Saimaan ammattikorkeakoulu
Liiketalous Lappeenranta
Liiketalouden koulutusohjelma
Yritysten ja taloushallinnon juridiikka

Kaisa Kurkaa

Yksityishenkilöön kohdistuva identiteettivarkaus

Opinnäytetyö 2013

Tiivistelmä

Kaisa Kurkaa
Yksityishenkilöön kohdistuva identiteettivarkaus, 39 sivua
Saimaan ammattikorkeakoulu
Liiketalous Lappeenranta
Liiketalouden koulutusohjelma
Yritysten ja taloushallinnon juridiikka
Opinnäytetyö 2013
Ohjaajat: Raili Toikka, Saimaan ammattikorkeakoulu

Opinnäytetyön aiheena on tutkia identiteettivarkauden vaikutusta yksityishenkilöön. Tarkemmin perehdytään sosiaalisessa mediassa tapahtuviin identiteettivarkauksiin, sillä sosiaalinen media sekä erilaiset verkkoyhteisöt ovat valtaosalla ihmisistä päivittäisessä käytössä. Tämän vuoksi myös rikollisuus on siirtynyt verkkoon, koska siellä on mahdollista tavoittaa suuret ihmismäärät.

Identiteettivarkaus voidaan määrittää toisen henkilötietojen, kuten nimen tai henkilötunnuksen oikeudettomana käyttönä. Identiteettivarkaus esiintyy taloudellista hyötyä tavoittelevana sekä kiusantekona tai ilman vahingoittamistarkoitusta, jolloin tekijä ei välttämättä ymmärrä tehneensä mitään väärää. Verkkoaikakauden myötä identiteettivarkauksista on tullut täysin uudenlainen ongelma. Erilaisiin verkkoyhteisöihin esimerkiksi Facebookiin perustetaan toisen henkilön nimissä sivuja, joilla levitetään loukkaavaa ja virheellistä aineistoa. Valesivuista on tullut moderni koulukiusaamisen muoto.

Opinnäytetyössä käydään läpi identiteettivarkauden määritelmät, miten identiteettivarkaus tapahtuu, sen keskeiset uhat ja uhrin asema. Pääpaino on identiteettivarkauksien ehkäisyssä. Nykyinen lainsäädäntö ei ole pysynyt alati kasvavan verkkorikollisuuden mukana. Identiteettivarkaus pitäisi kriminalisoida, koska nykylainsäädäntö ei suojele uhria tarpeeksi.

Asiasanat: Identiteettivarkaus, sosiaalinen media, lainsäädäntö

Abstract

Kaisa Kurkaa
Identity Theft of a Private Person, 39 pages
Saimaa University of Applied Sciences
Faculty of Business Administration, Lappeenranta
Degree Programme in Business Administration
Specialization in Business Law
Bachelor's Thesis 2013
Instructor: Ms Raili Toikka, Senior Lecturer

The subject of this thesis is to investigate identity theft of a private person. The main focus is on identity thefts that take place in social networks, because social media and social networks are used every day by most people. This is why this type of crime has moved to the Internet.

Identity theft can be specified as use of another person's personal details, such as name or social security number, without permission. Identity thefts can emerge in pursuit for financial benefit or as sabotage or without any intention to do harm, when the subject does not necessarily understand his or her actions. In the age of the Internet, identity thefts have become a whole new kind of a problem. In different networks, for example Facebook, pages are set up under the names of other persons and used to spread insulting or false content. Fake pages have become a modern form of school teasing.

This thesis opens up definitions of identity theft and describes how identity thefts are committed, focusing on the main threats and the status of the victim. The main focus is on how to prevent identity thefts. Legislation has not been able to keep up with the constantly growing cybercrime. Identity theft should be criminalized immediately, because current legislation does not sufficiently protect the victim.

Keywords: Identity theft, social media, legislation

Sisällys

1 Johdanto

Opinnäytetyöni tavoitteena on selvittää, mikä identiteettivarkaus on. Se koostuu hyvin monista ja vaikeasti määriteltävistä kokonaisuuksista, koska identiteettivarkauden käsite ei ole yksiselitteinen tai täysin määritelty. Tämä asetti opinnäytetyön tekemiselle omat haasteet ja ongelmat. Identiteettivarkaus tarkoittaa suurta joukkoa erilaisia tekokokonaisuuksia. Yhteistä näille teoille on se, että jotakin identiteettitietoa kerätään oikeudetta.

Identiteettivarkaus esiintyy taloudellista hyötyä tavoittelevana, kiusantekona ja pilailuna tai ilman vahingoittamistarkoitusta, jolloin tekijä ei välttämättä edes ymmärrä teon vaikutusta. Sen yleisimmät esiintymismuodot sosiaalisessa mediassa ovat kunnianloukkaus, yksityiselämää loukkaavan tiedon levittäminen, viestintäsalaisuuden loukkaus, petos, laiton uhkaus, luvaton käyttö ja tietomurto. Sosiaalinen media sekä erilaiset verkkoyhteisöt ovat valtaosalla ihmisistä päivittäisessä käytössä ja käyttäjien joukko kasvaa jatkuvasti. Tavoitteena on saada mahdollisimman kattava näkemys niistä yksityishenkilön identiteettivarkauksiin liittyvistä keskeisistä uhista, jotka aiheutuvat sosiaalisen median käytöstä. Olen myös perehtynyt tarkemmin siihen, kuinka identiteettivarkauksilta voi suojautua. (Poliisi. Identiteettivarkaudet 2013.)

Suomessa pohditaan tällä hetkellä identiteettivarkauden kriminalisoinnin tarvetta, koska tietoverkko on muuttanut toimintaympäristöä niin merkittävästi. Lainsäädäntö tulisi päivittää ajan tasalle, jotta identiteettivarkaus saataisiin kriminalisoitua. Tällä hetkellä uhrin asema identiteettivarkaudessa on huono, sillä nykyinen lainsäädäntö ei ole pysynyt verkkorikollisuuden valtavan kasvun mukana.

1.1 Tavoitteet ja tutkimusmenetelmät

Tavoitteena on saada selvyys siitä, mikä identiteettivarkaus on, selvittää uhrin asema ja tarkemmin etsiä tietoa siitä, miten identiteettivarkaudelta voi yrittää suojautua.

1.2 Tutkimusongelma

Identiteettivarkaudet ovat hyvin monimuotoisia eikä niille löydy yksiselitteisiä määritelmiä. Alkuun ongelmaksi muodostui vähäinen faktatieto aiheesta. Lopulta, kun tietoa alkoi löytyä, niin sitä oli hieman vaikea rajata ja pysyä pääaiheessa.

2 Identiteettivarkaus

Identiteettivarkaus tarkoittaa toisen henkilötietojen, kuten nimen tai henkilötunnuksen oikeudetonta käyttöä. Identiteettivarkaus on laaja joukko erilaisia tekokokonaisuuksia, yhteistä näille teoille on se, että kerätään oikeudetta jotakin identiteettitietoa. Kerättyä identiteettitietoa käytetään edelleen joko rikoshyödyn hankkimiseksi tai tavalla, josta aiheutuu identiteetin haltijalle vahinkoa. Tyypillisesti tekijä pyrkii näissä teoissa hyötymään tekemällä rahanarvoisia sitoumuksia toisen henkilön nimissä. Esimerkiksi ottaa luottoja toisen nimeen. (Henkilöllisyyden luomista koskeva hanke 2010.)

2.1 Identiteettivarkauden määritelmät

Identiteettivarkaus ilmenee yleensä taloudellista hyötyä tavoittelevana, kiusantekona ja pilailuna tai ilman vahingoittamistarkoitusta, jolloin tekijä ei välttämättä edes ymmärrä tekevänsä mitään väärää. Nimityksenä identiteettivarkaus on jopa harhaanjohtava, sillä toisin kuin varkausrikoksessa (RL 28:1), identiteettivarkaudessa identiteettiä ei välttämättä oteta missään vaiheessa pois rikosuhrin hallusta. (Henkilöllisyyden luomista koskeva hanke 2010.)

Usein identiteettitietoja kerätään laajasti eri lähteistä. Yleisimmät näistä lähteistä ovat sähköisesti kerättävät yksityisyystiedot, joita saadaan erilaisten verkon haitta- tai vakoiluohjelmien kautta. Esiintyminen toisena henkilönä voi pilata uhrin nimen ja maineen. Seuraukset voivat olla pitkäaikaisia ja hankaloittaa uhrin elämää hyvin kauankin, jopa monia vuosia. (Henkilöllisyyden luomista koskeva hanke 2010.)

2.2 Perinteiset identiteettivarkaudet

Perinteiset identiteettivarkaudet tuleva ilmi väärennysrikoksina (RL 33) tai petosrikoksina (RL 36). Rikollinen ottaa pikavippejä, ostaa tavaraa tai lainaa pankista rahaa väärillä tiedoilla. Tietoja saadaan esimerkiksi varastetun lompakon sisällöstä, murtautumalla netissä oleviin tietokantoihin, pankkiautomaattiin asennettavasta lukulaitteesta tai jopa kohdehenkilön roskia penkomalla. (Henkilöllisyyden luomista koskeva hanke 2010; Poliisi. Identiteettivarkaudet 2013.)

Viime kesänä Sorjosen bändi keikkaili kuopiolaisessa ravintolassa. Keikan päätyttyä Sorjonen huomasi, että joku oli käynyt penkomassa hänen takkiaan. Taskusta oli hävinnyt puhelin ja lompakko. (Yle. Identiteettivarkaus sekoittaa elämän 2012.)

Sorjonen kuoletti välittömästi pankkikorttinsa ja teki poliisille ilmoituksen näpistyksestä. Hän ajatteli kaiken olevan kunnossa. Kuukauden päästä tapahtuneesta hän sai oudon puhelun Kuopion maistraatista. Maistraatin mukaan Sorjonen oli tehnyt väliaikaisen osoitteenmuutoksen Kuopioon. Sorjonen otti yhteyttä poliisin ja kertoi jonkun esiintyvän hänenä. Tapaus ei jäänyt ainoaksi, sillä kesän aikana identiteettivaras esiintyi lukuisia kertoja Sorjosena käyttäen häneltä varastamaansa ajokorttia. (Yle. Identiteettivarkaus sekoittaa elämän 2012.)

Hänen nimissään oli avattu useita puhelinliittymiä, tilattu tietokoneita ja taulutelevisioita, vuokrattu auto jonkun toisen varastetuilla papereilla, mutta käytetty Sorjosen nimissä avattua kännykkäliittymää yhteystietona. Jättimäiset tuhansien eurojen puhelinlaskut tulivat muutaman kuukauden kuluttua tapahtuneesta. Uhrin pitää pystyä todistamaan, että joku muu on laskujen takana. Sorjonen ei joutunut vastuuseen varkaan aiheuttamista laskuista, mutta vaivaa ja aikaa meni paljon asioiden selvittelyyn. (Yle. Identiteettivarkaus sekoittaa elämän 2012.)

2.3 Identiteettivarkauksien määrän lisääntyminen

Identiteettivarkaus on yksi nopeimmin kehittyvistä rikollisuuden muodoista. Erilaiset tietoverkoissa tapahtuvat tietojen kalasteluyritykset, huijaukset ja niiden yritykset sekä identiteettivarkaudet ovat lisääntyneet merkittävästi verkkoaikakauden myötä. Suomen rikoslaissa ei ole vielä kriminalisoitu identiteettivarkautta eli identiteettivarkaus ei sinällään ole rikos. Suomen laki ei kiellä esiintymistä toisena henkilönä. Identiteettivarkaus ei ole nykylainsäädännön mukaan rikos, jos sen avulla ei tehdä mitään rikollista. Mikäli ei tee petosta, niin on laillista esimerkiksi ilmoittaa yritykselle väärät henkilötiedot, mutta väärien henkilötietojen antaminen viranomaiselle on rikos. Lakimuutos on ollut suunnitteilla jo jonkin aikaa, mutta toistaiseksi tietoa sen toteutumisesta ei ole. (Yle uutiset 2012.)

Sosiaalinen media on luonut täysin uudet ulottuvuudet rikolliselle toiminnalle. Tieto netissä altistuu helposti väärinkäytöksille ja identiteettivarkaudet ovat nykypäivää. Identiteettivarkauksien määrää ovat lisänneet merkittävästi tietotekniikan lisääntyminen ja sähköisten palveluiden yleistyminen. (Haasio 2013, 46 - 47.)

Identiteettivarkaus on nimityksenä jollain tapaa harhaanjohtava, sillä toisin kuin varkausrikoksessa (RL 28:1), identiteettivarkaudessa identiteettiä ei oteta yleensä pois rikosuhrin hallusta missään vaiheessa. Rikoksentekijä vain kopioi tiedon myös omaan käyttöönsä. Identiteettitietoa kerätään ja käytetään tyypillisesti identiteettivarkauksissa siten, että teolla tavoitellaan suurta taloudellista rikoshyötyä tai loukataan identiteetin todellisen haltijan perustuslaissa säädettyjä oikeuksia. (Henkilöllisyyden luomista koskeva hanke 2010.)

2.4 Yleisimmät teon tarkoitukset

Identiteettivarkaus on usein kaksivaiheinen prosessi. Joku varastaa ensin tietosi. Sitten varas esiintyy sinuna ja suorittaa varkauden tietojesi avulla. Identiteettivaras hankkii tietoonsa identiteettivarkauden uhrin sosiaaliturvatunnuksen, luottokortin numeron ja osoitteen käyttäen näitä omaksi hyödykseen. Toiselle henkilölle voi tehdä paljon taloudellista vahinkoa jo pelkästään näiden muutamien perustietojen avulla. Verkkokaupassa nämä tiedot riittävät ostosten tekemiseen, ja ne on melko helppo hankkia. Uhrin nimissä onkin usein otettu pikavippejä, tilattu tavaroita, lainattu pankista rahaa sekä avattu puhelinliittymiä. Kiusaamistarkoituksessa tehtävät identiteettivarkaudet lisääntyvät jatkuvasti. Toisen henkilön tiedoilla voidaan tehdä esimerkiksi verkkoyhteisöön profiili ja haukkua muita henkilöitä tai laittaa sinne siveettömiä kuvia nimenomaan kiusaamistarkoituksessa. (Haasio 2013, 46 – 47; Norton. Identiteettivarkauden välttäminen.)

2.5 Identiteettivarkauksiin liittyviä rikosnimikkeitä sosiaalisessa mediassa

Tässä luvussa on käytetty lähteenä Poliisin internetsivuja. (Poliisi. Identiteettivarkaudet 2013.)

Identiteettivarkauden yleisimpiä esiintymismuotoja sosiaalisessa mediassa ovat:

Viestintäsalaisuuden loukkaus: Tämä tulee kyseeseen joka kerta, kun joku käyttää ilman lupaasi sinun profiiliasi, jossa on mahdollista viestiä yksityisesti. Tämä koskee myös sähköposteja ja muita vastaavia palveluja sekä erilaisia pelitilejä. Oleellista on se, onko tekijällä ollut mahdollisuus lukea palvelussa olevia viestejä.

Petos: Luodaan esimerkiksi profiili taloudellisen hyödyn tavoittelemiseksi. Useimmiten nettipetokset eivät tapahdu varsinaisesti sosiaalisessa mediassa, vaan erilaisilla kaupankäyntisivuilla.

Luvaton käyttö: Jos käyttää luvatta toiselle kuuluvaa käyttäjätiliä, kyseeseen voi tulla luvaton käyttö**.**

Laiton uhkaus: Jos uhkaillaan valeprofiililla, niin tällöin kyseeseen voi tulla laiton uhkaus. Näissä tapauksissa asianomistajana on vain uhattu, mutta kyseeseen voi tulla myös kunnianloukkaus sen osalta jonka nimissä esiinnytään.

Yksityiselämää loukkaava tiedon levittäminen voi tulla kyseeseen: Jos toisesta kertoo profiilissa jotain arkaluontoista tietoa. Tämä rikos voi täyttyä myös, jos profiilissa käyttää esimerkiksi loukatun alastonkuvaa. Samalla teolla voi syyllistyä myös kunnianloukkaukseen.

Kunnianloukkaus ei yleensä tule suoraan kyseeseen identiteettivarkauksissa. Poikkeuksena tästä on esimerkiksi seuranhakuilmoitus loukatun tiedoilla.

Tietomurto: Jos murtautuu tai kirjautuu luvatta toisen profiiliin, niin tietomurto täyttyy. Tietomurto väistyy kuitenkin rikosnimikkeenä, jos samalla teolla täyttyy jokin muu rikos ja sen rangaistusmaksimi on vähintään vuosi vankeutta.

Suurin osa identiteettivarkauksista sosiaalisessa mediassa tehdään kiusaamistarkoituksessa. Siihen liittyy erilainen asiaton kommentointi tekaistulla tai kaapatulla profiililla. Kommentointi täyttää yleensä kunnianloukkauksen tunnusmerkistön, ja asianomistajana voi olla se, jolle loukattu teksti on kirjoitettu, mutta myös se, jonka nimissä loukkaus on valheellisesti kirjoitettu.

2.6 Henkilön oikeus omiin tietoihinsa

Toisen henkilön nimissä esiintyminen loukkaa henkilön oikeuksia, vaikkei mielipiteenilmaisusta aiheutuisikaan aineellista vahinkoa. Aiemmin tällaisen teon kriminalisointiin ei ole nähty tarvetta, mutta tietoverkko on muuttanut tilannetta. Toisen nimissä tietoverkkoon laitetut mielipiteet ovat näkyvillä käytännössä ikuisesti. Näiden virheellisten tietojen korjaaminen voi olla mahdotonta, joten nyt on alettu pohtia kriminalisoinnin tarpeellisuutta. (Henkilöllisyyden luomista koskeva hanke 2010.)

Tietoverkkoympäristössä henkilöllä ei aina ole mahdollisuutta hallita omaa henkilöllisyyttään tai omia tietojaan, vaikka jokaisella yksityishenkilöllä on oikeus omiin tietoihinsa. Käytännössä tämä tarkoittaa sitä, että jokaisella yksityishenkilöllä on oikeus hallita omia henkilötietojaan ja päättää niiden käsittelystä. Identiteettivarkaus tapahtuu esimerkiksi silloin, kun Facebookiin luodaan profiili toisen henkilön nimellä, kuvalla ja tiedoilla. Tämän tekaistun profiilin turvin voidaan syyllistyä esimerkiksi herjauksiin tai kunnianloukkauksiin. Toimintaympäristönä verkkoympäristö on erilainen kuin reaalimaailmassa ja tekijöiden saaminen vastuuseen on hankalampaa, lisäksi verkkoympäristössä tapahtuvan identiteettivarkauden seuraukset voivat olla hyvinkin vakavia yksilö tasolla. Tietoverkkojen käyttämiseen liittyviä riskejä voi olla myös vaikea havaita. Yhä useammin ihmisiltä esimerkiksi kysellään tietoverkoissa heidän identiteettinsä kannalta keskeisiä tietoja, eivätkä kaikki suhtaudu kyselyihin riittävän varauksellisesti. (Kuluttajavirasto 2011.)

2.7 Identiteettivarkauden monet muodot

Identiteettivarkauksiin liittyy toisinaan ison mittakaavan tietomurto ja toisinaan takana on vain kavala hyökkäys yksittäistä henkilöä kohtaan. Identiteettivarkauden uhrin nimissä tehdään usein erilaisia liittymäsopimuksia. Tällöin uhrille voi tulla maksukehotuksia ostoksista, joita hän ei itse ole tehnyt. Toisinaan onkin todella lähellä, että uhri joutuu maksuhäiriö listalle, jolloin luottotiedot menevät. Tällaisesta jää pysyvä jälki luottohistoriaan. (Tranberg & Heuer 2013, 95 - 97.)

Aineellisten menetysten lisäksi tulevat vahingot siitä, että koko oma identiteetti ja yksityiset asiat paljastuvat. Uhria pelottaa usein vuosia identiteettivarkauden jälkeenkin ajatus siitä, että roistot palaavat. Asianomainen huomaa harvoin, ilmestyykö omaa elämää koskevia tietoja jossakin julkisuuteen. Kaapatut tilit on kuitenkin helpompi tunnistaa, esimerkiksi silloin, jos joku alkaa käyttää Facebook- tai Yahoo-tiliäsi. Vastatoimiksi on vaihdettava salasanat, hankittava uudet pankki- tai luottokortit sekä seurattava tarkasti, tuleeko luvattomia tiliveloituksia tai näkyykö outoja sähköpostiviestejä. (Tranberg & Heuer 2013, 95 - 97.)

2.8 Tilastotietoa

Poliisin tilastointi Suomessa perustuu lähtökohtaisesti rikosnimikkeisiin. Identiteettivarkauksilla aiheutetusta vahingosta ei ole saatavilla yhteismitallista tilastotietoa, koska identiteettivarkauden kuvaavaa rikosnimikettä ei ole. (Henkilöllisyyden luomista koskeva hanke 2010.)

Identiteettivarkauksiin liittyvät tapaukset olisi seulottava käsin koko rikosilmoitusmassasta. Tehtävä olisi varsin mittava, koska identiteettivarkaudella on useita eri ilmenemismuotoja ja tekotapoja. (Henkilöllisyyden luomista koskeva hanke 2010.)

2.9 Identiteettivarkaus sosiaalisessa mediassa

Digitaalisen median ja uuden teknologia myötä on tullut uusia ongelmia, yksi näistä ongelmista on identiteettivarkaus sosiaalisessa mediassa. Verkkorikollisuus on internetin mahdollistaman tiedon vapaan saatavuuden sekä mielipiteen vapauden kääntöpuoli. Verkossa voi tehdä lainvastaisia tekoja, kuten tosimaailmassakin. Kiinnijäämisen riski on verkkorikollisuudessa huomattavasti pienempi kuin reaalimaailmassa. Varkaat ja huijarit liikkuvat siellä missä laajat kansanjoukot viettävät aikaansa. (Tranberg & Heuer 2013, 94.)

Verkossa mikään ei ole täysin turvassa**,** ei henkilötunnus, tilinumero, luottokorttitiedot, ei edes sähköposti, ellei käytetä salattua yhteyttä. Ilmaiset sähköpostipalvelut käyvät postilaatikollasi nuuskimassa ilmaisuja ja avainsanoja, joiden perusteella mainontaa voi kohdistaa. Sanomattakin on selvää, että avointen sosiaalisten verkkojen välityksellä, kuten esimerkiksi Facebookissa, tapahtuva viestintä on vielä vähemmän turvassa. Facebookin kaltaiset suositut sosiaalisen median palvelut ovatkin muodostuneet rikollisten suosimiksi paikoiksi. (Haasio 2013, 13; Tranberg & Heuer 2013, 101.)

Useat tärkeitä tietoja käsittelevät yritykset, kuten pankit, välitysliikkeet, puhelinyhtiöt ja kaapeliyritykset käyttävät henkilötunnusta yhtenä ja joskus jopa ainoana tietona, jolla henkilöllisyys varmennetaan. Omia henkilötietoja ei kannata tarpeettomasti luovuttaa verkossa. On todella harmillista joutua tilanteeseen, missä joku yrittää pilata maineesi verkossa ja joudut kamppailemaan asian korjaamiseksi ja väärien tietojen poistamiseksi. (Tranberg & Heuer 2013, 94 - 95.)

2.10 Tietoa voidaan klassisesti huijata käyttäjältä

Tiedonhankintamenetelmää kutsutaan phishingiksi. Peitetarinalla, joka kuulostaa järkevältä, kysytään suoraan käyttäjältä tietoa. Rikoksentekijä väärentää esimerkiksi sähköpostiviestin verkkokaupan nimissä, jossa pyytää asiakasrekisteriongelman vuoksi käyttäjää päivittämään asiakastietonsa www-lomakkeella. Lomake tallettaa tiedot rikoksentekijän hallussa olevaan tietovarastoon. Yleensä tällainen teko täyttää petoksen (RL 36:1) tunnusmerkistön. Rikolliset ovat kehit-

täneet tietoteknisiä menetelmiä kaapata tietoja myös asiakaspäästä, koska suuri osa käyttäjistä ei enää usko huijaussähköposteihin. (Henkilöllisyyden luomista koskeva hanke 2010.)

Käyttäjä voidaan myös ohjata virheelliseen osoitteeseen puuttumalla tietoteknisin keinoin haavoittuvan työaseman liikenteenohjaukseen. Rikolliset murtautuvat käyttäjän työasemalle ja muuttavat nimipalveluasetuksia siten, että käyttäjän avatessa yhteyden verkkokauppaan yhteys kirjautuukin palveluun, joka on rikollisen hallussa. Näin rikollinen saa kerättyä käyttäjän verkkokauppaan antamat kirjautumistunnukset. Käyttäjän koneelle syötetään päivittämättömän www-selaimen, sähköpostiohjelman tai jonkin edellisten käyttämien apuohjelmien haavoittuvuutta hyväksikäyttäen haittaohjelma. Haittaohjelma voi kerätä www-lomakkeiden näppäinpainalluksia. Näin rikoksentekijä voi saada haltuunsa luottokorttinumeron tarkistetietoineen, jos käyttäjä maksaa sillä esimerkiksi ostoksiaan verkkokaupassa. (Henkilöllisyyden luomista koskeva hanke 2010.)

2.11 Tietoverkoissa toteutettavat identiteettivarkaudet

Identiteettitiedon väärinkäyttöä on olennaisesti muuttanut tietoverkko. Verkkoympäristössä kokonaisten henkilöhistorioiden kopioiminen on mahdollista suhteellisen nopealla työllä. Tieto monistuu ja leviää huomattavasti nopeammin verkkoympäristössä kuin reaalimaailmassa. Tietoverkossa toteutetussa rikollisuudessa ominaispiirteenä on suuri hyötypotentiaali suhteessa pieniin toteutuskustannuksiin sekä kiinnijäännin riskiin. Siinä, missä identiteettivarkaudet reaalimaailmassa ovat usein yksittäistapauksia, niin verkossa toiminnan voi automatisoida. Rikoksentekijät pystyvät käsittelemään kohtuullisen pienin kustannuksin suuria määriä oikeudetta hankittuja identiteettejä. (Henkilöllisyyden luomista koskeva hanke 2010; Oikeusministeriö 2013.)

Teot, jotka tähtäävät huomattavan taloudellisen hyödyn tavoitteluun tai henkilön vakavaan vahingoittamiseen, ovat poikkeuksetta hyvin suunnitelmallisia. Verkossa kiinnijäännin riski on reaalimaailmaa huomattavasti pienempi, koska rikokset tehdään jälkien peittämiseksi sivullisilta rikollisten haltuun kaapatuista verkkoliittymistä, jolloin tutkintatoimet kohdistuvat aina ensin sivulliseen. Rikoksentekijän näkökulmasta verkko on täysin globaali. Suojattuihin henkilötietoihin

kohdistuvat identiteettivarkaudet tapahtuvat lähes aina tietoverkoissa. (Henkilöllisyyden luomista koskeva hanke 2010; Oikeusministeriö 2013.)

3 Identiteettivarkauden monet syyt

Taloudellista hyötyä tavoittelevan identiteettirikollisuuden tarkoituksena on saada mahdollisimman suuri rikoshyöty. Verkon identiteettirikoksissa ansaintalogiikka perustuu tietomassan suureen kokoon. Identiteettivarkauksia tehdään myös kiusanteon tai pilailun takia. (Henkilöllisyyden luomista koskeva hanke 2010.)

3.1 Taloudellista hyötyä tietoverkoissa tavoitteleva identiteettirikollisuus

Taloudellista hyötyä tietoverkoissa tavoittelevan identiteettirikollisuuden kohteena ovat tyypillisesti maksuvälinetunnisteet, kuten esimerkiksi verkkopalveluiden asiointitunnukset, luottokorttinumerot sekä sähköpostiosoitteet. (Henkilöllisyyden luomista koskeva hanke 2010.)

Rikolliset keräävät entistä enemmän kuitenkin myös henkilötietoja, kuten henkilötunnuksia, henkilöiden nimiä, katuosoitetietoja ja työnantajatietoja. Rikoshyötyä pyritään hankkimaan kaappaamalla rikoksen uhreilta mitä tahansa automatisoidusti kerättävissä olevaa identiteettitietoa mikä on helposti rahaksi muutettavaa. (Henkilöllisyyden luomista koskeva hanke 2010.)

3.2 Ansaintalogiikka perustuu

Ansaintalogiikka perustuu ennen kaikkea tietomassan valtavaan kokoon verkon identiteettirikoksissa. Yksittäinen luottokorttinumero ei ole vielä kovin arvokas, mutta suuri määrä luottokorttinumeroita muodostaa jo hyvinkin merkittävän resurssin. Resurssia käytetään helposti jälleenmyytävän omaisuuden hankkimiseen verkkokaupoista, esimerkkinä kallis elektroniikka. Ensisijaisesti rikollinen pyrkii iskemään sinne, missä tieto on helpoiten saatavilla. Kyse on massailmiöstä eli ansaintalogiikka ei näin ollen perustu ensisijaisesti jonkin todella arvokkaan yksittäisen tiedon kaappaamiseen. (Henkilöllisyyden luomista koskeva hanke 2010.)

3.3 Ilman taloudellisen hyödyn tavoittelua tehtävät identiteettivarkaudet

Henkilötietojen väärinkäyttö, joka tehdään ainoastaan kiusanteon tai pilailun takia, on muodostunut ongelmaksi. Rikosoikeudellisin keinoin on katsottu vain rajoitetusti olevan tarvetta puuttua toisen henkilötietojen käyttöön sellaisenaan, ilman taloudellisen hyödyn tarkoitusta tai vahingoittamistarkoitusta. (Henkilöllisyyden luomista koskeva hanke 2010.)

Vaikka identiteettitiedon käyttäjän tavoitteena ei ole loukata yksittäistä nimettyä kohdetta, eikä tekijä välttämättä lainkaan ymmärrä tekoa tehdessään tekonsa vaikutusta, niin silti tietoverkossa voi syntyä suurta vahinkoa. Esimerkiksi oikeuskäytännön perusteella henkilörekisteririkos ei ilmeisesti täyty, jos tietoja kerätään ilman tarkoitusta loukata rekisteröidyn yksityisyyttä. (Henkilöllisyyden luomista koskeva hanke 2010.)

3.4 Identiteettirikollisuus, jonka tavoitteena on vahingoittaa kohdetta

Identiteettivarkaudet voivat ilmetä verkossa myös sellaisina koulu- ja työpaikkakiusaamisina, joissa ei tavoitella taloudellista hyötyä. Ongelmana ovat kiusaamistarkoituksessa tehdyt teot, toisena esiintyen kirjoitetut tekstit verkkoon/profiiliin. Tällöin kiusaajan tavoitteena on vahingoittaa jotakin lähipiirin henkilöä, kuten entistä puolisoa, koulukaveria, opettajaa, taikka jotakin julkisen vallan käyttäjää. Identiteettivarkaus kohdistuu nykyään useasti myös julkisuuden henkilöihin, esimerkiksi sosiaalisessa mediassa esiinnytään julkisuuden henkilönä. (Oikeusministeriö 2013.)

Tämä kiusaamisen uusi muoto voi saada kohtuuttomia mittasuhteita uudessa toimintaympäristössä, jossa tiedon jakaminen on todella helppoa. Kunniaa tai yksityisyyttä loukkaava tieto voidaan saada tietoverkossa leviämään paljon reaalimaailmaa suuremmalle joukolle. Tieto voi myös olla hyvin vaikeaa poistaa verkosta sen päästyä kerran leviämään riittävän laajalle. Tämän takia teon vaikutukset voivat seurata rikoksen asianomistajaa kohtuuttoman kauan.
Tietoverkossa tapahtuva kiusanteko saattaa täyttää esimerkiksi kunnianloukkauksen (RL 24:9) tai yksityiselämää loukkaava tiedon levittäminen (RL 24:8) tunnusmerkistön. (Haasio 2013, 47; Oikeusministeriö 2013.)

3.5 Suurin epäkohta

Ilman varsinaista vahingoittamistarkoitusta on viime aikoina esille tullut verkon yhteisömedioihin rekisteröityminen jonkun muun, esimerkiksi julkisuudenhenkilön tai oman opettajan nimellä. Tekijä ei välttämättä lainkaan ymmärrä sitä, että teosta saattaisi koitua uhrille haittaa tai mielipahaa. Kysymyksessä on kasvava ilmiö. (Henkilöllisyyden luomista koskeva hanke 2010.)

Tämä uudenlainen tekomuoto saattaa aiheuttaa kuitenkin huomattavaa haittaa, vaikka tekijä ei tekisi tekoa vahingoittamistarkoituksessa. Näissä tapauksissa ei voida havaita selvää konkreettista hyötytarkoitusta eikä teon ensisijaisena tavoitteena ole aiheuttaa varsinaista vahinkoa tietylle henkilölle, joka on teon kohteena. (Henkilöllisyyden luomista koskeva hanke 2010.)

Nimen todellisella haltijalla ei ole mahdollisuutta saada nimenhaltijan nimissä esitettyä sisältöä verkosta pois, ja harvoin saadaan selville, kuka teon takana on, kun teko tehdään ilman, että kunnianloukkaus (RL 24:8) tai yksityiselämää loukkaava tiedon levittäminen (RL 24:8) täyttyy identiteetin käyttäjän osalta. (Henkilöllisyyden luomista koskeva hanke 2010.)

3.5.1 Esimerkkitapaus

Oppilas on ajattelemattomuuttaan tehnyt opettajansa nimissä profiilin ilman tarkoitusta vahingoittaa sen enempää ja ymmärtämättä teon seurauksia. Jos nimen todellisen haltijan ystäväpiiri erehtyy pitämään identiteetin käyttäjää nimen todellisena haltijana, niin identiteetin käyttäjä voi saada tietoonsa nimen haltijan tai tämän lähipiirin yksityisyyden piirin kuuluvaa tietoa. Kohdehenkilön yksityisyys kiistatta vaarantuu. Nimen todellinen haltijan saattaa tuntea tällä tavoin haittaa, mutta esitutkintaviranomaisella ei ole toimivaltuutta käynnistää esitutkintaa tapahtuman selvittämiseksi, koska mikään rikostunnusmerkistö ei täyty. (Henkilöllisyyden luomista koskeva hanke 2010.)

3.5.2 Esimerkki identiteettitiedon oikeudettomasta käytöstä

Henkilö täytti toisen puolesta netissä olevan kirkosta eroamisilmoituksen. Maistraateissakin muutama eroamisilmoitus meni läpi. Teko onnistuu, kunhan tietää erotettavan nimen, kotiosoitteen ja henkilötunnuksen. Sähköpostilla onnistuu myös toisen erottaminen, mikäli maistraatissa ei osata epäillä osoitetta vääräksi. Kuka tahansa voi hankkia ilmaisen sähköpostiosoitteen kenen nimellä tahansa. Eroaminen kirkosta onnistuu myös Vapaa-ajattelijaliiton sähköistä kirkosta eroamislomaketta käyttämällä. Toki eroamisen voi mitätöidä, ja maistraatista lähtee aina vahvistuskirje sähköisesti kirkosta eronneelle. Teosta aiheutuu vaivaa kohteelle ja teko loukkaa henkilön oikeutta päättää tietojensa käytöstä. Perustuslain 10 §:n mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu, mutta tällaisissa tilanteissa mikään rikoslain tunnusmerkistö ei tarjoa teon uhrille suojaa. (Henkilöllisyyden luomista koskeva hanke 2010.)

4 Voit suojautua identiteettivarkaudelta huolellisuudella

Identiteettivarkaudelta voi suojautua omalla huolellisuudella. Verkkorikolliset pyrkivät varastamaan henkilökohtaisia tietoja monin eri tavoin. Kannattaa suhtautua aina varauksellisesti viesteihin tai sivustoihin, jotka pyytävät henkilökohtaisia tietojasi. Hoida raha-asioita vain turvallisilla verkkosivuilla ja tarkasta luottotiedot säännöllisesti epätavallisten tapahtumien varalta. (Google. Turvassa pysyminen verkossa.)

4.1 Ole tarkka, mitä tietoa annat itsestäsi verkossa

Täysin vaarattomalta tuntuvan informaation, kuten syntymäajan, kotiosoitteen tai puhelinnumeron avulla taitava nettisurffaaja voi kerätä tietoja eri reittien varrelta. Ne saattavat aiheuttaa suurta tuhoa vääriin käsiin joutuessaan. Tällöin voi maineensa lisäksi menettää myös rahansa. Suuri osa petoksista on siirtynyt verkkoon, sillä siellä on luontevaa esiintyä anonyyminä. (Anna 2013.)

Sähköpostien salasanoja sekä verkkopankkitunnuksia on täysin sallittua urkkia. Toiminta muuttuu rikolliseksi vasta, kun tiedoilla hankitaan taloudellista hyötyä. Pikavippejä ja puhelinliittymiä oli melko helppo ottaa toisen nimiin vielä jokin aika sitten. Kuluttajansuojalakia tiukennettiin kuitenkin vuonna 2011. Tällä hetkellä luotonantajaa velvoitetaan tarkistamaan entistä huolellisemmin hakijan henkilöllisyys. (Anna 2013.)

4.2 Ole huolellinen

Verkkorikolliset pyrkivät varastamaan henkilökohtaisia tietoja ja rahaa monin eri tavoin. Murtovarkaille ei kannata ojentaa kotiavaimia, joten myös verkossa kannattaa olla varuillaan. Yksinkertaisille vinkeillä voi suojautua identiteettivarkaudelta. Kannattaa suhtautua aina varauksellisesti viesteihin tai sivustoihin, jotka pyytävät henkilökohtaisia tietojasi tai viesteihin, joissa sinut yritetään ohjata tuntemattomalle sivulle antamaan jokin seuraavista: käyttäjänimet, salasanat, syntymäpäivä, henkilötunnus, pankkitilien numerot, PIN-koodit, luottokorttien koko numerot. (Google. Turvassa pysyminen verkossa.)

On myös oltava varuillaan mikäli saa sähköpostia, jossa kysytään henkilökohtaisia tietoja. Oikeat yritykset eivät koskaan kysy henkilökohtaisia tietoja sähköpostilla, vaikka lähettäjäksi olisi merkitty pankki, yritys tai viranomaisorganisaatio. (Tranberg & Heuer 2013, 101.)

Kuluttajaa yritetään jymäyttää verkossa monin eri tavoin. Yleinen keino on sähköpostiviesti arpajaisvoitosta, jonka voi lunastaa lähettämällä tilinumeronsa. Kannattaa muistaa, että jos uutinen vaikuttaa liian hyvältä ollakseen totta, kyseessä on todennäköisesti huijaus. (Anna 2013.)

Jos päädyt epäilyttävän viestin kautta sivuille, joissa pyydetään täyttämään lomakkeelle henkilökohtaisia tietoja, älä kirjoita siihen mitään. Koska jos edes kirjoitat tietoja lomakkeelle, saatat lähettää tietoja identiteettivarkaille, vaikket painaisi lähetä. Salasanaa ei myöskään kannata kirjoittaa sivustossa, johon päätyy epäilyttävän sähköposti- tai muun viestin kautta. Luotettavat palvelut ja sivustot eivät pyydä salasanaa sähköpostilla, joten kannattaa jättää vastaamat-

ta viesteihin, joissa pyydetään antamaan verkkopalveluiden salasanoja. (Google. Turvassa pysyminen verkossa.)

Jos joku on saanut haltuunsa sähköpostisi salasanan, hän voi lukea henkilökohtaisia viestejäsi ja yrittää päästä muihin käyttämiisi verkkopalveluihin, esimerkiksi verkkopankkiin tai sosiaalisen median palveluihin sähköpostitilisi kautta. Henkilö voi esiintyä sosiaalisessa mediassa sinuna tilisi avulla. Koska salasanat ovat niin tärkeitä, kannattaa harkita tarkkaan, ennen kuin niitä luovuttaa muille, koska tilien väärinkäytön riski kasvaa aina mitä enemmän salasanoja jakaa eteenpäin. (Google. Turvassa pysyminen verkossa.)

4.3 Voit vaikuttaa omalla toiminnallasi huijausten ehkäisyyn

Käyttäjä voi vaikuttaa omalla toiminnallaan, erilaisten huijausten onnistumiseen. Internetissä ja sähköpostissa kysellään yhä useammin kuluttajilta heidän identiteettinsä kannalta keskeisiä tietoja. (Henkilöllisyyden luomista koskeva hanke 2010.)

Kuluttajavirasto, tietosuojavaltuutetun toimisto ja viestintävirasto ovat monesti tiedottaneet, että kaikkiin tunnistetietojen pyyntöihin on syytä suhtautua varauksellisesti. Tietoja ei pidä paljastaa tuntemattomille tahoille, ellei voi olla varma niiden turvallisesta käsittelystä. Tunnistetietoja tulee säilyttää yhtä huolellisesti kuin käteistä rahaa, pankkikorttia ja luottokorttia. (Henkilöllisyyden luomista koskeva hanke 2010.)

4.4 Tietoverkossa toteutettujen identiteettivarkauksien ennaltaehkäisy

Taloudellista hyötyä tavoittelevan ammattimaisesti toteutetun tietoverkossa tapahtuvan identiteettirikollisuuden tekee poikkeuksellisen kannattavaksi sen toteuttamisen kustannustehokkuus sekä pieni kiinnijäännin riski. Eräs rikostorjunnan keino tulee lähitulevaisuudessakin olemaan rikosten liiketoimintamallin tunnistaminen ja toteuttamisen vaikeuttaminen, koska viranomaisten toimivaltuudet eivät aina kaikilta osin tue rikosten menestyksellistä tutkintaa. (Henkilöllisyyden luomista koskeva hanke 2010.)

Parantamalla olennaisesti yleistä tietoturvatilannetta, mihin tarvitaan lukuisten yksityisten ja julkishallinnon toimijoiden yhteistyötä, ennaltaehkäistään tietoverkossa tapahtuvaa identiteettirikollisuutta. Taloudellista hyötyä tavoittelevien identiteettirikosten uhka tuskin tulevaisuudessa kohdistuu ensisijaisesti palveluntarjoajiin, vaan se kohdistuu asiakkaisiin, joiden käyttämien laitteiden tietoturvallisuus on lähes kokonaan palveluiden tarjoajien ulottumattomissa. Suomessa tietoturvallisuus on huomioitu suunnittelussa, ja henkilötietojen käsittelyä säätelevää lainsäädäntöä on systemaattisesti jalkautettu palveluiden tarjoajien helposti ymmärtämään muotoon. (Henkilöllisyyden luomista koskeva hanke 2010.)

4.5 Suojaa tietosi

Identiteettivarkaus verkossa on kasvava ja vaikea ongelma. Varkaat esiintyvät aitoina organisaatioina käyttäen valesähköpostiosoitteita ja -verkkosivustoja. Varkaat huiputtavat luovuttamaan henkilökohtaisia tietoja, kuten salasanoja ja tilinumeroita ja käyttävät hyväkseen luottamusta. Hakkerit ja virukset voivat samalla tavalla tunkeutua tietokoneeseen ja asentaa näppäilyntallennusohjelmia, jotka varastavat tietoja tai sieppaavat salasanoja ja nimiä samalla, kun niitä näppäilee. Ennakoimalla voi kuitenkin estää identiteettivarkautta hyvin. Tunnista vilpilliset verkkosivustot, sähköpostiviestit ja muut hälytysmerkit, jotka liittyvät tietojenkalasteluun. Hoida raha-asioita vain turvallisilla verkkosivuilla. Virustentorjuntaohjelmisto, henkilökohtainen palomuuri, vakoiluohjelmien torjuntaohjelmisto sekä roskapostisuojaus on hyvä asentaa oman henkilökohtaisen turvallisuuden vuoksi. (Norton. Identiteettivarkauden välttäminen.)

Nuoret kuluttajat ovat tietoverkkojen käyttäjinä kohtuullisen valistuneita. Vanhempiin ikäryhmiin kuuluvat kuluttajat, jotka ovat tottumattomampia käyttämään tietoverkkoja ja sähköisiä palveluita, eivät aina osaa varoa tietoverkoissa eteen tulevia houkuttelevan tuntuisia sivustoja, jotka todellisuudessa ovatkin jotain muuta, kuin miltä ne ensi silmäyksellä vaikuttavat. (Kuluttajavirasto 2011.)

4.6 Seuraa tilitapahtumiasi

On hyvin tärkeää valvoa tilejään ja luottotietojaan, koska identiteettivarkauden uhriksi joutuminen saattaa paljastua vasta kuukausien kuluttua. Tänä aikana varkaat saattavat ryöstellä tilejä ja velkaannuttaa sinut korviasi myöten. Se, että olet ollut varovainen omien tietojesi kanssa, ei merkitse sitä, etteikö joku pystyisi murtautumaan työnantajasi tai pankkisi tietokoneisiin. Joihinkin asioihin et pysty vaikuttamaan, vaikka itse pystytkin tekemään paljon identiteettisi suojaamiseksi. (Norton. Identiteettivarkauden välttäminen.)

4.7 Mitä voit itse tehdä

Nettipoliisina työskentelevä vanhempi konstaapeli Jutta Antikainen korostaa yksilön vastuuta identiteettivarkauksien torjunnassa. Suurin haaste tässä on se, että ihmiset osaisivat käyttää sosiaalista mediaa oikein. Kannattaa tarkastaa luottotiedot säännöllisesti epätavallisten tapahtumien varalta. Valvo jatkuvasti tiliesi – pankki-, sijoitus- ja luottokorttitilien – tapahtumia. Selvitä asia välittömästi, jos huomaat jotain odottamatonta tai outoa, kuten esimerkiksi sinulle tuntemattoman uuden luottorajan. Rahayritykset tarjoavat useasti tapahtumahälytyksiä, ne on hyvä ottaa käyttöön. On syytä reagoida välittömästi, jos saat hälytyksen tai rahalaitos ilmoittaa epätavallisesta toiminnasta. (Norton. Identiteettivarkauden välttäminen; Yle Poliisi-TV 2013)

Voit minimoida vahingot toimimalla nopeasti, jos huomaat, että joku on varastanut tietosi. Seuraavat ohjeet auttavat sinua vahinkojen minimoinnissa: Sulje tilit, jotka saattavat olla vaarassa. Ilmoita rikoksesta viranomaisille. Lisää luottotietoihisi petoshälytys ja valvo tietoja tarkasti seuraavien vuosien ajan. (Norton. Identiteettivarkauden välttäminen.)

4.7.1 Omatieto-palvelu

Identiteettivarkauksilta suojautuminen on vaikeaa. Omatieto-palvelulla voit seurata omia tietojasi. Saat ilmoituksen, jos joku toinen yrittää tehdä sopimuksia tai hakea lainaa nimissäsi. Palveluun sisältyy myös hälytyspalvelu, joka ilmoittaa luottotietojen muutoksista automaattisesti. Omatieto-palvelu sisältää luottotietoraporttisi sekä tietovahdit henkilötietojen suojaksi. Tietovahti kertoo sinulle, jos luottotietojasi käytetään sekä näet, kuka tietojasi kysyi ja miksi. (Suomen Asiakastieto Oy 2013.)

4.7.2 Oma luottokieltopalvelu

Jos epäilet henkilötietojesi väärinkäyttöä, kannattaa sinun asettaa lisäksi oma luottokielto –merkintä. Tämän asettamisella vaikeutetaan merkittävästi identiteettivarkauden riskiä ja vähennetään tietojesi väärinkäytön mahdollisuutta, koska luotollista sopimusta tehtäessä luotonmyöntäjä näkee merkinnän ja kysyy aina oma luottokielto -todistusta. Todistus vaikeuttaa huomattavasti rikollista luotonhakua. (Suomen Asiakastieto Oy 2013.)

4.8 Epäkohdat identiteettivarkauden selvittämisessä

Yhteiskunnan tulisi suojella henkilöitä identiteettivarkauksilta tai ainakin niiden vaikutuksilta. Voidaan tehostaa ennaltaehkäisyä ja toipumista, mutta on hyvä miettiä myös, ovatko rikosoikeudelliset keinot ajan tasalla maailman muuttuessa. Tuomioistuimen päättämää televalvontaa voidaan käyttää vasta, kun tietoverkossa kerättyä identiteettitietoa on käytetty väärin. Keräämisestä syntynyt tietotekninen jälki ei kuitenkaan ole enää jäljellä siinä vaiheessa. Tällaisiin epäkohtiin tulisi kiinnittää huomiota. (Henkilöllisyyden luomista koskeva hanke 2010.)

Henkilökorttien ja passien varastamisen jälkeiseen väärinkäyttöön fyysisessä tunnistamistilanteessa ei auta kuin niiden haltuun saaminen tekijältä. Ajokorttia ei voi mitenkään sulkea, eli jos ajokortti varastetaan, niin tekoketjua ei saada välttämättä loppumaan edes tekijän kiinnijäämiseen, ennen kuin itse kortti saadaan tekijän hallusta pois. (Henkilöllisyyden luomista koskeva hanke 2010.)

4.9 Lainsäädännön ajantasaisuus

Lainsäädännön olisi pysyttävä ajan tasalla, silloin kun ympäristö olennaisesti muuttuu. Verkkoympäristö on kansalaisille hankala ja riskien tunnistaminen on vaikeaa. Kyse on myös kansainvälisestä toimintaympäristöstä, siksi kenelläkään ei ole täydellistä kontrollia verkkoympäristöön. Rikosoikeutta ja pakkokeinoja on aina pidettävä viimesijaisina keinoina ongelman ratkaisuun, siksi myös kevyempiä vaihtoehtoja on syytä aina harkita, vaikka verkkoympäristö onkin tässä suhteessa erityisen haasteellinen. (Henkilöllisyyden luomista koskeva hanke 2010.)

4.10 Identiteettivarkauden kohteeksi joutuminen

Identiteettivarkauden kohteeksi joutuminen sekoittaa elämän. Joku on tullut yksityisimmälle alueellesi ja penkonut kaiken, mitä sinulla on. Tämä voisi olla verrattavissa esimerkiksi siihen, että joku murtautuu kotiisi. Aivan kuten reaalimaailmassakin, niin on tehtävä inventaari ja koetettava selvittää, mitä on kadonnut. Tietysti tiedostojen ja digitaalisen informaation tapauksessa ei ole juurikaan mahdollista tietää, mitä kaikkia yksityiselämän asioita on lähtenyt varkaan mukaan. Kopiota jaetaan verkossa ja siellä ne liikkuvat. (Tranberg & Heuer 2013, 96.)

5 Lainsäädäntö tällä hetkellä

Eriasteiset identiteettivarkaudet ovat huolestuttava ilmiö tämän päivän verkkomaailmassa. Tärkeintä on miettiä, miten kansalaista voidaan suojella identiteettivarauksilta. Identiteettivarkauksia koskeva lainsäädäntö on saatettava ajan tasalle. (Digitoday 2011; Uusi Suomi. Identiteettivarkaudet saatava kuriin 2011.)

5.1 Identiteettivarkauksien lainsäädäntö tällä hetkellä

Lainsäädäntö ei tällä hetkellä anna poliisille riittäviä toimivaltuuksia selvittää identiteettivarkauksiin liittyviä rikoksia, ei välttämättä edes isojakaan tietomurtoja. Tilanne käy sen vuoksi käsittämättömäksi, sillä verkossa tapahtuviin väärinkäytöksiin tai oikeudenloukkauksiin ei voida puuttua, koska teolle ei ole selvää rikosnimikettä. Henkilötietojensa jakamisesta verkossa yksittäisen kansa-

laisen oma vastuu on varsin suuri. Yleistä tietoisuutta verkkohenkilöllisyyden ja verkossa asioinnin riskeistä täytyy lisätä tämän vuoksi. (Digitoday 2011; Uusi Suomi. Identiteettivarkaudet saatava kuriin 2011.)

5.2 Hallituksen valmistelut

Sisäasiainministeri Päivi Räsänen sanoo, että identiteettivarkauksiin liittyvää lainsäädäntöä ollaan kiristämässä. Räsäsen on itsekin joutunut valeprofiilien kohteeksi ja kertoo valeprofiilin aiheuttavan syvää kiusaa ihmiselle, vaikka rikoksen tunnusmerkit eivät täyttyisi. Identiteettivarkauksien torjuntaan on tulossa lisätoimia. Jo edellisellä hallituskaudella sisäasiainministeriö esitti identiteettivarkauksien kriminalisointia, mutta oikeusministeriön mukaan se onnistuisi vain rajallisesti. Parhaillaan hallitus valmistelee uusia toimia identiteettivarkauksien ja tietoverkkorikollisuuden estämiseksi. (Taloussanomat 2013.)

5.3 Mahdollinen lainsäädäntömuutostarve

Selvitettäessä mahdollista lainsäädäntömuutostarvetta täytyy huomiota kiinnittää siihen, että identiteettivarkauden määritelmää tulee selventää ja täsmentää. Verkkoympäristössä muuttuneet teko-olosuhteet tulee ottaa huomioon kriminalisointitarpeen arvioinnissa. Suomen tuomariliiton mukaan täytyy selvittää, miten voimassaolevat kriminalisoinnit kattavat nimenomaan oikeudettoman identiteettitietojen keräämisen ja käyttämisen. Tietoverkko mahdollistaa identiteettitietojen väärinkäytön eri mittakaavassa kuin reaalinen ympäristö. Seurauksena voi olla pitkäkestoinen ja laaja rikoskokonaisuus, ja vahingot yksilötasolla saattavat olla kohtuuttoman suuret. Suomen Asianajajaliiton mukaan lainsäädännön kehittämisessä tulee edetä EU jäsenmaiden kesken tiiviissä yhteydessä. (Asianajajaliitto. Tiedotteita ja lausuntoja 2013, Oikeusministeriö 2013.)

5.4 Kriminalisoinnin hankaluus

Toisen nimissä esiintymisen kriminalisointi on monimutkaista. Juridisesti epäselvä nykytila ei kuitenkaan ole vaihtoehto, sillä poliisille tulee usein rikoksia, joihin sillä ei ole toimivaltaa. (Helsingin Sanomat. Identiteettivarkaus.)

On pohdittu jo vuosia identiteettivarkauden kriminalisointia. Toisena henkilönä esiintyminen on jo yleensä rangaistavaa jonain muuna rikoksena, esimerkiksi väärennyksenä, petoksena tai kunnianloukkauksena, tämä on lisännyt kriminalisoinnin varovaisuutta. Tällä hetkellä henkilöllisyyden valehteleminen on jo rangaistavaa, jos tarkoituksena on erehdyttää tällä toiminnalla viranomaista. Yksityishenkilöiden välisissä suhteissa väärän nimen käyttäminen pelkästään ei ole rikos. (Helsingin sanomat. Väärän nimen käyttäminen voi tulla rangaistavaksi.)

5.5 Kriminalisointi tällä hetkellä

Tekotavan mukaan identiteettitiedon keräämistä verkossa ei ole joko lainkaan kriminalisoitu tai se on kriminalisoitu tavalla, joka ei mahdollista menestyksellistä esitutkintaa tietoverkossa, sillä alkuperäistä epäillyn jäljille johtavaa identiteettitiedon keräämisestä syntynyttä tietoteknistä jälkeä ei yleensä enää ole olemassa kerätyn identiteettitiedon oikeudettoman käytön aikana. Yksityishenkilölle ja viranomaiselle esiintyminen tulisi kriminalisoida samantasoisesti, siksi tulisi lisäselvittää yksityishenkilölle toisena henkilönä esiintymisen kriminalisointia. (Henkilöllisyyden luomista koskeva hanke 2010.)

Kriminalisoinnin tulisi olla viimesijainen keino henkilöiden oikeuksien turvaamiseksi, mutta verkossa ei välttämättä ole muita keinoja. Oikeudeton identiteetin käyttö rajoittaa henkilön tiedollista itsemääräämisoikeutta ja rikkoo siten perustuslaissa taattua oikeutta yksityisyyteen. Identiteettivarkauden uhrille yksityisyyden menetys voi merkitä myös taloudellista menetystä tai muuta perinteistä vahinkoa huomattavampaakin haittaa. Siitä voi tulla esimerkiksi merkittäviä sosiaalisia seuraamuksia. Silti tekoa ei tällä hetkellä ole säädetty kaikilta osin rangaistavaksi. (Henkilöllisyyden luomista koskeva hanke 2010.)

5.6 Poliisin toimivalta identiteettirikollisuutta vastaan

Keskusrikospoliisin ylitarkastaja Sari Kajantie sanoo, että poliisin toimivaltuudet verkossa ovat rajalliset, koska tuomioistuin päättää, mitä viestejä poliisi voi saada haltuunsa. Tuomioistuimen päätös riippuu siitä, kuinka korkeasti rangaistavaa rikosta tutkitaan. Rikoksesta epäilty voi vakoilla rikoksen uhrin viestintää,

mutta rikosta ei voida selvittää, koska siinä tapauksessa poliisi loukkaisi rikoksesta epäillyn oikeutta liian vahvasti. Rikoksen uhrin ja rikoksesta epäillyn oikeudet eivät siis ole tasapainossa. Tällä hetkellä suojataan rikoksesta epäillyn oikeutta luottamukselliseen viestintään vahvemmin kuin kenenkään muun. Suomi odottelee EU:n lopullista linjausta identiteettivarkauksien kriminalisoinnista, ennen oman lainsäädännön muuttamista. (Yle Poliisi-TV 2013.)

Poliisi ei nykyisen lainsäädännön puitteissa pääse identiteettivarkaiden jäljille. Keskusrikospoliisin mukaan kyse on laajamittaisesta ja organisoidusta rikollisesta liiketoiminnasta. Tietosuojavaltuutettu Reijo Aarnion mukaan identiteettikaappauksen kriminalisointi alkaa olla välttämätöntä. Nykyinen järjestelmä ei riittävästi suojaa identiteettivarkauden kohdetta. (Uusi suomi 2009.)

5.7 Identiteettivarkauden vaikea selvittäminen

Tietoverkossa rikoksen tutkiminen on usein liian myöhäistä tiedon väärinkäyttöön liittyvien tunnusmerkistöjen täyttyessä, sillä tiedon keräämiseen liittyvä tietotekninen jälki ei enää ole tallella. Identiteettirikollisuuden tutkinnassa verkkoliikenteen seuraamiseen saa luvan vasta, kun tutkitaan törkeää rahanpesua, siinä vaiheessa rikollisten jäljet ovat jo kadonneet, sillä varsinaiset identiteettikaappaukset ja korttipetokset ovat tapahtuneet paljon aiemmin. Lainsäädäntö estää poliisia tutkimasta verkossa uhreja uhkaavaa rikollisuutta, vaikka kyse on rikoksen uhrin oikeusturvasta. KRP:n ylitarkastajan Sari Kajantien mukaan koneiden välisen tietoliikenteen seuraaminen on ainoa tapa päästä identiteettivarkaiden jäljille. Näin ainakin voitaisiin varoittaa ihmisiä ja kuolettaa kortit, vaikka tekijöitä ei saataisikaan kiinni. Identiteettirikollisuus on organisoitua liiketoimintaa, joka toimii alihankintaverkostona toisin kuin perinteinen järjestäytynyt rikollisuus. (Uusi Suomi 2009)

Petosvyyhtien ja isojen tietomurtojen takana on usein järjestäytynyt rikollisuus. Tekijöitä on vaikea jäljittää. Usein uhri havaitsee identiteettivarkauden vasta pitkän ajan kuluttua sen tapahtumisesta. Tämä hankaloittaa rikoksen selvittämistä, koska urkinnasta syntyvä tekninen jälki on jo saattanut kadota. Omaa rahaliikennettä kannattaa seurata aktiivisesti. Se onnistuu esimerkiksi Suomen asiakastiedon tarjoaman omatietopalvelun kautta. Aina, kun jokin taho kysyy

luottotietoja, järjestelmä lähettää asiakkaalle ilmoituksen tästä. Varastettujen henkilöpapereiden käytön voi estää oma luottokielto -merkinnällä. (Anna 2013.)

6 Uhrin asema

Identiteettivarkauden uhrin asema on tällä hetkellä huono. Identiteettivarkaus voi sekoittaa elämän pitkäksi aikaa. Virheelliset tiedot ovat voineet levitä internetissä hyvinkin laajalle ja niiden poistaminen on lähes mahdotonta. Identiteettivarkauden uhrilla tulisi olla nykyistä paremmat edellytykset toipua identiteettivarkaudesta ilman kohtuutonta vaivannäköä. (Henkilöllisyyden luomista koskeva hanke 2010.)

6.1 Identiteettivarkaudet voivat loukata myös omistusoikeutta

Identiteettivarkaudet loukkaavat omistusoikeutta, silloin kun rikoksella aiheutetaan uhrille taloudellista vahinkoa. Identiteettivarkaudet loukkaavat myös oikeutta yksityisyyteen sekä yksityisen viestinnän suojaan. Tietoverkko eroaa huomattavasti fyysisestä ympäristöstä, vaikka sääntely reaalimaailmassa olisi aivan riittävää, niin se ei välttämättä tarjoa vastaavaa suojaa tietoverkossa. Samojen vaikutusten tulisi olla kriminalisoituna molemmissa toimintaympäristöissä tasapuolisesti. (Henkilöllisyyden luomista koskeva hanke 2010.)

6.2 Uhrin asema identiteettivarkauksissa

Tietoverkossa lainsäädäntö pitää henkilöllisyysrikoksen uhrina palveluntarjoajaa, jota on harhautettu toisen henkilötiedoilla, vaikka tosiasiallisesti myös identiteettinsä menettänyt henkilö on uhri.

Merkittävin epäkohta uhrin asemassa on se, ettei viranomaisilla ole aina toimivaltuutta torjua vahinkoja. Uhrilla ei ole välttämättä edes tietoa rikoksen tapahtumisesta, jos rikollinen on tehnyt uhrin nimissä osoitteenmuutoksen. Luottotiedot voivat vaarantua uhrin tietämättä. Identiteettivarkauden tapahtumisesta todistustaakka on tällä hetkellä käytännössä rikoksen uhrilla.

Rikosilmoituksen tekemisen jälkeenkin, uhri joutuu usein vakuuttamaan palveluntarjoajille tai perintäyrityksille, ettei hän ole laskujen aiheuttaja. Tästä aiheu-

tuu merkittävästi haittaa ja vaivaa uhrille. (Henkilöllisyyden luomista koskeva hanke 2010.)

Identiteettivarkauksilta suojautuminen ja ennaltaehkäisy ovat olennaisimpia seikkoja. Identiteettitietojen helppo saatavuus altistaa henkilöitä identiteettivarkauksille. Identiteettivarkauksia on tapahtunut erilaisia viranomaisten julkisia rekisterejä, esimerkiksi kaupparekisteriä, hyväksikäyttäen. Myös nämä viranomaistiedoissa olevat aukot on selvitettävä ja tukittava identiteettivarkauksien ehkäisemiseksi. Tarkastelun pääkohdaksi tulee nostaa uhrin asema. Toipumista edistävät toimet ovat erityisen tärkeitä. Uhrin aseman kannalta ongelmallisena voidaan pitää sitä, että vahingonkorvauslaki ei mahdollista uhrille oikeutta kärsimyskorvaukseen, vaikka identiteettivarkaudet voivat aiheuttaa huomattavaa kärsimystä ja vahinkoa niiden uhreille. (Lakimiesliitto 2013.)

6.3 Identiteettivarkauden vaikutus uhriin

Identiteettivarkaus voi sekoittaa elämän vuosikausiksi. Virheelliset tiedot ovat voineet levitä netissä hyvinkin laajalle. Virheellisten tietojen korjaaminen vaatii aikaa ja rahaa. Uhri voi silti menettää luottotietonsa. (Anna 2013.)

Hän saattaa myös törmätä nimissään esitettyihin arveluttaviin mielipiteisiin esimerkiksi työpaikkaa hakiessaan. Myös henkinen taakka on raskas. On ahdistavaa ajatella, että joku ehkä esiintyy minuna. (Anna 2013.)

6.4 Uhrin aseman turvaaminen identiteettivarkauden jälkeen

Identiteettivarkauden uhrilla tulisi olla nykyistä paremmat edellytykset toipua identiteettitiedon kaappaamisesta ja taloudellisesta väärinkäytöstä ilman kohtuutonta vaivannäköä. Sisäministeriön työryhmä ehdottaa ensimmäisenä toimenpiteenä toimintaohjeen tekemistä henkilöllisyysvarkauden uhrin jatkotoimista. (Henkilöllisyyden luomista koskeva hanke 2010.)

Tulisi tarkastella mahdollisuutta rakentaa keskitetty ilmoitusjärjestelmä, jonka kautta tieto identiteettikaappauksista välittyisi nopeasti velkojille ja viranomaistahoille. Sisäministeriön työryhmä ehdottaa selvitystä, onko tällainen keskitetyn

ilmoitusjärjestelmän luominen käytännössä mahdollista. (Henkilöllisyyden luomista koskeva hanke 2010.)

7 Tulevaisuus

Tulevaisuudessa tärkeää on identiteettivarkauksilta suojautuminen ja ennaltaehkäisy. Suunnitteilla on erillinen työryhmä ongelmien ratkaisemiseksi. Olisi tarpeen linjata periaatteet, joiden mukaan henkilön katsotaan joutuneen identiteettivarkauden uhriksi. Nykyinen rikoslaki ei toimi tarvittavalla tavalla tilanteessa, jossa henkilö esiintyy toisen nimellä kiusantekomielessä. (Oikeusministeriö 2013.)

7.1 Sisäasiainministeriön henkilöllisyyden luomista koskeva hanke

Valtioneuvoston hyväksymän ja sisäasiainministeriön johtaman sisäisen turvallisuuden ohjelman yksi osa-alue on tietoverkkorikollisuus ja siihen liittyvät identiteettivarkaudet. (Henkilöllisyyden luomista koskeva hanke 2010.)

Sisäasiainministeriön henkilöllisyyden luomista koskevan hankkeen keskeisenä tavoitteena on henkilöllisyyden turvaaminen ja toisen henkilöllisyyden väärinkäytön ennalta estäminen. Poliisilla on toisen henkilöllisyyden väärinkäytön osalta keskeinen käytännön toimijan rooli. (Henkilöllisyyden luomista koskeva hanke 2010.)

7.2 Oikeusministeriön lausunto

Oikeusministeriö pitää oleellisimpina seikkoina identiteettivarkauksilta suojautumista ja ennaltaehkäisyä. Ennen kaikkea korostetaan valistusta, tiedotuskampanjoita ja oikeiden toimintamallien omaksumista. Identiteettivarkauksilta suojautumiseen kuuluvat asianmukainen virustorjunta, ohjelmistopäivitykset, postin ja asiakirjojen sekä henkilötietojen oikeanlainen käsittely. (Oikeusministeriö 2013.)

Hyvin tärkeänä seikkana pidetään identiteettivarkauksista toipumisen helpottamista. Tärkeä ja konkreettinen asia on se, miten rikoksen jälkeen saadaan korjattua virheet esimerkiksi erilaisissa rekistereissä. Tärkeää olisi, että käytännön

apu virheiden korjaamisessa, selvittämisessä ja sen ohjeistamisessa olisi riittävän laajaa. (Oikeusministeriö 2013.)

7.3 Suunnitteilla erillinen työryhmä ongelmien ratkaisemiseksi

Ongelmien ratkaisemiseksi olisi aihetta perustaa erillinen työryhmä, johon voisi nimetä jäseniksi eri viranomaisten edustajia sekä yksityissektorin edustajia. Identiteettivarkaudesta toipumista edistävät toimet ovat tässä erityisen tärkeitä. Identiteettitiedon saatavuuden helppous altistaa henkilöitä identiteettivarkauksille. Identiteettivarkauksia tapahtuu myös viranomaisten julkisia rekistereitä hyväksikäyttäen, siksi viranomaistiedoissa olevat aukot tulisi tukkia. (Oikeusministeriö 2013).

Mikäli identiteettivarkaus tekomuotona haluttaisiin erikseen kriminalisoida, tulisi tällöin pyrkiä seuraamaan kansainvälisiä mittapuita. Esiin tulee myös nostaa tietoverkkorikosdirektiivi. Lainsäädäntö ja rikosoikeus toimivat suhteellisen huonosti kansainvälisesti avoimessa tietoverkossa. Toisena esiintymisen kriminalisointi erityisesti kiusaamistarkoituksessa on iso kysymys, minkä vaikutusta yksilön oikeusturvaan on syytä edelleen tarkastella vakavasti. (Oikeusministeriö 2013.)

Identiteettivarkauden luomista koskevan hankkeen ongelmaksi jäävät viestintäsalaisuuden loukkauksen tunnusmerkistö sekä oikeudetta, mutta ilman vahingoittamistarkoitusta luodut valeprofiilit. Ensimmäinen ongelma on lakitekninen ja helposti korjattavissa, sitten kun perustelut muutostarpeelle ovat riittävät. Valeprofiilit onkin poliittisempi ja riippuu lainsäätäjän tahdosta, halutaanko erilaiset sosiaalisen median huiputukset säätää rangaistaviksi. Toisen henkilötietojen käyttämisessä ei aina ole kyse välttämättä vakavista tapauksista Valtakunnansyyttäjänviraston mukaan. On tarpeetonta silti väheksyä sitä loukkausta, minkä henkilötietojen luvaton käyttö saattaa aiheuttaa, riippumatta siitä, onko menettelystä aiheutunut konkreettista vahinkoa. (Oikeusministeriö 2013.)

7.4 Helsingin syyttäjänviraston mielipide

Helsingin syyttäjänviraston mukaan tulee kuitenkin ottaa huomioon, että toisen henkilön nimissä esiintyminen sisältää tietoisen riskin vahingosta tai haitasta sille, jonka nimeä tai identiteettiä on käytetty. Esiintyminen toisena tapahtuu ilman rikoksen uhrin tietoa siitä tai tietoa tarkoituksesta, johon nimeä tai identiteettiä on käytetty. Kriminalisointia pohdittaessa tulisi ottaa huomioon tilanteet, joissa jollekin tosiasiallisesti aiheutuu väärällä identiteetillä esiintymisen johdosta vahinkoa tai haittaa ilman, että sitä olisi suoranaisesti tarkoitettu. (Oikeusministeriö 2013.)

Nykylainsäädännön mukaan tällaiset tilanteet, joissa ei ole varsinaisesti haluttu aiheuttaa haittaa, jäävät tekojen tahallisuudessa ilmenevien puutteiden johdosta rankaisemattomiksi. Sellaiset tilanteet, joissa tekijä mieltää väärän identiteetin käyttämisestä voivan todennäköisesti aiheutua vahinkoa tai haittaa jollekin, täytyisi voida kriminalisoida, vaikka väärän identiteetin luominen olisi ongelmallista kriminalisoida. (Oikeusministeriö 2013.)

7.5 Tulevat toimenpiteet

Keskeisimmät toimenpidekohteet liittyvät tällä hetkellä uhrin avustamiseen. Olisi tarpeen linjata periaatteet, joiden mukaan henkilön katsotaan joutuneen identiteettivarkauden uhriksi. Dosentti Seppo Virtasen mukaan henkilön saadessa identiteettivarkauden uhrin statuksen viranomaiselta, olisi hänen todennäköisesti helpompaa edistää identiteettivarkaudesta johtuvien ongelmiensa ratkomista. Tärkeää on virheellisten rekisterimerkintöjen poistaminen. Tilanteiden selvittämisessä todennäköisesti auttaisi, se että henkilöllä olisi viranomaisen määrittämä identiteettivarkauden uhrin status. (Oikeusministeriö 2013.)

7.5.1 Sulkulistapalvelu

Sisäasianministeriön työryhmä ehdottaa ajokorttien, henkilökorttien ja passien sulkulistapalvelun toteuttamismahdollisuuden selvittämistä**.** Identiteettivarkauksien estämiseksi on syytä korostaa toimenpiteen merkitystä. Sulkulistan tulisi olla kaikkien poliisin myöntämien henkilöllisyyttä osoittavia asiakirjoja hyödyntävien palveluntarjoajien, kuten pankkien, kauppojen ja tunnistuspalvelun tarjoaji-

en käytettävissä. Sulkulistapalvelu olisi hyvä vaihtoehto identiteettivarkauksien torjuntaan, koska ne parantaisivat selvästi identiteettivarkauksien kohteeksi joutuneiden yksityishenkilöiden asemaa. Sulkulistapalvelua käyttämällä henkilö voisi saada samanaikaisesti suljettua keskeiset henkilöllisyyttä osoittavat asiakirjansa, kuten ajokortin ja henkilökortin. (Henkilöllisyyden luomista koskeva hanke 2010; Kuluttajavirasto 2011.)

7.5.2 Pakkokeinolaki 1.1.2014

Mahdollisuuksia tietoverkoissa tehtävien rikosten selvittämiseen lisää uusi 1.1.2014 voimaan tuleva pakkokeinolaki. Lainsäännökset antavat riittävät edellytykset tutkia tietoverkoissa tapahtuvia rikoksia Suomessa. (Oikeusministeriö 2013.)

Uutta pakkokeinolakia ollaan vielä täydentämässä ennen sen voimaantuloa, tietoverkoissa tapahtuvaan rikollisuuteen liittyen. (Oikeusministeriö 2013.)

7.5.3 EU:n tietoverkkodirektiivi

Sisältää määräyksiä myös identiteettivarkauksista. Raskauttavana asiana direktiivin mukaan pitäisi ottaa huomioon, että jos tietoverkkorikosten tekemisessä on käytetty toisen ihmisen henkilötietoja luottamuksen voittamiseksi ja sitä kautta aiheutettu uhrille vahinkoa. Sitä, miten direktiivi vaikuttaa Suomen lainsäädäntöön on vielä vaikea arvioida, sillä työryhmän työ on vasta alkamassa. (Helsingin Sanomat. Väärän nimen käyttäminen voi tulla rangaistavaksi.)

Esiintyminen väärällä nimellä voi tulla rangaistavaksi omana rikoksenaan. Valtakunnansyyttäjänvirasto kannattaa asiaa voimakkaimmin. Asia tulee pohdittavaksi pian oikeusministeriön työryhmässä, jossa selvitetään EU:n tietoverkkodirektiivin vaikutuksia Suomeen. Nykyinen rikoslaki ei toimi tarvittavalla tavalla tilanteessa, jossa henkilö esiintyy toisen nimellä kiusantekomielessä. Valtakunnansyyttäjänvirasto kannattaa asiaa voimakkaimmin. Nykyisin identiteettivarkaus on rangaistavaa vain, jos sillä pyrkii saamaan taloudellista hyötyä tai aiheuttamaan toiselle vahinkoa. Nyt valtakunnansyyttäjä katsoo aiheelliseksi kriminalisoida myös muun kiusanteon, koska sitä on esiintynyt huomattavan paljon

viime aikoina. (Helsingin Sanomat. Väärän nimen käyttäminen voi tulla rangaistavaksi.)

7.5.4 Oikeusministeriön arviomuistio

Oikeusministeriö laati asiasta arviomuistion keväällä 2013, johon pyydettiin lausuntoja eri tahoilta. Valtakunnansyyttäjänvirasto (VKSV) kannattaa voimakkaimmin uutta säännöstä identiteettivarkauksista, sillä yksityisissä suhteissa väärällä nimellä esiintyminen voi aiheutua toiselle ihmiselle paljon haittaa ja vahinkoa. Esimerkkejä VKSV on kerännyt elävästä elämästä. Näitä tilanteita ovat olleet tennisvuorojen, ravintolapöytien ja parturiaikojen varaaminen väärällä nimellä, sekä noloissa tilanteissa kollegan nimellä esiintyminen. Tällainen toiminta voi aiheuttaa paljon haittaa henkilölle. VKSV huomauttaa, että kiusanteon seuraukset voivat olla vakavia. (Helsingin Sanomat. Väärän nimen käyttäminen voi tulla rangaistavaksi.)

Voidaan tietysti ajatella, että syyllinen saa rangaistuksensa, jos tilaa toisen nimellä esimerkiksi huumeita internetistä, koska hän saa tuomion huumausainerikoksesta. Syyttömälle henkilölle aiheutuu kuitenkin huomattavaa haittaa tämän joutuessa mahdollisesti epäillyksi ja viranomaistoimenpiteiden kohteeksi sen takia, että joku on esiintynyt hänen nimellään. Tällaisia tekoja voidaan syyttää kunnianloukkauksina, mutta ne ovat kaukana pykälän ydinalueesta. (Helsingin Sanomat. Väärän nimen käyttäminen voi tulla rangaistavaksi.)

Tilanteita varten täytyisi olla oma säännöksensä, joka olisi arvioitu nykyisen sosiaalisen maailman pohjalta. Jos rikoslaki säädettäisiin vasta nyt, sinne säädettäisiin identiteettivarkaus. Ongelmana on myös sisäministeriön mukaan kiusaamistarkoituksessa tehdyt teot. Esimerkkejä tällaisista on internetiin luodut valeprofiilit, vaikkapa blogin tai facebook-sivun tekeminen toisen nimissä. Sisäministeriö arvioi, että tämä kiusaamisen ja pahoinvoinnin uusi muoto voi saada kohtuuttomia mittasuhteita uudessa toimintaympäristössä. Tiedon jakaminen verkossa on helppoa, mutta tiedon poistaminen on usein mahdotonta, mikä on uhrin kannalta ongelmallista. (Helsingin sanomat. Väärän nimen käyttäminen voi tulla rangaistavaksi.)

8 Yhteenveto ja pohdinta

Tutkin opinnäytetyössäni identiteettivarkautta. Päädyin aiheeseen, koska se on hyvin ajankohtainen ja mielenkiintoinen. Identiteettivarkaudet ovat olleet paljon esillä viime aikoina. Usein toisen nimissä esiinnytään esimerkiksi facebookissa ja twitterissä. Todellisen henkilöllisyyden haltijan maineen voi pilata tällä tavalla.

Työn tarkoituksena oli saada käsitys siitä, mikä on identiteettivarkaus ja perehtyä tarkemmin siihen, kuinka identiteettivarkaus sosiaalisessa mediassa ilmenee. Tarkastelun pääkohdaksi nousi identiteettivarkaudelta suojautuminen. Omalla huolellisuudella ja tarkkaavaisuudella voi suojautua jo hyvin pitkälle identiteettivarkauden torjunnassa. Tietenkään kaikissa tapauksissa oma huolellisuuskaan ei takaa sitä, etteikö joutuisi identiteettivarkauden uhriksi.

Identiteettivarkaus pitäisi kriminalisoida mahdollisimman nopeasti, sillä nykyinen lainsäädäntö ei ole pysynyt alati kasvavan verkkorikollisuuden mukana. Sisäasianministeriön henkilöllisyyden luomista koskevassa hankkeessa vuonna 2010 tarkasteltiin identiteettivarkauden kriminalisointia. Asia ei ole edennyt juurikaan ja nyt sisäasianministeriö pohtii erillisen työryhmän perustamista ongelmien ratkaisemiseksi. Tämä on hyvä asia, sillä sen avulla asia voi edetä.

Ongelmakohdaksi kriminalisointia pohdittaessa nousivat tilanteet, joissa jollekin tosiasiallisesti aiheutuu väärällä identiteetillä esiintymisen johdosta vahinkoa tai haittaa ilman, että sitä suoranaisesti olisi tarkoitettu. Suurimmat epäkohdat liittyvät ilman vahingoittamistarkoitusta luotuihin valeprofiilit.

Tällä hetkellä keskeisimmät toimenpidekohteet liittyvät uhrin avustamiseen. Tarpeen olisikin linjata periaatteet ja näiden periaatteiden mukaan henkilön katsottaisiin joutuneen identiteettivarkauden uhriksi. Jos identiteettivarkauden uhri saisi viranomaiselta uhrin statuksen, hänen olisi todennäköisesti helpompaa ratkoa identiteettivarkaudesta aiheutuvia ongelmia. Virheellisten rekisterimerkintöjen poistaminen nousee hyvin tärkeään asemaan.

Sisäasianministeriön työryhmän ehdottama ajokorttien, henkilökorttien ja passien sulkulistapalvelu on identiteettivarkauden estämisen kannalta erittäin merkittävässä asemassa. Sulkulistapalvelua käyttämällä henkilö voisi saada suljettua yhtä aikaa keskeiset henkilöllisyyttä osoittavat asiakirjansa, kuten henkilökortin ja ajokortin. Tällainen sulkulistapalvelu parantaisi selvästi identiteettivarkauksien kohteeksi joutuneiden yksityishenkilöiden asemaa.

Opinnäytetyö on tehty Internet-sivuja ja lehtiartikkeleita hyödyntäen. Sain paljon tietoa myös poliisin sivuilta. Opinnäytetyön tekeminen oli mielenkiintoista. Opinnäytetyötä aloittaessani en tiennyt juuri mitään identiteettivarkaudesta. Tiesin, että se on kasvava ja ajankohtainen rikollisuudenmuoto, koska lehdissä käsiteltiin usein aihetta, mutta en tiennyt, millaisina muotoina se voisi esiintyä. Opinnäytetyö oli hieman hankala tehdä sen vuoksi, että tietoa piti kerätä sieltä täältä. Hankaluutta lisäsi myös se, että kirjallisuutta aiheesta ei juuri löytynyt.

Tietoa oli kuitenkin mielenkiintoista etsiä. Nyt tiedän, kuinka identiteettivarkaudelta kannattaa yrittää omalla huolellisuudella suojautua. Tästä lähtien tulen kiinnittämään huomattavasti enemmän huomiota huolellisuuteen Internetissä, koska nyt tiedän riskit.

LÄHTEET

Anna 2013. Joku voi varastaa sinut. http://www.anna.fi/hyva-olo/varo-joku-voi-varastaa-sinut/. Luettu 20.7.2013

Asianajajaliitto. Tiedotteita ja lausuntoja 2013. http://www.asianajajaliitto.fi/viestinta/tiedotteita_ja_lausuntoja/lausunto_identiteettivarkaus-tyoryhman_loppuraportista.6328.news. Luettu 10.10.2013

Digitoday.2011.http://www.digitoday.fi/yhteiskunta/2011/01/26/facebook-todistaa-oikeusturva-pettaa-identiteettivarkauksissa/20111241/66. Luettu1.9.2013

Google. Turvassa pysyminen verkossa. http://www.google.com/intl/fi_fi/goodtoknow/online-safety/identity-theft/. Luettu 28.9.2013

Haasio A. 2013. Netin pimeä puoli. Helsinki: Suomalaisen kirjallisuuden seura

Helsingin Sanomat. Identiteettivarkaus. 8.12.2012 http://www.hs.fi/kotimaa/Identiteettivarkauden+kriminalisointi+ei+ole+edennyt/a1305626526975. Luettu 26.10.2013

Helsingin Sanomat. Väärän nimen käyttäminen voi tulla rangaistavaksi. 11.11.2013 http://www.hs.fi/kotimaa/V%C3%A4%C3%A4r%C3%A4n+nimen+k%C3%A4ytt%C3%A4minen+voi+tulla+rangaistavaksi/a1384143030696. Luettu 14.11.2013

Henkilöllisyyden luomista koskeva hanke 2010. Sisäasiainministeriön julkaisuja 32/2010. http://www.intermin.fi/download/16144_Identiteettiohjelman_loppuraportti.pdf. Luettu15.8.2013

Kuluttajavirasto 2011. Lausunnot ja kannanotot. http://www.kuluttajavirasto.fi/fi-FI/lausunnot/lausunnot/?groupId=2b878133-40ec-4663-a1ec-4ce25d3362da&announcementId=e4590fc6-3e77-452c-8242-2aad4ff0e7d4. Luettu 19.9.2013.

Lakimiesliitto. Lausunto oikeusministeriölle 15.5.2013 http://www.lakimiesliitto.fi/liitto/kannanotot-ja-lausunnot/lausunto-oikeusministeriolle-identiteettivarkauksista/. Luettu 8.11.2013

Norton. Identiteettivarkauden välttäminen. http://fi.norton.com/identity-theft-primer/article. Luettu 30.8.2013

Oikeusministeriö 2013. Lausunto tiivistelmä http://oikeusministerio.fi/fi/index/julkaisut/julkaisuarkisto/1380522953940/Files/OMML_47_2013_Idetiteetti_laustiiv_34s.pdf .Luettu 30.10.2013

Poliisi. Identiteettivarkaudet 2013. http://www.poliisi.fi/poliisi/helsinki/home.nsf/pages/4AA4B4D403026EC2C2257A7E0034F614?opendocument. Luettu 29.7.2013

Suomen Asiakastieto Oy 2013.
https://www.omatieto.fi/luottotiedot/actValitseOtp.do. Luettu 11.12.2013

Taloussanomat 2013. Identiteettivarkauksien torjuntaa tehostetaan.
http://www.taloussanomat.fi/tietoliikenne/2013/06/30/rasanen-hslle-identiteettivarkauksien-torjuntaa-tehostetaan/20139101/12. Luettu 28.10.2013

Tranberg P, Heuer S. 2013. Älä kerro kaikkea itsepuolustusopas verkkoon. Helsinki: Talentum.

Uusi Suomi. Identiteettivarkaudet saatava kuriin 2011.
http://www.uusisuomi.fi/kotimaa/111484-holmlund-identiteettivarkaudet-saatava-kuriin. Luettu 15.9.2013

Uusi Suomi 2009. http://www.uusisuomi.fi/kotimaa/63266 poliisi-laissa-puute-identiteettivarkaita-ei-saada-kuriin. Luettu 12.8.2013

Yle. Identiteettivarkaus sekoittaa elämän 2012.
http://yle.fi/aihe/artikkeli/2012/02/02/identiteettivarkaus-sekoittaa-elaman.
Luettu 10.12.2013

Yle Poliisi-TV. Rikoksesta epäillyn oikeudet verkossa uhria paremmat. Esitetty 22.2.2013. http://yle.fi/ohjelmat/kortit/poliisi-tv/jaksot/94201403000.html.
Luettu 3.10.2013

Yle uutiset. 2012 Identiteettivarkaus on suomessa toistaiseksi tuntematon rikos.
http://yle.fi/uutiset/identiteettivarkaus_on_suomessa_toistaiseksi_tuntematon_rikos/5293044_30.7.2009 päivitetty 27.5.2012. Luettu 30.6.2013