarkoittaa sitä, ettei henkilön nimi- ja osoitetietoja luovuteta esimerkiksi oppilaitoksen entisistä oppilaista tehtävää matrikkeliä varten
- Estää henkilötietojen välittämisen sukututkimuksiin ja suoramarkkinointiin
- Kielto estää ainoastaan postitse saapuvan mainonnan

Henkilön oikeudet ja muut keinot suojaautua

Salainen numero

- Henkilö itse määrittää numeron salaiseksi palveluntarjoajalta
- Numero on salainen ja sitä ei löydy erillisistä numero- ja osoitepalveluista
- Palvelu ei ole automaattisesti päällä
- Numeron salaus astuu voimaa parin päivän viiveellä
- Numero löydettävissä julkisesti, mikäli henkilö liittänyt sen esim. some-tileihin

Henkilötietolaki 22.4.1999/523

- Jokaisella henkilöllä on henkilötietolain mukaan tarkastusoikeus omiin rekisteriin talletettuihin tietoihin tai saada tieto siitä, ettei hänestä ole rekisterissä tietoja. Rekisterin ylläpitäjän on samalla ilmoitettava rekisteröidylle ne lähteet, josta rekisteröidyn tietoja on hankittu ja mihin rekisteröityjä tietoja luovutetaan.
- Henkilön itse pitää olla tietoinen ja valveutunut siitä missä toiminnassa hän tai hänen lähiomaisensa ovat ja voiko tieto mahdollisesti päätyä nettisivuille tai julkiseen jäsenrekisteriin tai henkilömatrikkeliin.

Henkilötietolaki 22.4.1999/523

- Henkilötietolain 29§:n nojalla rekisterin pitäjän on oikaistava tai poistettava sellainen tieto mikä voi loukata rekisteröidyn yksityisyyden suojaa tai oikeuksia.

Suomen perustuslaki 11.6.1999/731

- Perustuslain 10§:n mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu.

Euroopan unionin tuomio C-131/12

- Mikäli henkilö haluaa tietojaan poistettavan hakukonepalvelusta, on asianomistajan itse tehtävä pyyntö suoraan hakukonepalvelun ylläpitäjälle tietojen poistamiseksi. Mikäli ylläpitäjä ei poista tietoja, voi asianomainen käännyä toimivaltaisen viranomaisen puoleen.
- Asianomaisen on syytä huomioida se, etteivät tiedot poistu internetistä kokonaisuudessaan, vaan niiden hakeminen ei ole enää mahdollista kyseisellä hakukonepalvelulla. Pyyntöä jälkeen asianomaisen on huolehdittava myös siitä, että tieto poistetaan siitä lähteestä missä tieto on alun perin julkaistu. Tämäkään ei kuitenkaan vielä varmista, että tieto on täysin hävinnyt internetistä, koska joku muu taho on voinut taltioida tiedon ja julkaista sen toisen väylän kautta uudestaan tai säilöä sen omiin tarpeisiinsa.

Julkisen sanan neuvoston periaatepäätös (4069/SL/09)

- Henkilöllä ei ole oikeutta vaatia nimeensä liittyviä juttuja poistettavaksi tiedotusvälineiden ja lehtien verkkoarkistoista. Tietosuojadirektiivin rekisterinpitäjän velvollisuudet eivät siis koske tiedotusvälineitä ja näin ollen heidän ylläpitämänsä juttuarkistot eivät ole henkilörekistereitä.

Kuvio 4: Uhkamalli

8 Johtopäätökset

Opinnäytetyön tarkoituksena oli tarkastella julkisia tiedonhakulähteitä ja mahdollisuuksia kerätä tietoa indeksoidusta osasta tietoverkkoa. Lisäksi tarkoituksena oli selvittää keinoja miten yksittäinen henkilö voi torjua hänen tietojensa leviämisen julkisesti haettavaksi. Tutkimuksessa tuotiin esille mahdollisuuksia ja tapoja suorittaa henkilötiedustelua pääosin tietoverkkojen kautta. Lisäksi tuotiin esille se, millaisia erityyppisiä henkilötietoja on ja kuinka paljon niitä on saatavissa yksittäisestä henkilöstä. Tutkimuksessa käsiteltiin myös sitä, että henkilöön kytköksissä olevat toiset henkilöt sekä tapahtuvat paljastavat äärimmäisen paljon tarkkailtavan kohteesta. Hankkeen lähtökohtana ei ollut antaa täysin kattavaa listaa tiedonhaun keinoista. Tiedot, tavat, ohjelmat ja lait kehittyvät huimalla vauhdilla ja osa työssä esitellyistä keinosta voi hyvinkin olla vanhentuneita tai poistettu käytöstä opinnäytetyön muuten kuivuttua. Kokonaisvaltainen käsitys ja ymmärrys julkisen tiedonhaun mahdollisuuksista, antaa kuitenkin työn lukijalle näkemyksen siitä, millä tavoin tietoa valuu julkisesti saataville,

joko passiivisesti tai aktiivisesti. Tämä tieto muodostaa yksittäiselle ihmiselle merkittävän henkilöturvallisuusriskin.

Ennen henkilötietojen luovutuskieltojen hankkimista, tulisi henkilön tiedostaa se mitä tietoja hänestä on haettavissa. Tämän kartoittamiseksi henkilön olisi syytä selvittää omat ja perheenjäsenten julkiset vastuutehtävät, yritys- ja harrastustoiminta ja käytössä olevat puhelinliittymät. Lisäksi tulisi selvittää se mitä tietoja on itsestään antanut julkaistavaksi sosiaalisen median palveluiden kautta tai jossain muussa tilanteessa, kuten lehtihaastattelussa. Järeän turvakiellon käyttäminen on täysin turhaa, mikäli henkilöstä löytyy asuinpaikkatietoja, esimerkiksi taloyhtiönhallitukseen kuulumisen johdosta tai jos hän päivittää aktiivisesti tietoja henkilökohtaisista asioistaan sosiaalisessa mediassa.

Henkilöturvallisuuden kannalta olisi syytä harkita sosiaaliseen mediaan kuulumista tai ainakin rajoittaa se täysin yksityiseen käyttöön. Tämän lisäksi henkilön olisi suotavaa neuvoa ja kehottaa perhettään ja läheisiään huolellisuuteen sosiaalisen median käytössä. Millä ehdoin henkilötietoja ja niihin rinnastettavia yksilöiviä tietoja sosiaalisessa mediassa julkaistaan. Sellaisia tietoja ovat esimerkiksi kuvat tai paikkatiedot. Lisäksi henkilön ja hänen lähipiirinsä olisi tiedostettava ketä henkilöitä hyväksytään omaan verkostoon liitettäväksi eli miten hyvin voit luottaa siihen, että jaettu tieto ei siirry kolmansille osapuolille. (VAHTI 4/2010, 21)

Mikäli henkilö haluaa toimia sosiaalisessa mediassa, hän voi rajoittaa tiedonkalastelua toimimalla väärillä henkilötiedoilla sekä kuvilla ja huomioimalla yksittäisen sähköpostitilin tuomat haitat eri sosiaalisten median palveluiden kartoittamiseksi. Tämä ei kuitenkaan poista sitä, että tilin kautta julkaistu tieto ei päädy väärin käsiin ja sitä yhdistelemällä voi antaa itseltään sellaista tietoa, minkä ei ole tiedostanut olevan haitallista omalle turvallisuudelle.

Työssä kasattuun teoriapohjaan perustuen, henkilön on äärimmäisen vaikea tiedostaa, sitä tosiasiallista tiedon määrää ja kanavia mitä kautta hänestä on tietoa julkisesti havaittavissa. Lisäksi tutkimus perustui periaatteessa strukturoidun tietoverkon materiaaliin ja näin ollen kokonaisuuskuvaa ei edes esitelty. Huomioitavaa on kuitenkin se, että julkisen tiedon etsiminen on nykypäivänä tehty hyvin helpoksi, eikä se vaadi juurikaan teknistä osaamista, mikäli pysytään juuri strukturoidun tietoverkon puolella. (Kuvio 3: Uhkamallikuvio)

Yhtenä tärkeimmistä tutkimuksen löydöksistä oli se, että yksittäisen henkilön nimi- ja osoitetietojen salassa pitäminen on äärimmäisen vaikeaa, vaikka henkilöllä olisi käytössä järein turvautumiskeino eli turvakielto. Mikäli henkilö toimii minkäänlaisissa vastuutehtävissä, esimerkiksi taloyhtiön hallituksessa, ovat osoitetiedot tai vähintään kotikuntatiedot julkisia ja yhdistettävissä ja haettavissa ainoastaan henkilön nimellä. Tätä voi toki yrittää rajoittaa vedoten henkilötietolakiin, mutta se vaatii henkilön omia toimenpiteitä ja valvutuneisuutta.

Nimi- ja osoitetietojen valuminen kolmannelle osapuolelle ei kuitenkaan ole suurin uhka, vaan passiivisten rekistereiden kautta saatu tieto ainoastaan varmentaa ja takaa tiedon oikeellisuutta. Lisäksi yksityisten tahojen, esimerkiksi urheiluseurojen, ylläpitämät henkilörekisterit luovuttavat paljon tietoa, jota saadaan rikastutettua seurojen julkisten nettisivujen kautta.

Suurimpana uhkana ovat kuitenkin aktiiviset julkiset lähteet. Näiden palveluiden muuttuvat tietosuojakäytännöt ovat periaatteessa mahdottomia tiedostaa, ainakaan ajantasaisesti niiden muuttuessa palvelun päivityksen yhteydessä. Mikäli henkilöllä tai hänen läheisillään on käytössä erilaisia sosiaalisen median palveluita tai ovat kirjautuneita joihinkin verkkopalveluihin, on täällä luovutettu tieto vaikea salata.

Julkisten lähteiden hyödyntämisen ymmärtäminen on tärkein tapa suojautua ongelmaa vastaan. Henkilön tiedostaessa riskit siitä, että käyttäessään palveluita hän ei periaatteessa pysty olemaan jakamatta jonkinasteista tietoa itsestään muille. Lisäksi henkilön on ymmärrettävä se, että hänen ei itse tarvitse jakaa aktiivisesti tietoja, vaan ainoastaan läsnäolo palvelussa voi olla häntä vastaan käytettävä tieto, puhumattakaan siitä, että jokin läheinen ihminen joko julkaisee henkilöstä tiedon tai on ainoastaan henkilöön yhdistettävissä. Se, että henkilö hahmottaa ilmiön ja uhan kokonaiskuvan antaa hänelle ymmärryksen siitä, että varsinaisesti yksittäisellä tiedolla, kuten jonkin asian tykkäämisellä ei juurikaan ole merkitystä, mutta näitä kasattaessa henkilöstä muodostuva kuva on erittäin laaja ja monisyinen. Tietoja voidaan kasata takautuvasti jopa sukua koskevista kirkon kirjoista asti ja digitaalisessa yhteiskunnassa kaikki tiedot tulevat säilymään periaatteessa pysyvästi.

Oman oppimisen arviointi ja jatkotoimenpide-ehdotukset. Prosessina opinnäytetyö avasi tutkijalle paljon kehittämistyön menetelmiä ja niiden hyödyntämistä työelämäpohjaisissa projekteissa. Etenkin kun teoreettinen tutkimus oli tutkijalle varsin uutta, toi se selkeästi erilaisen näkemyksen ja lähestymistavan jo varsin pitkään työelämässä olleelle henkilölle. Työn aikana tutkija myös havaitsi sen, että työkokemuksen vaikutus lopullisen työn hyödynnettävyyden oikeassa elämässä kasvaa huomattavasti.

Opinnäytetyö oli toimintatutkimus, joka tehtiin palvelemaan työelämää. Tämän vuoksi tutkija käytti hyväkseen työyhteisössä työuransa aikana esiin tulleita oikeita uhkaustapauksia kirjallisuuskatsauksessa hankitun teoriapohjan muodostamisessa. Työkokemuksen nojalla tutkimuksen teoriapohjaa suunnattiin vastaamaan työyhteisön tarpeita ja osaltaan vastattiin osallistavaan kehittämiseen (Ojasalo, Moilanen & Ritalahti 2015, 59). Tutkijan harkittu valinta vaikutti tutkimuksen luotettavuuteen, jota olisi voitu lisätä suorittamalla esimerkiksi kyselytutkimus

työyhteisön sisällä. Tästä kuitenkin luovuttiin osittain ajallisen syyn vuoksi sekä kyselytutkimuksessa mahdollisesti saavutettujen uusien näkökulmien vähäisyyden vuoksi.

Opinnäytetyö avasi paljon myös sen tekijän näkökulmaa julkisten lähteiden aiheuttamasta turvallisuusriskistä. Tekniikan kehittyminen ja erilaisten ohjelmien ja sovellusten tarjoamat keinot antavat tulevaisuudessa todella laajan kirjon erilaisia mahdollisuuksia kehittää julkisten lähteiden tiedonkeruuta. Jatkotutkimuksen kannalta otollisia sektoreita olisivat julkisten tietojen keruun automatisointi ja strukturoimattoman tietoverkon hyväksikäyttäminen laajemman mittakaavan tiedonkeruussa. Suurten datamäärien hyödyntäminen luo tulevaisuudessa isoja uhkakuvia.

Lisäksi vihapuhe ja muuttunut turvallisuustilanne tuo esille uudenlaisia haasteita, etenkin julkisissa tehtävissä työskenteleville. Journalistisista ohjeista ei enää piitata, vaan erilaisiin epävirallisiin internetlehtiin sekoitetaan faktaa ja fiktiota, jotka pääosin ovat hankittu julkisten lähteiden avulla. Lisäksi virkamiehiä valokuvataan ja videokuvataan virkatehtävissä ja heidän löydettyjä henkilötietojaan julkaistaan erilaisissa foorumeissa. Yksityisyyden rajat ovat menettämässä merkitystään ja yksittäiset henkilöt asetetaan voimakkaan arvostelun kohteeksi. Näin esimerkiksi vihapuhe ja julkisesti hankittavat tiedot linkittyvät toisiinsa ja voisivat avata mielenkiintoisia tutkimuskohteita.

8.1 Työelämää hyödyntävät vaikutukset

Opinnäytetyön taustalla oli työyhteisössä esille tullut ongelma, jossa havaittiin usean eri tahon kautta, että joissakin tapauksissa yksittäisistä henkilöistä julkisista lähteistä saatava tieto aiheuttaa turvallisuusriskin. Työyhteisössä ei ollut käytettävissä selkeää ja kattavaa yksinkertaista ohjeistusta omien tietojen jakamisen rajaamiseksi taikka salaamiseksi. Käytössä olleet ohjeet olivat hajanaisia, eikä niissä oltu otettu huomioon esimerkiksi tietojenluovutuskieltojen haittavaikutuksia yksilölle.

Opinnäytetyön lopputuloksina syntyneitä uhkamallikuviota ja uhkamallia hiottiin yhdessä valtionhallinnon viraston kanssa, jonka avulla niiden käytettävyyttä pystyttiin tehostamaan. Saadun suullisen palautteen nojalla tutkija arvioi ja suunnitteli toimintatutkimuksen prosessia mukailen malleja vastaamaan paremmin juuri suomalaisen valtion viraston tarpeita (Ojasalo, Moilanen & Ritalahti 2015, 60). Saadun kirjallisen palautteen nojalla, tutkimuksessa saavutettuja tuloksia tullaan hyödyntämään oman henkilöstön, sidosryhmien sekä joissakin tapauksissa asiakkaiden ohjeistamisessa sekä koulutuksessa.

Saadun palautteen perusteella opinnäytetyö antaa kattavan ja helposti ymmärrettävän kuvan Suomessa tällä hetkellä olevista julkisista lähteistä sekä keinoista jolla yksilö pystyy rajaamaan tietojen näkyvyyttä. Lisäksi työtä pystytään hyödyntämään valtion virastossa myös

henkilöstön oman työn helpottamiseksi. Työssä esiteltyjen esimerkkien avulla työntekijät voivat itse suorittaa tiedonhankintaa julkisten lähteiden avulla.

Lähteet

Painetut lähteet:

Appel, J.A. 2015. Internet Searches for Vetting, Investigations, and Open-Source Intelligence. 2., painos. USA: CRC Press

Bazzel, M. 2014. Open Source Intelligence Techniques. 3., painos. USA

Bertram, S. 2015. The Tao of open source intelligence. UK: IT Governance

Hirsjärvi, S., Remes, P. & Sajavaara P. 2001. Tutki ja kirjoita. 6.-7., painos. Vantaa: Tummavuoren kirjapaino

Järvinen, P. 2012. Arjen tietoturva. Jyväskylä: Docendo

Korhonen, P. 2003. Perus rekisterit ja tietosuojat. Helsinki: Edita.

Layton, R. & Watters, P. 2016. Automating open source intelligence. USA: Elsevier

Meyer, E. & Schroeder, R. 2015. Knowledge Machines: Digital Transformations of the Sciences and Humanities. England: The MIT Press

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2015. Kehittämistyön menetelmät. 3.-4., painos. Helsinki: Sanoma Pro

Vehkamäki, P. & Tamminen-Dahlman, A. 2006. Julkisuus ja tietosuojat opetustoimessa - opas koulujen ja oppilaitosten käyttöön. 3. muuttamaton painos. Helsinki: Opetushallitus

Vuorinen, T. 2013. Strategiakirja 20 työkalua. Helsinki: Talentum

Sähköiset lähteet:

Avidian. 2017. Viitattu 7.4.2017.

<https://www.avidian.com/blog/social-media-and-psychology-why-do-people-share>

CIA. 2010. Viitattu 6.6.2017.

<https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html>

Elisa - asiakasrekisteri. 2016. Viitattu 8.1.2017.

<https://elisa.fi/asiakaspalvelu/aihe/sopimusehdot/ohje/asiakasrekisteriseloste/>

Elisa - salainen numero. 2017. Viitattu 8.1.2017.

<https://elisa.fi/asiakaspalvelu/aihe/matkapuhelinliittymat/ohje/salainen-numero/>

Ethority 2017. Viitattu 28.2.2017.

<http://ethority.net/social-media-prisma/>

Euroopan Unionin tuomio C-131/12.

<http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:62012CJ0131&from=FI>

Facebook. 2017. Viitattu 30.1.2017.

<https://www.facebook.com/login/identify?ctx=recover&lwv=100>

Facebook Developers. 2017. Viitattu 28.2.2017.

<https://developers.facebook.com/docs/graph-api/>

First Draft News. 2016. Viitattu 23.4.2017.

<https://firstdraftnews.com/tool-for-newsgathering-find-geolocated-pics-with-yomapic-journalism-instagram-vkontakte/>

Fonecta. 2016. Viitattu 14.12.2016.

<https://hyotyieto.fonecta.fi/fonectan-palvelut-kuluttajille/tietosuoja>

Fonecta. 2017. Viitattu 8.1.2017.

<https://www.fonecta.fi/info/hyodyllista-tietoa/rekisteriselosteet/fonectan-asiakasrekisteri/>

Fotoforensics. 2017. Viitattu 27.3.2017.

<http://fotoforensics.com/tutorial-meta.php>

Geneologia. 2017. Viitattu 4.1.2017.

<http://www.geneologia.fi/kirkonkirjat>

Google. 2017. Viitattu 20.2.2017.

<https://support.google.com/websearch/troubleshooter/3111061?hl=fi>

Harvard. 2015. Viitattu 28.2.2017.

<https://blogs.harvard.edu/philg/2015/01/28/web-publishers-can-delete-stuff-from-archive-org/>

Henkilötietolaki 22.4.1999/523. Viitattu 28.2.2017.

<http://www.finlex.fi/fi/laki/ajantasa/1999/19990523#L4P19>

IBM. 2017. Viitattu 6.6.2017.

<https://www.ibm.com/big-data/us/en/>

Inteltechniques. 2017. Viitattu 30.1.2017.

<https://inteltechniques.com/menu.html>

Inteltechniques - Facebook. 2017. Viitattu 28.2.2017.

<https://inteltechniques.com/osint/facebook.html>

Internet Archive. 2017. Viitattu 28.2.2017.

<http://archive.org/web/>

Julkisen sanan neuvosto päätös 4069/SL/09. Viitattu 28.2.2017.

<http://www.jsn.fi/periaatepaatokset/periaatepaatos-verkkoarkistoista/>

Kiinteistörekisterilaki 16.5.1985/392. Viitattu 28.2.2017.

<http://www.finlex.fi/fi/laki/ajantasa/1985/19850392>

Laki ajoneuvoliikennerekisteristä 13.6.2003/541. Viitattu 28.2.2017.

<http://www.finlex.fi/fi/laki/ajantasa/2003/20030541>

Laki ulosottokaaresta 15.6.2007/705. Viitattu 28.2.2017.

<http://www.finlex.fi/fi/laki/ajantasa/2007/20070705#L1>

Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621. Viitattu 28.2.2017.

<http://www.finlex.fi/fi/laki/ajantasa/1999/19990621>

Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista 21.8.2009/661. Viitattu 28.2.2017.

<http://www.finlex.fi/fi/laki/ajantasa/2009/20090661>

Lifewire - email. 2016. Viitattu 28.2.2017.

<https://www.lifewire.com/why-you-need-a-disposable-email-account-2487629>

Lifewire. 2016. Viitattu 28.2.2017.

<https://www.lifewire.com/highlight-keyword-google-cache-search-1616811>

Maanmittauslaitos - kiinteistö. 2017. Viitattu 8.1.2017.

<http://www.maanmittauslaitos.fi/kiinteistot/rekisterit-otteet/kiinteistotietojarjestelma-ktj>

Maanmittauslaitos - lainhuuto. 2017. Viitattu 8.1.2017.

<http://www.maanmittauslaitos.fi/aineistot-ja-palvelut/palvelut/lainhuutotodistus>

Minilex. 2017. Viitattu 6.6.2017.

<https://www.minilex.fi/a/yksityisyyden-suojan-m%C3%A4%C3%A4ritelm%C3%A4>

Moyer, S., Hamiel, N. 2008. Satan is on my Friend List: Attacking Social Networks. BlackHat USA Briefings. 2008. Viitattu 7.4.2017.

https://www.blackhat.com/presentations/bh-usa-08/Moyer_Hamiel/BH_US_08_Moyer_Hamiel_Satan_is_on_my_Friends_List_Whitepaper.pdf

Oikeusrekisterikeskus. 2017. Viitattu 17.2.2017.

<http://www.oikeusrekisterikeskus.fi/fi/index/rekisterit/muutrekisterit.html>

Palloliitto. 2017. Viitattu 14.1.2017.

<https://www.palloliitto.fi/pelipaikka/rekisteriseloste>

Pew Research Center. 2016. Viitattu 6.6.2017.

<http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/>

Pipl. 2017. Viitattu 17.2.2017.

<https://pipl.com/>

PRH - yhdistysrekisteri. 2017. Viitattu 4.1.2017.

<https://www.prh.fi/fi/yhdistysrekisteri.html>

PRH - kaupparekisteri. 2017. Viitattu 4.1.2017.

https://www.prh.fi/fi/kaupparekisteri/yleista/kaupparekisterin_julkisuus.html

PRH - tiedot. 2017. Viitattu 4.1.2017.

https://www.prh.fi/fi/kaupparekisteri/yleista/henkilotunnuksista_ja_kotiosoitteista.html

PRH. 2017. Viitattu 8.1.2017.

https://www.prh.fi/fi/uutislistaus/2012/P_693.html

Puolustusministeriö. 2015. Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tulostettu 15.2.2017.

http://www.defmin.fi/files/3016/Suomalaisen_tiedustelulainsaadannon_suuntaviivoja.pdf

Social-Searcher. 2017. Viitattu 30.1.2017.

<https://www.social-searcher.com/about/>

Sonera. 2017. Viitattu 8.1.2017.

<https://www.sonera.fi/asiakastuki/ohjeet/Matkapuhelinliittyma-numero--ja-asiakastiedot?id=1192>

Suomen Asiakastieto Oy Viitattu. 2017. 17.2.2017.

<https://www.asiakastieto.fi/>

Suomen perustuslaki 11.6.1999/731.

<http://www.finlex.fi/fi/laki/ajantasa/1999/19990731#L2P10>

Techbout. 2015. Viitattu 8.1.2017.

<http://www.techbout.com/whatsapp-without-phone-number-sim-5365/>

Techland. 2012. Viitattu 17.2.2017.

<http://techland.time.com/2012/02/17/how-target-knew-a-high-school-girl-was-pregnant-before-her-parents/>

The Guardian. 2015. Viitattu 28.2.2017.

<https://www.theguardian.com/world/2015/jun/03/bloggers-social-media-russian-soldiers-fighting-in-ukraine>

The psychology of sharing. 2011. Viitattu 7.4.2017.

<http://www.iab.net/media/file/POSWhitePaper.pdf>

Tietosuojaavaltuutetun toimisto. 2010. Yhdistyksen jäsenluettelot ja henkilötietolaki. Viitattu 8.1.2017.

http://www.tietosuoja.fi/material/attachments/tietosuojaavaltuutettu/tietosuojaavaltuutetun-toimisto/oppaat/6JfqOozpn/Yhdistyksen_jasenluettelot_ja_henkilotietolaki.pdf

Tietosuojaavaltuutetun toimisto. 2017. Miten valmistautua EU:n tietosuoja-asetukseen? Viitattu 8.1.2017

http://www.tietosuoja.fi/material/attachments/tietosuojaavaltuutettu/tietosuojaavaltuutetun-toimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Tietosuoja. 2013. Viitattu 8.1.2017.

<http://www.tietosuoja.fi/fi/index/rekisterinpitajalle/minkalaisiahenkilotietojavoikasitella.html>

Tineye. 2017. Viitattu 30.1.2017.

<https://www.tineye.com/>

Trafi. 2016. Viitattu 16.12.2016.

http://www.trafi.fi/tietopalvelut/trafin_rekisterit/

Trafi. 2017. Viitattu 4.1.2017.

http://www.trafi.fi/tietopalvelut/trafin_rekisterit/tietojenluovutuskiellot

Ulkoasianministeriö. 2011. Viitattu 30.1.2017.

<http://www.formin.fi/public/default.aspx?contentid=223872&contentlan=1&culture=fi-FI>

Valtiovarainministeriö 2010. Sosiaalisen median tietoturvaohje (VAHTI 4/2010). Viitattu 4.1.2017 https://www.vahtiohje.fi/c/document_library/get_file?uuid=8b44c0bf-cff3-4e6c-a587-eea58a9e3ad7&groupId=10229

VTJ. 2016. Viitattu 16.12.2016.

<http://vrk.fi/vaestotietojarjestelma>

Väestörekisterikeskus. 2016. Viitattu 16.12.2016.

<http://vrk.fi/suoramarkkinointi-henkilomatrikkeli-ja-sukututkimuskielto>

Väestörekisterikeskus. 2017. Viitattu 4.1.2017.

<https://verkkopalvelu.vrk.fi/Omat/Etusivu.aspx>

Väestörekisterikeskus - turvakielto. 2016. Viitattu 16.12.2016.

<http://vrk.fi/turvakielto>

Väestörekisterikeskus - tiedot. 2016. Viitattu 16.12.2016.

<http://vrk.fi/yhteystietojen-luovutuskielto>

Väestörekisterikeskus - osoite. 2016 Viitattu 16.12.2016.

<https://eevertti.vrk.fi/osoitetietoja-vaestotietojarjestelmasta-paivittavat-asiakkaat>

Wassame. 2017. Viitattu 8.1.2017.

<http://wassame.com/frequently-asked-questions/>

Whatsapp. 2017. Viitattu 8.1.2017.

<https://www.whatsapp.com/faq/fi/general>

Wikipedia. 2017. Viitattu 28.2.2017.

<https://fi.wikipedia.org/wiki/IP-osoite>

10minutemail. 2017. Viitattu 28.2.2017.

<https://10minutemail.com/10MinuteMail/about.html?dswid=-6890>

Kuvat:

Kuva 1: Sosiaalisen median prisma (Ethority 2017).....	14
Kuva 2: Isoimmat syyt tietojen jakamiseen verkossa (Avidian).....	15
Kuva 3: ATJ:sta tilattavat ajoneuvon perus- ja historiatiedot.....	21
Kuva 4: ATJ:sta tilattavat ajoneuvon tekniset tiedot.....	22
Kuva 5: Yritysten haku Virre-palvelun avulla.....	23
Kuva 6: Esimerkki yrityshausta Fonectan Finder palvelusta	24
Kuva 7: Haku yhdistysrekisteristä	25
Kuva 8: Esimerkki henkilöhausta Fonectan Finder palvelussa.	28
Kuva 9: Kuvakaappaus IntelTechniquesin Facebook-hausta.....	37
Kuva 10: Facebookin käyttäjätilin tunnistaminen	40
Kuva 11: Facebookin käyttäjätilin tunnistamisen esimerkkihaku ja tulokset	40

Kuviot

Kuvio 1: Tiedustelusykli (Puolustusministeriö 2015, 15).....	10
Kuvio 2: Opinnäytetyön viitekehys.....	10
Kuvio 3: Uhkamallikuvio	45
Kuvio 4: Uhkamalli.....	50