

Henkilöllisyyden todentamisvelvollisuus osana väärinkäytösten ehkäisemistä – luotto ja verkkomaksaminen

Nora Perko

5/2023

TIIVISTELMÄ

Nora Perko: Henkilöllisyyden todentamisvelvollisuus osana väärinkäytösten ehkäisemistä – luotto ja verkkomaksaminen

Opinnäytetyön muoto: Tutkimuksellinen

Julkisuusaste: Julkinen

Ohjaaja: Olavi Kujanpää, Sanna Virtanen

Tutkinto: Poliisi (AMK)

Tämän opinnäytetyön tarkoituksena oli selvittää mitä muutoksia lokakuussa vuonna 2023 kuluttajansuojalain luottoja koskevaan lukuun ja tarkemmin henkilöllisyyden todentamisvelvollisuutta koskeviin säännöksiin on väärinkäytösten ehkäisemiksi tulossa. Lisäksi tarkoituksena oli selvittää mistä syystä nyt voimassa olevat henkilöllisyyden todentamisvelvollisuutta koskevat säännökset ovat syntyneet ja mitä vaikutuksia niiden voimaantulo vuonna 2010 toi väärinkäytösten vaikeutuksessa. Opinnäytetyössä käsitellään lisäksi rikoksia, joita toisten henkilötiedoilla luotonannossa ja verkkomaksamisessa voi tehdä, eli petosrikollisuutta ja identiteettivarkauksia, sekä sivutaan myös asianomistajalle tällaisista rikoksista aiheutuvia haittoja. Tutkimusmetodina on käytetty lainopillista ja oikeushistoriallista metodia. Lähdeaineistona on toiminut suurelta osin lainvalmisteluaineisto sekä erilaisten aiheeseen liittyvien työryhmien tutkimukset.

Vuonna 2010 kuluttajansuojalakiin asetettiin luotonmyöntäjille velvollisuus tunnistaa lainanhakijat huolellisesti ja vahvan sähköisen tunnistamisen avulla, mikäli lainaa haettiin verkossa. Erityisesti tekstiviestitse haettavissa lainoissa oli esiintynyt väärinkäytöksiä, joissa lainaa otettiin toisen henkilötiedoilla. Vuonna 2020 julkiseksi tulleen Psykoterapiakeskus Vastaamon tietomurron jälkeen oikeusministeriö julkaisi tiedotteen, jossa kerrottiin, että väärin käsiin joutuneiden henkilötietojen avulla tehtäviä rikoksia on pystyttävä estämään asettamalla korkeampia vaatimuksia henkilöllisyyden todentamiseksi ja kuluttajansuojalain käyttöalaa on laajennettava. Kuluttajansuojalakiin 1.10.2023 voimaantulevilla muutoksilla pyritään estämään väärinkäytöksiä entistä tehokkaammin ja suurimpana muutoksen lakiin tulee vahvan sähköisen tunnistamisen vaatimus myös silloin, kun kuluttaja tilaa tuotteen myöhemmin maksettavaksi eli laskulle. Muutoksella pyritään estämään tilauspetoksia. Lisäksi vahvan tunnistamisen vaatimuksia laajennetaan myös luotonannon eri tilanteiden osalta.

Sivumäärä: 31

Tarkastuskuukausi ja vuosi: 5/2023

Avainsanat: Henkilöllisyys, maksaminen, luotto, todentaminen, identifiointi, identiteettivarkaus, petos

SISÄLLYS

1 JOHDANTO	1
1.1 Tutkimuksen aihe	1
1.2 Tutkimuskysymykset	2
1.3 Tutkimuksen rajaus ja aikaisempi tutkimus	3
1.4 Tutkimusmetodi, lähteet ja rakenne	4
2 KESKEISET KÄSITTEET.....	4
2.1 Henkilöllisyys ja henkilötunnus	4
2.2 Tunnistaminen ja todentaminen.....	5
2.3 Sähköiset tunnistamisvälineet.....	6
2.4 Luotto	8
2.5 Teemaan liittyvä rikollisuus.....	9
2.5.1 Petos	9
2.5.2 Identiteettivarkaus.....	9
2.5.3 Tietomurto.....	10
3 HUOMION KIINNITTÄMINEN VÄÄRINKÄYTÖKSIIN.....	11
3.1 Keskustelua identiteetin suojelemisesta	11
3.2 Pikaluottotyöryhmän perustaminen.....	12
3.3 Ongelmat luotonhakijan tunnistamisessa.....	13
3.3 Kuluttajansuojalain muutos 2010	14
3.3.1 Luotonhakijan henkilöllisyyden todentaminen.....	14
3.3.2 Ehdotusta koskeva lausuntopalaute	15
3.4 Laki vahvasta sähköisestä tunnistamisesta ja allekirjoituksista	17
3.5 Muutoksen voimaantulon vaikutukset	18
4 SÄÄNTELYN PÄIVITTÄMINEN	19
4.1 Verkon muuttunut toimintaympäristö.....	19
4.2 Kuluttajaluottotyöryhmän perustaminen	20
4.3 Kuluttajansuojalain muutos 2023	21
4.3.1 Lainanhakijan henkilöllisyyden todentaminen.....	21

4.3.2 Verkkosto laskulle	22
4.4 Ehdotusta koskeva lausuntopalaute	23
4.5 Vastuu väärinkäytöksistä ja uhrien asema	24
4.6 Muut aiheeseen liittyvät lainsäädäntöhankkeet	26
5 JOHTOPÄÄTÖKSET	27
6 POHDINTA	31
LÄHTEET	32

1 JOHDANTO

1.1 Tutkimuksen aihe

Verkko rikoksentekeväliseenä mahdollistaa paljon ja laajentaa väärinkäytösten mahdollisuuksia. Näin etenkin silloin, kun tällaisten väärinkäytön tekeminen mahdollistetaan palveluntarjoajan tarjoamassa palvelussa, esimerkiksi mahdollisuutena tilata tuotteita verkosta toisen henkilön tiedoilla. Viime vuosina onkin herätty siihen, että vääriin käsiin joutuneiden henkilötietojen avulla tehtäviä rikoksia on pystyttävä estämään asettamalla korkeampia vaatimuksia henkilöllisyyden todentamiseksi. Pääministeri Sanna Marinin hallitusohjelman mukaisesti verkossa tapahtuvan rikollisuuden tutkintaa ja torjuntaa aiotaan vahvistaa (Sanna Marinin hallitusohjelma 2019, 81).

Identiteettitiedon väärinkäyttöä on olennaisesti muuttanut tietoverkko, jossa tapahtuvan rikollisuuden ominaispiirteenä on suuri hyöty suhteessa pieniin kustannuksiin. Verkossa toiminnan voi automatisoida, jolloin rikoksen tekijät voivat käsitellä suuriakin määriä oikeudettomasti hankittuja identiteettejä. Verkko on myös globaali. (Identiteettiohjelma 2010, 53.) Verkossa tapahtuvan väärää henkilöllisyyttä hyödyntävän rikollisuuden voidaan myös sanoa olevan massailmiö. Tällä tarkoitetaan sitä, että vaikka oikeudettomasti hankittu yksittäinen luottokorttinumero itsessään ei ole arvokas, voi mittava määrä luottokorttinumeroita muodostaa merkittävän resurssin, jolla voidaan hankkia esimerkiksi arvokasta elektroniikka verkosta tilaamalla ja jälleenmyymällä. (Identiteettiohjelma 2010, 54.) Poliisihallituksen mukaan henkilötietojen väärinkäyttö identiteettivarkauksissa ja niihin liittyvissä petoksissa tapahtuukin usein sillä tavoin, että kolmas henkilö hankkii uhrin nimen ja osoitteen sekä henkilötunnuksen. Näillä tiedoilla tilataan hyödykkeitä verkkokaupasta, jolloin rikoksen uhri saa tiedon väärinkäytöksestä vasta, kun hän saa laskun tuotteista, joita hän ei ole tilannut. (POL-2020-84764, 2.)

Opinnäytetyön tarkoituksena on tutkia sitä, millaisia muutoksia kuluttajansuojalakiin (KSL, 38/1978) on tehty luotonantoon ja verkkomaksamiseen liittyvissä tilanteissa oikean henkilöllisyyden todentamiseksi sekä kuinka kyseisillä säännöksillä on pyritty ehkäisemään toisten henkilötietojen avulla tehtyjä väärinkäytöksiä, erityisesti petosrikollisuutta ja identiteettivarkauksia. Olen kiinnostunut erityisesti talous- sekä verkkorikollisuudesta, jonka vuoksi halusin valita aihepiirini jostain tältä sektorilta.

Aihe on ajankohtainen, sillä viime vuosina erityisesti lokakuussa 2020 julkiseksi tulleen Psykoterapiakeskus Vastaamon tietomurron jälkeen on ollut paljon keskustelua siitä mitä toisten henkilötiedoilla voi tehdä verkossa. Tietomurron jälkeen oikeusministeriö julkaisikin tiedotteen, jossa ilmais-

tiin, että luotonottoon ja maksamiseen liittyvien väärinkäytöksiä estämiseksi henkilöllisyyden todentamisvelvollisuuteen esitetään tiukennuksia. Velvollisuuden kerrottiin koskevan kaikkia kuluttajaluottoja ja tilanteita verkkoasioinnissa, jossa kuluttaja valitsee laskun maksutavaksi. Tiedotteen mukaan tiukennuksilla oli tarkoitus estää verkkokauppaostosten tekeminen käyttämällä toisen ihmisen henkilötunnusta sekä muita tietoja. (Oikeusministeriö 2020.)

1.2 Tutkimuskysymykset

Tarve toisen henkilön tiedoilla tehtyjen rikosten ennalta ehkäisyyn henkilöllisyyden todentamisvelvollisuuden avulla on tunnustettu jo aiemmin. Vuonna 2010 kuluttajansuojalakiin tehtiin muutoksia, joiden tavoitteena oli pääasiassa torjua pikaluottojen tarjontaan liittyviä ongelmia, mutta toisena tavoitteena oli myös parantaa tilaa, jossa lainaa haettaessa puutteellinen henkilöllisyyden todentaminen mahdollisti väärinkäytöksiä. Ongelmana olivat tuohon aikaan niin sanotut pikaluotot, joita pystyi hakemaan pelkällä tekstiviestillä. (HE 218/2022, 9.) Ennen kyseistä vuonna 2010 voimaan tullutta muutosta luotonantajilla ei ollut lainsäädännössä nimenomaista velvollisuutta tunnistaa tai todentaa asiakasta. Tuolloin voimaantulleet säännökset ovat voimassa tälläkin hetkellä.

Kuten aiemmin mainittiin, vuoden 2020 paikkeilla havahduttiin siihen, että todentamisvelvollisuutta koskevan kuluttajansuojalain sääntelyn käyttöalaa oli tarpeen laajentaa ja muultakin osin päivittää. Osa sellaisista maksupalveluntarjoajista ja luotonantajista, jotka eivät olleet velvollisia tunnistamaan asiakkaita vahvaa tunnistautumismenetelmää käyttämällä, olivat pyrkineet torjumaan identiteettivarkauksia ja petosrikoksia erilaisilla muilla keinoilla. Ottaen kuitenkin huomioon Poliisihallituksen tiedot rikosmääristä, nämä vapaaehtoiset keinot todettiin riittämättömiksi. (HE 218/2022, 23.)

Poliisihallituksella on ollut käytössään testianalytiikkatyökalu, jolla käytiin läpi kaikki aikavälillä 1.1.2020-30.11.2021 kirjatut rikosilmoitukset, joissa rikosnimikkeeksi oli kirjattu petosrikos. Näistä järjestelmä tulkitsi yhteensä 1860 tapausta, joissa oli tilattu tuotteita toisen henkilön henkilötunnuksella. Kun materiaalia käytiin läpi, huomattiin, että järjestelmän tekemät haut olivat oikeansuuntaisia. On kuitenkin huomattava, että Poliisihallituksen mukaan tapauksia on enemmän. Aineistosta nimittäin puuttuivat rikosilmoitukset, joissa nimikkeeksi oli kirjattu vain identiteettivarkaus, kun rikosilmoituksen selostetta lukemalla on ilmennyt, että kyse on selvästi myös petoksesta. Poliisihallituksen mukaan tilauspetosten määrä on kasvanut vuosi vuodelta. (HE 218/2022, 18.)

Opinnäytetyössäni tutkin sitä, mitä muutoksia henkilöllisyyden todentamisvelvollisuutta koskevaan kuluttajansuojalainsäädäntöön ollaan tänä vuonna tekemässä ja mikä muutosten tavoitteena on rikosten ennalta ehkäisyyn kannalta. Lisäksi tutkin voimassa olevien säännösten taustaa, eli syitä, jotka johtivat luotonhakijan huolellisen tunnistamisen vaatimukseen vuonna 2010. Tarkoituksena on

myös käydä läpi ne rikokset, joita näillä muutoksilla ennalta ehkäistään sekä arvioida sääntelyn vaikutuksia. Opinnäytetyössä tulen myös sivuamaan asianomistajalle tällaisista rikoksista aiheutuvia haittoja.

Tutkimuskysymykset ovat seuraavat:

- Millaisia rikoksia toisten henkilötiedoilla voi luotonannossa ja verkkomaksamisessa tehdä?
- Mistä syystä kuluttajansuojalain voimassa olevat luottoja koskevat henkilöllisyyden todentamisvelvollisuutta koskevat säännökset ovat syntyneet ja mitä vaikutuksia niiden voimaantulo vuonna 2010 toi väärinkäytösten ehkäisemiseksi?
- Mitä muutoksia todentamisvelvollisuutta koskeviin kuluttajansuojalain säännöksiin ollaan vuonna 2023 tekemässä ja mistä syystä?

Opinnäytetyö auttaa hahmottamaan henkilöllisyyden todentamiseen mahdollisesti liittyviä riskitekijöitä sekä avaa taustaa lainsäädännön muuttamiselle. Opinnäytetyö voi olla hyödyllinen esimerkiksi talous- ja verkkorikollisuuden parissa työskenteleville sekä muille poliisiorganisaation ulkopuolella, joita henkilöllisyyden todentaminen koskettaa työn puolesta.

1.3 Tutkimuksen rajaus ja aikaisempi tutkimus

Kun henkilöllisyyden todentamisvelvollisuuden tehtiin kuluttajansuojalaissa ensimmäiset merkittävät muutokset vuonna 2010, käsiteltiin ehdotuksessa myös muita luotonantoon liittyviä muutoksia, kuten kiskontaan ja viivästyskorkoon liittyviä asioita. Niin ikään lokakuussa 2023 voimaantulevaa kuluttajansuojalakia koskevaan hallituksen esitykseen on sisältynyt monia muita muutoksia, joiden tavoitteena on muun muassa ollut vähentää velkaongelmia, joita kuluttajaluottoihin liittyy sekä ohjata näiden luottojen hinnoittelua ja markkinointia yhteiskunnallisesti hyväksyttävämpään suuntaan (HE 218/2022, 23). Opinnäytetyössä ei ole tarkoitus käsitellä näihin ehdotuksiin sisältyviä muita muutoksia, vaan ainoastaan niitä, jotka koskevat henkilöllisyyden todentamisvelvollisuutta.

Rajaan opinnäytetyön ulkopuolelle myös henkilöllisyyden todentamisen muissa palveluissa kuin luotonantoon ja verkkomaksamiseen liittyvissä tilanteissa. Kuluttajia tunnistetaan myös esimerkiksi terveydenhuollossa ja työsuhteessa. Työn tarkoituksena ei ole kuitenkaan tutkia millä tavalla henkilöllisyyden todentaminen varmistetaan kaikissa mahdollisissa tilanteissa. Lisäksi tarkoituksena ei ole käsitellä maksukorttien ynnä muiden vastaavien huolimattomasta käsittelystä johtuvia vastuukysymyksiä, jotka ovat kokonaan oma aiheensa. Samoin ulkomaalaista lainsäädäntöä ei opinnäytetyön laajuuden vuoksi ole mahdollisuutta käsitellä.

Opinnäytetyön aihepiiriin liittyviä teemoja, esimerkiksi Psykoterapiakeskus Vastaamon tietomurtoa ja identiteettivarkautta on tutkittu erilaisissa opinnäytteissä. Lisäksi kuluttajansuojalain pikaluottoja

koskevaa muutosta vuodelta 2010 on kokonaisuudessaan tutkittu erilaisin näkökulmin opinnäytetöissä, mutta varsinaista henkilöllisyyden todentamisvelvollisuuteen keskittynyttä tutkimusta ei selvittelyni perusteella ole tehty. Lokakuussa 2023 voimaantuleva kuluttajansuojalain muutos on lisäksi niin ajankohtainen, että muutosta koskevia muita mahdollisia opinnäytetöitä ei ole vielä julkaistu.

1.4 Tutkimusmetodi, lähteet ja rakenne

Opinnäytetyö on tutkimusmetodiltaan pääasiassa lainopillinen. Lainoppi tuottaa tietoa voimassa olevan oikeuden sisällöstä (Kaisto 2005, 162) ja sen tarkoituksena on myös tulkita ja systematisoida sen sisältöä (Hirvonen 2011, 21). Opinnäytetyö on myös osaltaan oikeushistoriallinen, vaikkakin tutkimuksessa käydään läpi lyhyehkön ajan oikeudellista muutosta. Oikeushistoriallisella tarkastelulla voidaan auttaa ymmärtämään nykyhetkeä sekä tuoda esiin oikeudellisen muutoksen ja sen taustasyitä luonnehtivia ja selittäviä säännönmukaisuuksia (Kekkonen 1999, 8–9). Oikeushistoriallisessa tutkimuksessa on siis tarkoitus esittää vastauksia kysymyksiin miksi ja miten joku muutos tapahtui. Kyse on oikeudellisen muutoksen analyysistä (Kekkonen 1997, 132).

Ottaen huomioon opinnäytetyön näkökulma, opinnäytteen lähdeaineistona on toiminut suurelta osin lainvalmisteluaineisto, eli hallituksen esitykset, lausunnot, arviomuistiot, mietinnöt ja erilaisten työryhmien sekä projektien julkaisut henkilöllisyyden todentamiseen liittyen. Lisäksi olen etsinyt tietoa oikeuskirjallisuudesta sekä muista tieteellisistä julkaisuista. Olen tutustunut myös median julkaisemiin artikkeleihin ja uutisiin aihepiiriä koskien, sillä aihe on ollut pinnalla myös mediassa.

Opinnäytetyö jakautuu viiteen kappaleeseen. Johdannossa johdetaan lukijan aihepiiriin, jonka jälkeen toisessa luvussa käydään läpi aihepiiriin kannalta keskeiset käsitteet sekä rikosnimikkeet. Kun puhutaan henkilöllisyyden todentamisesta, vahvasta tunnistautumisen sekä näihin liittyvistä rikostunnusmerkistöistä kuten identiteettivarkaudesta, on mielestäni syytä määritellä käsitteistöä. Kolmannessa kappaleessa käsittelen ensimmäistä kuluttajansuojalain muutosta ja siihen liittyviä syitä sekä muutoksen seurauksia. Neljännessä kappaleessa siirryn tänä vuonna voimaan tulevaan kuluttajansuojalain muutokseen sekä käsittelen myös asianomistajille aiheutuvia haittoja. Viidennessä kappaleessa esitän johtopäätökset ja kuudennessa kappaleessa arvioin opinnäytetyöprojektia kokonaisuudessaan.

2 KESKEISET KÄSITTEET

2.1 Henkilöllisyys ja henkilötunnus

Henkilöllisyys on kokonaisuus, joka muodostuu ihmisestä ja häneen liitetystä väestötietojärjestelmän tiedoista. Henkilöllisyys muodostuu sillä hetkellä, kun väestötietojärjestelmään (VTJ) luodaan

henkilöä koskeva tietue, joka yhdistetään fyysiseen henkilöön. (Identiteettiohjelma 2010, 17.) Käytännössä tämä tarkoittaa syntymää tai maahan muuttamaa ulkomaalaista henkilöä, joka rekisteröidään Suomen järjestelmään (Identiteettiohjelma 2010, 21).

Laissa vahvasta sähköisestä tunnistamisesta ja luottamuspalveluista (Tunnistuslaki, 617/2009) säädetään, että luonnollisen henkilön identiteetin luotettuja lähteitä ovat viranomaisen myöntämät passit ja henkilökortit sekä väestötietojärjestelmä. Luotettavana lähteenä pidetään myös poliisin rekisteriä passien ja henkilökorttien voimassaolosta. (Tunnistuslaki 3:17.)

Väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain (VTJ-laki, 661/2009) mukaan, kun henkilön tiedot talletetaan ensimmäisen kerran väestötietojärjestelmään, hänelle annetaan henkilötunnus. Henkilötunnus annetaan automaattisesti VTJ:stä eikä korjattua tai muutettua henkilötunnusta saa antaa toiselle henkilölle. Tunnus on yksilöllinen muodostuen syntymäajasta, yksilönumerosta ja tarkistusmerkistä. Yksilönumerolla erotetaan henkilöt, jotka ovat syntyneet samana päivänä ja henkilötunnus sisältää myös tiedon henkilön sukupuolesta. (VTJ-laki 2:11.)

On muistettava, että aina pelkkä henkilötunnuksen esittäminen ei tarkoita, että kyseessä olisi juuri tämän henkilötunnuksen omaava henkilö vaan henkilöllisyyden luotettavaan varmistamiseen tarvitaan muitakin tietoja. Henkilötunnus kun voi olla muunkin kuin sen omistajan tiedossa. Tämä mahdollistaakin henkilötunnuksen väärinkäytön tilanteissa, jossa sitä käytetään tunnistamisen keinona. (VN/26031/2020-VM-2, 5). Henkilötunnus ei siis ole mikään salaisuus. Sen voi saada tietoonsa esimerkiksi hotellin virkailija tai postin pisteessä pakettia luovuttava. Kirjallisuudessa on muun muassa lausuttu, että tieto henkilötunnuksen vaaroista ja väärinkäytöksistä on johtanut kansalaisten keskuudessa ylivarovaisuuteen eikä sitä uskalleta aina kertoa niissäkään tilanteissa, joihin se on tarkoitettu (Järvinen 2022, 23.)

Henkilötunnusta saa käsitellä sellaisissa tilanteissa, joissa yksilöinti on tärkeää (Järvinen 2022, 25). Tietosuojalain (1050/2018) perusteella henkilötunnusta saa käsitellä esimerkiksi luotonannossa, maksupalvelutoiminnassa ja osamaksukauppaa tehtäessä. (Tietosuojalaki 5:29). Näin ollen luottoa hakiessa ja maksaessa verkossa osamaksulla joutuu asiakas antamaan henkilötunnuksensa.

2.2 Tunnistaminen ja todentaminen

Tunnistaminen ja todentaminen ovat termejä, jotka menevät usein sekaisin, sillä niitä käytetään arkikielessäkin eri merkityksessä. Lainvalmisteluaineistossa tunnistaminen on määritelty erilaisten tietojen perusteella tehtäväksi asiakkaan henkilöllisyyden selvittämiseksi. Todentamisella taas tarkoitetaan asiakkaan henkilöllisyyden varmistamista luotettavasta ja riippumattomasta lähteestä olevien tietojen taikka asiakirjojen perusteella. (HE 64/2009, 6.) Sähköisessä ympäristössä tapahtunut

todentaminen tapahtuu siten, että asiakas tunnistautuu vahvalla sähköisellä tunnistusvälineellä palveluun ja palvelun todentamismekanismeilla autentikoidaan se, että vahvan sähköisen tunnistusvälineen käyttäjä on se henkilö, joka väittää olevansa. Todentamisesta käytetään siis myös nimitystä autentikointi tai verifiointi. (Traficom 2021, 10).

Kun puhutaan sähköisestä tunnistamisesta, voidaan se jakaa heikkoon ja vahvaan tunnistamiseen. Heikolla tunnistamisella tarkoitetaan käytännössä esimerkiksi käyttäjätunnuksen ja salasanan yhdistelmää (HE 36/2009, 30). Tällaisilla yhdistelmissä kirjaudutaan esimerkiksi yrityksen jäsenpalveluun, verkkokauppaan tai keskustelualueelle. Tunnistamista voidaan pitää heikkona, koska nämä tiedot voivat helposti päätyä muiden käsiin. Sillä miten salasana ja sen säilyttämiseen tarkoitettu tietojärjestelmä suojataan, on tämän suhteen suuri merkitys. Myös salasanan muoto vaikuttaa tietenkin suoraan siihen, kuinka helposti hyökkääjä voi päästä sisälle palveluun. (Traficom 2021, 26.)

Vahvaan tunnistamiseen voidaan taas lukea vain tietyn käyttäjän tietämät tai omistavat menetelmät. Erona heikkoon tunnistamiseen on se, että vahvan tunnistamisen vaatimuksena on se, että tunnistusväline muodostuu vähintään kahdesta erilaisesta todentamistekijästä, jotka eivät ole toisistaan riippuvaisia. Esimerkkeinä todentamistekijöiden yhdistelmistä voidaan mainita mobiilisovellus ja PIN-koodi sekä mobiilisovellus ja sormenjälki. (Traficom 2021, 28.) Vahvan tunnistautumisen ominaisuus on se, että tunnistamisväline ja sen käyttö voidaan aina yhdistää viime kädessä henkilön todelliseen henkilöllisyyteen siitäkin huolimatta, että kyseessä olisi anonyymi käyttö. Tällä tarkoitetaan tunnistautumista, jossa palveluntarjoajalle ei ilmoiteta henkilön todellisia henkilötietoja (HE 36/2009, 8.)

Varsinainen virallinen määritelmä vahvalle sähköiselle tunnistamiselle löytyy tunnistuslaista. Sillä tarkoitetaan tunnistuslain mukaan sellaista henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnisteiden aitouden ja oikeellisuuden todentamista sähköistä menetelmää käyttäen, joka täyttää sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksessa määritellyn korotetun tai korkean varmuustason vaatimukset (Tunnistuslaki 1:2). Tällaisia asetuksessa edellytetyjä vaatimuksia ovat muun muassa se, että tunnistusvälineen voi sulkea nopeasti, jos se joutuu vääriin käsiin ja se voidaan toimittaa haltijalle turvallisesti (Traficom 2021, 28). Liikenne- ja viestintävirasto Traficom pitää Suomessa julkista rekisteriä sellaisista tunnistuspalveluista, jotka täyttävät nämä vaatimukset. Rekisteriin tulee tehdä ilmoitus ennen toiminnan aloittamista. (Traficom 2021, 14.)

2.3 Sähköiset tunnistamisvälineet

Tällä hetkellä käyttäjille on tarjolla kolmenlaisia vahvoja sähköisiä tunnistusvälineitä. Näitä ovat verkkopankkitunnisteet, mobiilivarmenteet sekä Digi- ja väestötietoviraston (DDV) tarjoamat hen-

kilö- ja organisaatiovarmenteet. (Traficom 2021, 57). Traficomien mukaan suomalaiset vahvan sähköisen tunnistautumisen järjestelmät ovat kansainvälisesti vertailtuna korkeatasoisia ja vaatimukset tiukimmasta päästä (Traficom 2022).

Verkkopankkitunnisteet ovat tunnisteista yleisin tunnistusväline. Niiden käyttämiseen tarvitsee pankin käyttäjätunnuksen, salasanan sekä erillisen tunnuslukulistan fyysisessä muodossa taikka älypuhelimeen ladattavan tunnuslukusovelluksen. Verkkopankkitunnisteen voi saada vain kyseisen pankin asiakas. (Traficom 2021, 58.) 1990-luvun jälkipuoliskolla pankit kehittivät TUPAS-tunnistamisen (turvallinen pankkiasiointi), joka perustui asiakkaan käyttäjätunnuksen ja salasanastaan. Sittemmin älypuhelinien myötä tunnistaminen on pääasiassa siirtynyt pääasiassa pankkien sovelluksiin ja nettipankkeihin (Järvinen 2022, 86).

Mobiilivarmenteen käyttämiseksi tarvitaan matkapuhelinliittymä (SIM-kortti), mobiilivarmentelle käyttäjätunnus sekä salasana. Mobiilivarmenteet toimivat myös muissa kuin älypuhelimissa. (Traficom 2021, 57). Mobiilivarmenteen perustuu siihen, että kun palvelu lähettää tunnistuspyynnön, operaattori pyytää puhelinta todentamaan itsensä SIM-kortin siruun upotetulla salaisella avaimella. Käyttäjä näkee tunnistuspyynnön puhelimen näytöllä ja hyväksyy sen itse valitsemallaan PIN-koodilla. (Järvinen 2022, 93). Mobiilivarmenteen saa käyttöönsä operaattorin kautta pankkitunnisteilla (Järvinen 2022, 94). Esimerkiksi vuonna 2020 mobiilivarmenteen oli valtionvarainministeriön teettämän tutkimuksen mukaan käytössä 22 prosentilla. Osa operaattoreista tarjoaa mobiilivarmenteita ilmaiseksi ja osa pientä kuukausimaksua vastaan (Traficom 2021, 58).

DDV:n henkilö- ja organisaatiovarmenteilla tarkoitetaan varmentamista, jossa käyttäjä tarvitsee henkilö- tai organisaatiokortin, jossa henkilö- tai organisaatiovarmenteen on aktivoitu, kortinlukulaitteen, salasanan sekä tietotekniselle laitteelle ladattavan ilmaiseksi ladattavan ohjelmiston. Näitä ei voi käyttää älypuhelimella, vaan ne vaativat erillisen kortinlukulaitteen toimiakseen. (Traficom 2021, 57.)

Jotta sähköisen tunnistamisvälineen saa käyttöönsä, tulee tehdä niin kutsuttu ensitunnistaminen. Ensitunnistamisella tarkoitetaan siis sitä, että vahvan sähköisen tunnistamisvälineen hakija todentaa henkilöllisyytensä, kun hän hankkii tunnistamisvälineen. Ensitunnistaminen voidaan toteuttaa fyysisesti tai sähköisesti. Fyysinen tunnistaminen tapahtuu esimerkiksi paikan päällä pankin konttorissa, jossa henkilö esittää virallisen henkilötodistuksen kuten passin. Sen jälkeen henkilön ulkoisia ominaisuuksia verrataan tähän passiin. Sähköinen tunnistautuminen hoidetaan esimerkiksi vahvalla sähköisellä tunnistusvälineellä eli etämenettelyllä. Sen, joka tarjoaa vahvaa sähköistä tunnistautumisvälinettä, täytyy varmistua siitä, että toinen vahvan sähköisen tunnistautumisvälineen tarjoaja voi käyttää sen myöntämää tunnistautumisvälinettä ensitunnistukseen. Tämä voi perustua esimerkiksi passin esittämiseen etäyhteydellä sen ja tarkistamiseen. (Traficom 2021, 10–11.)

Varsinaisia tunnistusvälityspalveluita tarjoavat esimerkiksi Signicat AS (Signicat) sekä Nets Branch Norway (NETS). Ne ovat toimijoita, jotka välittävät tunnistustapahtumia. Itse tunnistamisvälineitä tarjoavat pankit, matkaviestintäverkkoyritykset (esimerkiksi Telia) ja DDV. Kyseessä ovat siis toimijat, jotka tarjoavat tunnistusvälinettä käyttäjille ja tunnistusvälityspalvelun tarjoajalle välitettäväksi. (Traficom 2021, 8). Selkeytän termistöä esimerkkitapauksella. Otetaan henkilö, joka menee verkkokaupan sivuille ostamaan tuotteita ja etenee ostokorista maksutapahtumaan. Maksu vaatii vahvan tunnistamisen, ennen kuin se asiakas voi ottaa tuotteen. Asiakas valitsee tunnistamisvälineistä verkkopankkinsa Danske Bankin tunnukset. Verkkokauppa on hankkinut vahvan sähköisen tunnistuspalvelun NETS:n kautta. Asiakkaan henkilöllisyyden todentaminen tapahtuu Danske Bankin verkkopankkitunnusten avulla ja tunnistustapahtuman verkkokaupassa välittää NETS.

Vahvaa sähköistä tunnistamista käytetään myös muun muassa terveydenhuoltoalan yrityksissä, apteekeissa ja postipalveluyrityksissä. Vaikka palvelussa käsiteltäisiin henkilötietoja, käyttää usea yksityisen alan toimija kuitenkin tunnistamisessa edelleen heikkoa tunnistautumista. (Traficom 2021, 63.)

2.4 Luotto

Luotonannolla voidaan tarkoittaa erilaisia tilanteita, jossa eri osapuolten välillä on saamissuhteita. Yksinkertaisemmillaan kyse on rahaan kohdistuvasta velasta, mutta luotonantona pidetään myös esimerkiksi tavaroiden myymistä ilman käteismaksua. (Aurejärvi ja Hemmo 2004, 1.) Suomessa varsinaisten virallisten luottojen myöntäminen alkoi vuonna 2005 (Valkama ja Muttilainen 2008, 9).

Kulutusluotolla, joita tässäkin opinnäytetyössä käsitellään, tarkoitetaan yleisesti luottoa, jonka elinkeinonharjoittaja (luotonantaja) sopimuksen mukaan myöntää tai lupaa myöntää kuluttajalle lainana, maksunlykkäyksenä tai muuna vastaavana taloudellisena järjestelyinä (KSL 7:1). Näitä luottoja voidaan jakaa myös pikaluottoihin. Pikaluotolla tarkoitetaan yleisesti nopeasti saatavia pieniä kulutusluottoja, joita myönnetään yksityishenkilöille lainahakemuksen perusteella ja joiden saamiseksi ei tarvita vakuuksia. Nämä luotot ovat yleensä alle kolmen kuukauden pituisia kulutusluottoja ja määrältään muutamista kymmenistä euroista alkaen aina moneen sataan euroon saakka. (HE 64/2020, 4.) Luottoja voidaan jakaa myös sen perusteella, miten luotto nostetaan tilille. Kertaluotoilla tarkoitetaan luottoja, jossa luotonantaja antaa koko sovitun luoton määrän kerralla velkaa hakevalle, kun taas limiittiluotoissa velalliselle myönnetään esimerkiksi pankkitiliin liittyvä luotto, josta hän voi nostaa lainaa enimmäismäärään saakka (Aurejärvi - Hemmo 2004, 8).

Termiä luotto voidaan käyttää muussakin, kun varsinaisen lainan myöntämisen yhteydessä. Verkossa tavaroita voidaan ostaa myös niin sanotusti velaksi. Luottokortilla käyttäjä voi tehdä maksuja käyttäen kortilla olevaa luottoa ja kortilla tehdyt ostokset laskutetaan luottokortin haltijalta sovitun luottoajan puitteissa. (Aurejärvi - Hemmo 2004, 321.)

2.5 Teemaan liittyvä rikollisuus

2.5.1 Petos

Väärillä henkilötiedoilla verkossa tehdyissä rikoksissa on usein kyse petosrikollisuudesta, jossa tarkoituksena on saada taloudellisesta hyötyä. Jos toisen henkilötiedoilla tilataan tavaraa netistä, annetaan usein erikseen tuomio petoksesta ja päälle vielä identiteettivarkaudesta. (Järvinen 2022, 169). Rikoslain (RL, 39/1889) mukaan petoksesta tuomitaan se, joka, hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä taikka toista vahingoittaakseen, erehdyttämällä tai erehdystä hyväksi käyttämällä saa toisen tekemään tai jättämään tekemättä jotakin ja siten aiheuttaa taloudellista vahinkoa erehtyneelle tai sille, jonka eduista tällä on ollut mahdollisuus määrätä. Rangaistusasteikko on sakkoa tai vankeutta enintään kaksi vuotta ja petoksen yritys on rangaistava. (RL 38:1.)

Lievästä petoksesta on kyse silloin, jos petos on kokonaisuutena arvostellen vähäinen ottaen huomioon tavoiteltu hyöty, aiheutetun vahingon määrä tai muut rikokseen liittyvät seikat. Tällöin rangaistusasteikko on sakkoa. (RL 38:3) Mikäli petoksella tavoitellaan huomattavaa hyötyä, aiheutetaan huomattavaa tai erityisen tuntuva vahinkoa, rikos tehdään käyttämällä hyväksi vastuulliseen asemaan perustuvaa erityistä luottamusta tai rikos tehdään käyttämällä hyväksi toisen erityistä heikkoutta tai muuta turvatonta tilaa, on kyse törkeästä petoksesta, jos rikos on lisäksi kokonaisarvottelen törkeä. (RL 38:2.)

Maksuvälinepetoksesta voi olla kyse, kun käytetään verkossa luvattomasti toisen henkilön maksukortin tietoja taikka verkkopankkitunnuksia. Usein tunnusmerkistön täytyessä täyttyy myös petoksen tunnusmerkistö, mutta maksuvälinepetos erityissäännöksenä syrjäyttää sen. (Riekkinen 2018, 82.) Rikoslain mukaan maksuvälinepetoksesta tuomitaan se, joka hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä esimerkiksi käyttää maksuvälinettä ilman sen laillisen haltijan lupaa, lupaan perustuvan oikeutensa ylittäen tai muuten ilman laillista oikeutta. Rangaistusasteikko on sama kuin perusmuotoisessa petoksessa. (RL 37:8.) Törkeästä maksuvälinepetoksesta on kyse, jos petoksessa 1) aiheutetaan huomattavaa tai erityisen tuntuva vahinkoa, 2) rikos tehdään erityisen suunnitelmallisesti tai 3) rikos tehdään osana järjestäytyneen rikollisryhmän toimintaa, ja maksuvälinepetos on myös kokonaisuutena arvostellen törkeä. Tällöin rangaistusasteikko on vankeutta vähintään neljä kuukautta tai enintään viisi vuotta. (RL 37:9.)

2.5.2 Identiteettivarkaus

Mikäli käytetään hyväksi toisen henkilöllisyyttä ja tällä tavoin aiheutetaan toiselle vahinkoa, on rikoslain tunnusmerkistöjä tarkastellessa todennäköisimmin kyse identiteettivarkaudesta, joka säädettiin rikoslakiin vuonna 2015. Rikoslain mukaisesti identiteettivarkaudesta tuomitaan se, joka

erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suu-
rempaa haittaa sille, jota tieto koskee. Rangaistuksena on sakkorangaistus. (RL 38:9.)

Kolmas erehdytetty osapuoli voi olla esimerkiksi lainan myöntänyt pikavippiyhtiö tai verkkokauppa, josta väärillä tiedoilla on tilattu tavaraa. Tunnusmerkistön täyttymiseksi tietojen käytön on oltava oikeudetonta. Tässä arvioinnissa olennaista on myös oikeiden tietojen haltijan huolellisuus, joka on kyberrikoksiin liittyvä erityispiirre. Verkkopankkitunnusten väärinkäytön osalta oikeuskäytännössä onkin arvioitu sitä, onko tunnuksia huolimattomasti säilyttänyt henkilö voinut myötävaikuttaa rikoksen syntymiseen. (Soininen 2017, 91.) Tunnusmerkistössä mainittu taloudellinen haitta voi esimerkiksi olla identiteettivarkauden avulla tehtyjen pikavippien summa ja niihin liittyvät korot (Soininen 2017, 98).

Identiteettivarkaus on asianomistajarikos eli syyttäjä ei voi viedä asiaa eteenpäin, ellei rikoksen uhri tee syyttämispyyntöä ja vaadi tekijälle rangaistusta (Järvinen 2022, 169). Toisin on petosrikoksen osalta, joka on virallisen syytteen alainen rikos. Identiteettivarkauden kriminalisointi paransi uhrin asemaa, koska hänestä tuli rikoksen osapuoli. Ennen kriminalisointia on katsottu pelkästään kauppojen olevan uhreja, joilta petoksella oli tavaroita tilattu. (Järvinen 2022, 169). Katsoakseni muutos on tuonut uhrin aseman niin sanotusti viralliseksi, kun se on lainsäädännön tasolla tunnistettu.

Kun identiteettivarkaus lisättiin rikoslakiin syyskuussa 2015, tehtiin siitä 530 rikosilmoitusta vuoden loppuun mennessä. Vuoden 2021 aikana identiteettivarkautta koskevia rikosilmoituksia tehtiin 3300 kappaletta (Rikos- ja pakkokeinotilasto SVT 2022). Keskimäärin per vuosi identiteettivarkauksia on sen säätämisen jälkeen tilastoitu noin 3000–4000 kappaletta (VN/26031/2020-VM-2, 4).

2.5.3 Tietomurto

Usein henkilötiedot päätyvät vääriin käsiin tietomurtojen kautta. Tietomurrosta tuomitaan rikoslain mukaan se, joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla, oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan. Rangaistusasteikko on sakkoa tai vankeutta enintään kaksi vuotta.

Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta 1) teknisen erikoislaitteen avulla tai 2) muuten teknisin keinoin turvajärjestelyn ohittaen, tietojärjestelmän haavoittuvuutta hyväksi käyttäen tai muuten ilmeisen vilpillisin keinoin oikeudettomasti ottaa selon 1 momentissa tarkoitettussa tietojärjestelmässä olevasta tiedosta tai datasta. Yritys on rangaistava. Tätä pykälää sovelletaan ainoastaan tekoon, josta ei ole muualla laissa säädetty ankarampaa tai yhtä ankaraa rangaistusta. (RL 38:8.)

Tietomurtojen ja -vuotojen lisäksi henkilötietoja voi päätyä ulkopuolisille esimerkiksi lompakkovarkauksissa, roskisdykkauksesta ja postivarkauksissa. (Järvinen 2022, 176). Joskus rikolliset keräävät henkilötietoja, jotta he voivat myydä niitä eteenpäin makkinoilla. Pimeässä verkossa eli Tor-verkossa näin tapahtuukin varsin avoimesti. (Haasio 2017, 84.) Useimmiten henkilötietojen väärinkäyttäjä ei siis välttämättä itse ole tehnyt tietomurtoa, mutta tiedot ovat levinneet hänelle muuta kautta.

3 HUOMION KIINNITTYMINEN VÄÄRINKÄYTYKSIIN

3.1 Keskustelua identiteetin suojelemisesta

Henkilöllisyyden oikeudettomaan käyttöön ja sen erityiseen suojaamiseen alettiin kiinnittää erityistä huomiota Suomessa ennen 2010-lukua. Sisäministeriö asetti vuoden 2008 lopulla hankkeen, jonka tarkoituksena oli vahvistaa henkilöllisyyden luomista koskevia menettelytapoja sekä laatia henkilöllisyyttä koskeva lainsäädäntö. Hankkeen perimmäinen tavoite oli luoda kansallinen identiteettiohjelma, jonka sisältönä oli suunnitella valtion tehtävää henkilöllisyyden luomisessa ja suojaamisessa erityisenä painoalueenaan identiteettivarkaudet ja niiden ennalta estäminen. Hanketyöryhmää kuului jäseniä mm. Keskusrikospoliisista, Poliisihallituksesta, poliisilaitoksilta sekä sisäasiainministeriön poliisiosastolta. Työryhmä julkaisi hankkeen loppuraportin sisäasiainministeriölle joulukuussa 2010 eli työryhmän toimikausi oli noin kahden vuoden mittainen. (Identiteettiohjelma 2010, 6.)

Työryhmä totesi raportissaan, että kansainvälisellä tasolla identiteettivarkaudet olivat muodostuneet vakavaksi ongelmaksi (Identiteettiohjelma 2010, 15–16). Esimerkiksi Britanniassa vuonna 2008 identiteettirikoksiin liittyvissä verkkopankkirikoksissa rikolliset hankkivat rikoshyötyä yli 29 miljoonaa euroa ja Suomessa vastaava luku oli yli 50 000 euroa (Identiteettiohjelma 2010, 48). Euroopan Unionissakin (EU) aloitettiin kuuleminen sen suhteen, tarvitaanko lainsäädäntöä tilanteissa, jossa tietoverkkorikollisuuteen liittyy henkilöllisyyden väärinkäyttö. Tätä koskevassa komission tiedonannossa todettiin, että EU:n lainvalvontayhteistyö huomioiden olisi parempi, jos väärän henkilöllisyyden käyttö määriteltäisiin rikokseksi kaikissa EU:n jäsenvaltioissa. (Identiteettiohjelma 2010, 52).

Identiteettiohjelman työryhmä huomioi, että verkossa tapahtuvien identiteettivarkauksien osalta kyse oli ennen kaikkea toimintaympäristön muutoksesta (Identiteettiohjelma 2010, 15–16). Todettiin, että verkon osalta tarvitaan myös muita kuin rikosoikeudellisia keinoja rikosten ennalta ehkäisyn tehostamiseksi ja tästä hyvä esimerkki olivat erilaisten palveluiden suunnittelussa tehdyt valinnat (Identiteettiohjelma 2010, 77). Uskoakseni tällä saatettiin tarkoittaa esimerkiksi yritysten erilaisia toimintatapoja todentaa asiakkaansa henkilöllisyys ja näin estää väärinkäytöksiä. Tästä esimerkkinä voidaan mainita vuonna 2007 Suomen Pienlainayhdistyksen hyväksyvät ensimmäiset eettiset säännöt pienlainatoimintaa koskien, joita myöhemmin on päivitetty. Yhdistyksen jäsenenä ei

ollut kuitenkin kuin pieni osa markkinoiden toimijoista, joten sääntöjen merkitystä ei voitu pitää kovin suurena. (Parkkali. E, Pönkä. V. 2010, 588). Säännöissä asetettiin jäsenyryyksille muun muassa velvollisuus käyttää luotettavia ja kulloinkin voimassa olevia keinoja lainanhakijan henkilöllisyyden todentamiseksi (HE 64/2009, 13).

Identiteettiohjelmassa huomautettiin, että uhrin oikeusasema ei ollut kovin hyvä. Vaikka uhri olisi tehnyt rikosilmoituksen, joutui hän vakuuttelemaan palveluntarjoajille ja perintäyryyksille, että hän ei aiheuttanut laskuja. (Identiteettiohjelma 2010, 85.) Työryhmän raportissa kiinnitettiin huomioita myös toimivaltaongelmaan, jonka syynä oli se, että ilman tietoverkon lokitietojen käsittelyä rikosentekijän jäljittäminen oli mahdotonta. Jos verkko-osoitteen käyttäjä ei ole asiakassuhteessa palveluntarjoajaan, epäilyllinen henkilöllisyys ei selviä verkko-osoitteella. Tilanne on tällöin se, että verkkoidentiteetti nauttii suurempaa suojaa kuin henkilö, joka on joutunut rikoksen uhriksi. (Identiteettiohjelma 2010, 81–82.)

Identiteettiohjelman suositukset koskivat esimerkiksi biometrisiä tunnisteita, tunnistamisasiakirjoja kuten ajokortteja ja ilmoitusjärjestelmän luomista identiteettivarkauksien osalta. Varsinaiseen henkilöllisyyden todentamista koskevaan lainsäädäntöön identiteettiohjelma ei paneutunut, sillä luottojen osalta tätä koskeva kuluttajansuojalain muutos oli käynnissä samaan aikaan, josta kerron tarkemmin seuraavassa kappaleessa.

3.2 Pikaluottotyöryhmän perustaminen

Noin vuosina 2005-2007 pikaluottoihin liittyvistä ongelmista jätettiin valtioneuvostolle useita kirjallisia kysymyksiä ja toimenpideohjeita ja kuluttajaviranomaiset julkaisivat useita tiedotteita vastaaviin ongelmiin liittyen (Valkama ja Muttilainen 2008, 9). Lokakuussa 2007 oikeusministeriö asettikin niin kutsutun pikaluottotyöryhmän, jonka tehtävä oli valmistella ehdotus pikaluottoihin liittyvän lainsäädännön muuttamisesta. Lainvalmistelu käynnistyykin ministeriössä lainvalmistelua koskevasta aloitteesta. Tällainen aloite voi olla esimerkiksi hallitusohjelman kirjaus tai ministeriön aloite esimerkiksi kerätyn tiedon, tutkimusten tai selvitysten taikka lainsäädännön täytäntöönpanon tai vaikutusten seurannan pohjalta. (Finlex) Tässä tapauksessa vaikutti siltä, että pikaluottoihin liittyvä keskustelu kävi kiivaana eri tahoilla jo ennen ministeriön työryhmän perustamista.

Ottaen huomioon sen, että opinnäytetyössäni käsittelen lainsäädännön muuttumiseen liittyviä syitä, on mielestäni syytä käydä lyhyesti läpi, miten lainvalmisteluprosessi etenee yleisellä tasolla. Näin lukijalle välittyy kuva siitä minkälaisen prosessin opinnäytetyössä käsitellyt lakimuutokset ovat käyneet läpi ennen niiden hyväksymistä ja minkä tahojen käsittelyssä esitykset käyvät. Näillä on kuitenkin merkitystä sen suhteen, minkälaiseksi valmis lainsäädäntö lopulta muodostuu.

Lainvalmistelun perusvalmistelu tehdään joko virkatyönä ministeriössä tai lainvalmisteluelimessä, joka taas on laajempi kokoonpano. Tässä tapauksessa lainvalmistelutyö tehtiin erillisessä lainvalmisteluelimessä, eli pikaluottotyöryhmässä, jossa oli mukana paljon muita tahoja kuin ministeriön virkamiehiä. Työryhmän edustukseen kuuluivat oikeusministeriö, valtiovarainministeriö, työ- ja elinkeinoministeriö, Kuluttajavirasto/kuluttaja- asiamies, Rahoitustarkastus, Finanssialan Keskusliitto ry, Suomen Kuluttajaliitto ry, Suomen Pienlainayhdistys ry sekä Velkaneuvonta ry (Työryhmämietintö 2008:7). Tämä vaihe valmistelusta on laajin, sillä se alkaa hankkeen toimeksiannosta ja päättyy siihen hallituksen esityksen luonnoksen valmistumiseen eli varsinaiseen lakiehdotukseen.

Tämän jälkeen esityksestä pyydetään lausuntoja erilaisilta asiaan liittyviltä sidosryhmiltä, joilta lausuntoja on voitu pyytää jo toki valmisteluvaiheessakin. Tällainen taho voi olla esimerkiksi Poliisihallitus. Lausuntojen perusteella ehdotukseen voidaan tehdä muutoksia. Kun varsinainen esitys on saatu kuntoon, viedään asia valtioneuvoston päätöksentekoon yleisistuntoon, jossa päätetään esityksen viemisestä eduskunnalle. Kun asia on viety eduskunnan käsittelyyn, käsitellään lakiesitystä erilaisissa eduskunnan valiokunnissa, jotka kuulevat asiaa valmistelleita virkamiehiä sekä muitakin aiheen asiantuntijoita. Eduskunta päättää lopuksi hyväksyykö vai hylkääkö se esityksen, jonka jälkeen presidentti päättää hyväksytyn lain vahvistamisesta. (Finlex.)

Pikaluottotyöryhmän mietinnön ehdotukset koskivat kiskontaa koskevaa rikoslain säännöstä, viivästyskorkoa koskevaa korkolain säännöstä ja kuluttajansuojalain 7. lukua, joka koski luottoja. Koko esityksen yleisenä tavoitteena oli vähentää pikaluottojen tarjonnassa esiintyneitä ongelmia. (Työryhmämietintö 2008:7.) Lakiesityksessä käsiteltiin siis paljon muitakin luotonantoon liittyviä ongelmia, mutta käsitellessäni tässä ainoastaan kuluttajansuojalain henkilöllisyyden todentamisvelvollisuuteen liittyviä muutoksia ja niitä koskevia perusteluja, kuten olen jo aiemmin todennut.

3.3 Ongelmat luotonhakijan tunnistamisessa

Pikaluottotyöryhmän perustamisen aikaan suurin osa luottosopimuksista tehtiin postin välityksellä. Luottolaitos lähetti asiakkaan väestötietojärjestelmään merkittyyn osoitteeseen luottosopimuksen allekirjoitettavaksi, jonka jälkeen asiakas palautti sopimuksen allekirjoitetun sekä henkilöllisyystodistuksesta otetun kopion kera. (HE 64/2009, 23.) Myös tekstiviestilainoja käytettiin ja tietävästi ensimmäinen tekstiviestiluotto myönnettiin jo vuonna 2005 (Parkkali ja Pönkä 2010, 585). Tunnistaminen perustui siihen, että oletettiin puhelimen käyttäjän olevan lainan hakemisen hetkellä kyseisen liittymän tilaaja. Lainan hakijan tietoja eli henkilötunnusta, nimeä ja osoitetta verrattiin väestorekisterikeskuksen ja numerotiedustelun tietoihin. (Tietosuojalautakunnan päätös nro 1/22.1.2008.) Asiakas kirjoitti viestiin lainasumman, laina-ajan sekä omat tietonsa ja tilinumeron. Yritys toimitti lainapäätöksen vastaamalla tekstiviestiin ja asiakkaan tuli vahvistaa se vielä uudella viestillä. Rahat tulivat tilille muutamassa minuutissa. (Valkama ja Muttilainen 2008, 11).

Lakiesityksessä katsottiin, että lainaa hakeneen henkilön henkilöllisyyden puutteellinen todentaminen oli mahdollistanut väärinkäytöksiä, joissa laina saatiin käyttämällä hyväksi toisen henkilön henkilötunnusta, osoitetta ja matkapuhelinta (HE 64/2009, 17). Sisäministeriön poliisiosaston mukaan poliisilla oli tutkittavanaan tapaus, jossa rikollisryhmä oli käyttänyt hyväkseen 60 ihmisen henkilötietoja ja saaneen yli 80 000 euron arvosta pikavippejä. Ryhmä käytti väärennettyjä ajokortteja, joiden avulla he sulkivat ihmisten puhelinliittymiä ja avasivat uusia, joilla pikavippejä epäiltiin nostetun. (Sisäministeriön poliisiosasto 2008.) Ryhmä avasi tiedoilla nopeita lainoja, tässä tapauksessa tarkoitetaan tekstiviestilainoja (Linnake, 2008). Myös tietosuojavaltuutettu oli kiinnittänyt huomiota tekstiviestilainoissa esiintyvään väärinkäyttöön mahdollisuuteen (Tietosuojalautakunnan päätös nro 1/22.1.2008). Kuluttaja-asiamieskin kiinnitti vuonna 2006 ja 2007 antamissaan luottoja koskevissa linjauksissaan huomiota luotonantajan vastuuseen sen suhteen, ettei lainaa saisi haettua toisen henkilötunnuksella (Parkkali ja Pönkä 2010, 585).

Koska pikaluottoja myöntäville luottolaitoksille ei ollut asetettu nimenomaista velvollisuutta henkilöllisyyden huolelliseen todentamiseen, poikkesivat lainanhakijan tunnistamismenetelmät toisistaan niiden luotettavuuden osalta. Tähän ongelmaan ei katsottu pystyvän puuttua muutoin kuin lainsäädännöllä. (HE 64/2009, 15.) Esimerkiksi vuonna 2008 tekstiviestiluottoja tarjosi kaikkiaan 50 yritystä, joista vain 10 yritystä käytti Tupas-tunnistamista asiakkaiden tunnistamisessa (Valkama ja Muttilainen 2008, 13). Ei ihme, että näin helpolla tavalla saataviin lainoihin kohdistui väärinkäytöksiä.

3.3 Kuluttajansuojalain muutos 2010

3.3.1 Luotonhakijan henkilöllisyyden todentaminen

Pikaluottotyöryhmän laatiman ehdotuksen seurauksena kuluttajansuojalain luottoja koskevaan lukuun tehtiin muutoksia, jotka tulivat voimaan 1.2.2010 (KSL 844/2009) ja ovat voimassa tälläkin hetkellä. Muutoksen seurauksena luotonantajan tuli todentaa lainanhakijan henkilöllisyys huolellisesti (KSL 7:15). Todentamisen tuli perustua luotettavaan viranomaisen antamaan asiakirjaan, joita katsottiin lakiesityksessä olevan ainakin passi ja henkilökortti. Jos todentaminen suoritettaisiin sähköisesti, tuli käyttää vahvaa tunnistautumismenetelmää (KSL 7:15).

Lisäksi säädettiin, että jos luotonantaja oli jo huolellisella tavalla todennut kuluttajan henkilöllisyyden, voitiin henkilöllisyys todentaa myös henkilökohtaisesti laaditun tunnisteiden avulla (KSL 7:15). Tämä katsottiin tarpeelliseksi, jotta tekstiviestilainoja voitaisiin vielä hakea, kun mobiilivarmenteita ei vielä tuohon aikaan ollut (HE 64/2009, 17). Esimerkkinä henkilökohtaisesta tunnisteesta mainittiin turvakoodi (HE 64/2009, 24).

Säädösmuutosta ennen luotonantajilla ei ollut lainsäädännössä nimenomaista velvollisuutta tunnistaa tai todentaa asiakasta. Luottolaitoksille oli kuitenkin vakituista asiakassuhdetta perustettaessa velvollisuus tunnistaa asiakas sekä todentaa tämän henkilöllisyys rahanpesun ja terrorismin rahoituksen estämiseksi ja selvittämiseksi. Erona rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä koskevasta lainsäädännöstä tuleviin velvoitteisiin oli se, että nyt muutettu kuluttajansuojalain säännös ei pohjautunut riskiperusteiseen arviointiin. Lisäksi tarkoituksena oli estää väärinkäytöksiä lainanotossa, eikä rahanpesua ja terrorismin rahoittamista kuten edellä mainitussa laissa. (HE 64/2009, 17.)

Muutos koski rahaluottoja ja hyödykesidonnaisia tililuottoja. Soveltamisalan ulkopuolelle jäivät siis hyödykesidonnaisen kertaluotot, joita tyypillisesti myytiin postimyynnin yhteydessä. Kuluttajaviraston tietojen mukaan tällaisissa luotoissa ei ollut esiintynyt väärinkäytöksiä samalla tavalla kuin pika-luotoissa, joten muutosta ei tämän vuoksi ulotettu koskemaan niitä. (HE 64/2009, 17.)

Kuluttajansuojalain mukaan luottoja koskevia säännöksiä valvovat kuluttajaviranomaiset (mm. kuluttaja-asiamies) sekä Finanssivalvonta silloin kun luotonanto liittyy sen valvomaan toimintaan (KSL 7:24) Uutena momenttina ehdotuksessa lisättiin Viestintävirastoa eli nykyistä Traficomia koskeva velvoite, jonka mukaan sen tuli antaa valvontaviranomaisen pyynnöstä tarvittaessa lausunto siitä, oli käytetty sähköinen todentamismenetelmä vahva tunnistamismenetelmä. Näin ollen Viestintävirasto toimi ikään kuin asiantuntija-apuna teknisen vaatimuksen valvonnan osalta.

3.3.2 Ehdotusta koskeva lausuntopalaute

Eduskunnan käsittelyssä ei henkilöllisyyden todentamisvelvollisuus aiheuttanut suurempaa keskustelua kansanedustajien keskuudessa, ja jos se keskustelussa esiin nousi, sitä kannatettiin (PTK 91/2009, PTK 92/2009, PTK 95/2009). Ennen eduskunnan käsittelyä työryhmän mietinnöstä pyydettiin kuitenkin lausuntoja eri tahoilta, jotka pääosin kannattivat ehdotusta. Keskusrikospoliisi piti lausunnossaan ehdotuksia tarpeellisina (Keskusrikospoliisi 2008), kuten piti myös sisäministeriön poliisiosasto, joka uskoi ehdotuksen todennäköisesti vähentävän väärinkäytöksiä (Sisäministeriön poliisiosasto 2008).

Yleisesti annetuissa lausuntovastauksissa korostuivat erityisesti väärinkäytösten todellinen laajuus. Suomen Pienlainayhdistyksen mukaan ongelmia tunnistamisen suhteen oli liioiteltu. Tunnistamisvirheitä tapahtui sen mukaan keskimäärin yksi per viisi tuhatta lainaa ja niissäkin tapauksissa kyse oli rikollisesti toiminnasta eli identiteettivarkauksesta. (Työryhmämietintö 2008:7.) Talousvaliokunnan mukaan esityksen käsittelyaikaan vuonna 2008 pikavippejä myönnettiin noin miljoona, joten tunnistamisvirheitä tällä logiikalla myönnettyjen lainojen määrästä oli vain noin 200 kappaletta. (TaVM 13/2009, 7). Rahoitusyhtiö GE Money totesi lausunnossaan, että väärinkäytökset pelkkään henkilöllisyyden todentamiseen liittyen olivat olleet harvassa ja kyse oli identiteettivarkauksista (GE

Money 2009). Helsingin Käräjäoikeus kiinnitti niin ikään huomiota siihen, ettei mietinnössä ilmennyt kuinka paljon väärinkäytöksiä henkilöllisyyden todentamisessa ilmenee. Käräjäoikeus pohti, oliko tarkoituksenmukaista säätää vahvan sähköisen tunnistautumisen vaatimus, joka edellyttäisi suuria järjestelmäinvestointeja, mikäli väärinkäytökset olivat vähäisiä. (Helsingin Käräjäoikeus 2008.) Myös Suomen Yrittäjät ry totesi, että ei ilmennyt kuinka laaja ongelma identiteettivarkaudet pika-luottojen osalta oli ja katsoi, että tätä tulisi jatkovalmistelussa selvittää (Suomen Yrittäjät ry 2008). Edellä esiin nostetuissa lausunnoissa ilmeni mielestäni se, ettei väärinkäytösten katsottu olevan tarpeeksi mittavia suhteessa lakiehdotuksen seurauksiin. Hyöty-haittasuhde ei siis ollut perusteltu.

Suomen Pienlainayhdistys, joka vastusti ehdotusta, katsoi, että ehdotettu muutos lainanhakijan henkilöllisyyden vahvasta sähköisestä todentamisesta loukkasi kokonaisuudessaan kuluttajien oikeutta valita heille parhain tapa raha-asioittensa hoitamiseen sekä asetti heitä eri arvioiseen asemaan (Työryhmämietintö 2008:7). Näin lausui myös GE Money ja syynä kannanottoon oli se, että kuluttajat olivat sidottuna pankkien tunnuksiin ja monilla tunnuksia ei edes ollut. Lisäksi GE Money lausui, että esimerkiksi perheenjäsenillä tunnukset saattoivat olla eri paikoissa, jolloin he eivät teknisesti pystyisi hakemaan pankin ulkopuoliselta luoton tarjoajalta lainaa. (Ge Money 2008.) Näiden ehdotuksen vastustamista koskevien kommenttien taustalla uskon olleen ajatuksen siitä, että vahvan sähköisen tunnistamisen vaatimukset vaikeuttaisivat lainanmyöntäjien markkinoita. Pienlainayhdistys lausui myös Helsingin Sanomille, että yksi syy ehdotuksen vastustamiseen oli se, että he eivät halunneet antaa vahvan sähköisen tunnistamisen järjestelmälle yksinoikeutta, koska pankit alkaisivat periä kallista hintaa niistä (Savolainen 2009).

Kantaa otettiin erityisesti myös siihen, että kenen vastuulla tällaiset väärinkäytökset olivat. Keskuskauppakamari ei pitänyt tarpeellisenä työryhmän ehdottamaa pakollista vahvaa tunnistautumista sillä perusteella, että tunnistamisessa tapahtunut virhe on luotonmyöntäjän vastuulla, koska asiakas ei vastaa luotosta, jos se oikeudettomasti on hänen tiedoillaan haettu (Keskuskauppakamari 2008). Myös Suomen Pienlainayhdistys kiinnitti huomiota siihen, että luotonantaja ottaa vastatakseen kaikista kustannuksista ja toimenpiteistä ei uhri näin ollen joudu kärsimään. (Työryhmämietintö 2008:7). Suomen Yrittäjät kiinnitti huomioita siihen, että toisen tiedoilla matkapuhelimella tilattu laina täyttää usein rikoksen tunnusmerkistön eikä se, jonka henkilötietoja ole käytetty, ole ollenkaan sidottu oikeustoimeen. (Suomen Yrittäjät ry 2008). Ymmärrän lausunnot siten, että koska väärinkäytöstapauksissa ei sopimus kuitenkaan sitoisi kuluttajaa, ei vahvan tunnistautumisen vaatimus olisi ollut tarpeellinen. Tietosuojavaltuutettu lausui kuitenkin painokkaasti, ettei toimintaa, joka identiteettivarkaudet mahdollistavat, voida pitää lainmukaisena eikä hyväksyttävänä (Tietosuojavaltuutetun toimisto 2008).

Vastaavasti lausunnoissa sekä asiaa käsitelleissä valiokunnissa kiinnitettiin kuitenkin huomioita myös uhrin asemaan väärinkäytöstilanteissa. Talousvaliokunta ja lakivaliokunta katsoivat, että

vaikka virheet ovat lainan myöntäjän vastuulla, aiheutuu tästä kuitenkin harmia ja haittaa niille, joiden nimissä luotto on otettu (TaVM 13/2009, 4 ja LaVL 12/2009, 3). Sisäministeriön poliisiosasto korosti fyysisen ensitunnistamisen merkitystä ja kiinnitti huomiota jo aiemmin mainitsemaani väärennyillä ajokorteilla tehtyyn rikossarjaan, jossa lainoja haettiin tekstiviestillä. Poliisiosasto huomioi myös sen, ettei identiteettivarkauksia koskevaa lainsäädäntöä ole Suomessa ja kansalaisten oikeuksiin ja eri osapuolten vastuisiin kohdistuukin merkittävä uhka sähköisessä tunnistamisessa. Poliisiosaston mukaan tulisi selkeästi kertoa oikeudet ja vastuut, jotka kansalaisiin kohdistuu. (Sisäministeriön poliisiosasto 2008).

3.4 Laki vahvasta sähköisestä tunnistamisesta ja allekirjoituksista

Osittain samanaikaisesti pikaluottoja koskevan lainsäädäntömuutoksen kanssa oli liikenne- ja viestintäministeriössä valmisteilla jo aikaisemmin mainittu laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista eli tunnistuslaki, joka tuli voimaan 1.9.2009 eli vuosi ennen KSL:n muutoksen voimaantuloa. Säädös korvasi lain sähköisistä allekirjoituksista (14/2003). Ehdotus sisälsi ne edellytykset, jotka määrittelivät tunnistautumisen vahvaksi (HE 64/2009, 17). Lain tarkoituksena oli edistää sähköistä tunnistamisen palveluiden tarjoamista, luoda säännökset niiden tarjontaan sekä varmistaa, että tunnistamisessa otetaan huomioon riittävä tietoturvan ja tietosuojan taso (HE 36/2009, 29). Lakiehdotuksessa todettiin, että sähköisen tunnistautumisen menetelmissä identiteettivarkaudet olivat helpommin torjuttavissa kuin heikon tunnistautumisen menetelmissä. (HE 36/2009, 9).

Lain taustalla oli syyskuussa 2008 liikenne- ja viestintäministeriön tietoyhteiskunnan neuvottelukunnan alaisuuteen perustettu sähköisen tunnistamisen kehittämissyhmä. Ryhmä julkaisi kansalliset linjaukset maaliskuussa 2009, jotka kuvasivat vahvan sähköisen tunnistamisen jatkokehittämisen toimintaympäristöä (Valtioneuvoston periaatepäätös 2009, 2). Periaatepäätöksessä todettiin, että henkilöllisyyttä suojataan välillisesti usein eri säädöksin, mutta sääntely ei ole kattavaa. Päätöksen mukaan lainsäädäntöä saatetaan tarvita tapauksissa, jossa tietoverkkorikollisuuteen liittyy henkilöllisyyden väärä käyttäminen. (Valtioneuvoston periaatepäätös 2009, 9.) Näiden periaatteiden pohjalta tunnistamislaki laadittiinkin.

Periaatepäätöksen mukaan verkkorikollisuuden todettiin olevan suuremmissa määrin piilorikollisuutta. Todettiin myös, että kansalaisen itse ei voida olettaa olevan tietoturvan asiantuntija, jonka vuoksi tunnistautumismenetelmän, jota kansalaiselle tarjotaan, tulisi olla luotettava. Henkilöllisyyden suojaamisen todettiin olevan kansalaisen perustavanlaatuinen oikeus. Päätöksen mukaan väärän henkilöllisyyden käyttäminen ja tietojen anastaminen tulisi pystyä estämään tehokkaalla tavalla. (Valtioneuvoston periaatepäätös 2009, 9.)

3.5 Muutoksen voimaantulon vaikutukset

Edellä käsitellyllä kuluttajansuojalain muutoksella arveltiin säädösvaiheessa olevan positiivisia vaikutuksia rikoksantorjuntaan ja turvallisuuteen (HE 64/2009, 21). Lain voimaantullessa oli pikaluotto-yhtiöitä arvion mukaan kokonaisuudessaan yli 100 kappaletta, mutta liikevaihtoja tarkastellessa toiminta näytti keskittyvän noin kymmenen suurimman yhtiön ympärille. (Parkkali ja Pönkä 2010, 586). Lain voimaantulon jälkeen toteutetussa valvonnassa keväällä 2010 kävi ilmi, että vain 30 yritystä 80:stä tunnisti luottoa hakevan voimaantulleen lain vaatimusten mukaisesti. Asiakkaan annettiin esimerkiksi valita käyttääkö hän pankkitunnuksiaan vai ei, eli vahvaa sähköistä tunnistautumista ei aina vaadittu. (Parkkali ja Pönkä 2010, 603). Kuluttajavirasto ja tietosuojavaltuutettu lähettivät valvontakampanjan jälkeen säännöksiä rikkoville yrityksille kirjeitä ja osa yrityksistä korjasikin toimintatapojaan. Tietosuojavaltuutettu joutui kuitenkin viemään osan yrityksistä tietosuojalautakuntaan, jotka tunnistivat puutteellisesti lainanhakijan henkilöllisyyden. (Savolainen 2010.)

Pikaluottoyrityksillä oli ennen lakimuutoksia vaikeuksia saada Tupas-varmenteita, mutta Finanssialan Keskusliiton periaatelinjaus helpotti tätä, koska sen takia pikaluottoyritysten mahdollisuudet saada Tupas-varmenteita helpottuivat. Keskusliiton periaatteet asettivat tiettyjä edellytyksiä, joiden vallitessa pankki saattoi kieltäytyä sopimuksesta palveluntarjoajan eli tässä tapauksessa luottolaitoksen kanssa. Ennen lain voimaantuloa arveltiinkin jo Tupas-varmenteiden myöntämisen ongelmien katoavan muutoksen myötä. (HE 64/2009, 20). Käytännön tasolla vahva sähköinen tunnistaminen oli siis nyt lainanmyöntäjille entistä helpompi toteuttaa.

Oikeustieteellisessä kirjallisuudessa esitettiin kritiikkiä säädösmuutosten tarpeellisuudesta. Katsottiin, että vähäisten tunnistamisvirheiden määrän vuoksi säännöksen lisääminen kuluttajansuojalakiin ei olisi ollut välttämätöntä, mutta sillä oli kuitenkin ennalta ehkäisevää vaikutusta ja ylisääntely oli parempi kuin epäkohtiin puuttumatta jättäminen. (Parkkali ja Pönkä, 2010, 603.) Lisäksi lausuttiin, että ennakkovalvonta eli luotonantajiin kohdistuva tunnistamisvelvollisuus oli oikeustaloustieteellisestä näkökulmasta kyseenalainen. Vaihtoehtoisesti esitettiin, että asia olisi voitu ratkaista asia jälkivalvonnalla, sitten kun väärinkäytöksiä oli jo tapahtunut. Pohdittiin myös sitä, että oliko lainsäätäjä yliarvioinut väärinkäytösten yleisyyden määrän sen jälkeen, kun on saatu enemmän tietoa yksittäistä tapauksista. (Määttä 2010, 40).

Samana vuoden lopulla kuluttajansuojalaki muutettiin jälleen ja 1.12.2010 voimaantulleeseen muutoksen pohjalla olivat muutoksia EU:n kulutusluottodirektiivin (Euroopan parlamentin ja neuvoston direktiivi 2008/48/EY kulutusluottosopimuksista ja neuvoston direktiivin 87/102/ETY kumoamisesta) vaatimukset, jotka eivät kuitenkaan koskeneet henkilöllisyyden todentamista. Kuluttajansuojalakiin lisättiin kuitenkin pykälä hyvästä luotonantotavasta, jonka mukaan luotonantajan oli luotonannossa meneteltävä vastuullisesti (747/2010, KSL 7:13). Hallituksen esityksen mukaan säännös ulottui

kaikkiin luottosuhteen vaiheisiin ja se täydensi esimerkiksi henkilöllisyyden todentamista koskevaa säännöstä (HE 24/2010, 33). Säännöksellä korostettiin näin ollen mielestäni luotonantajan vastuuta entisestään.

4 SÄÄNTELYN PÄIVITTÄMINEN

4.1 Verkon muuttunut toimintaympäristö

Poliisihallitus on kritisoinut maksupalvelun välittäjiä ja luotonantajien toimia sen suhteen, että toimet petosrikollisuuden ja identiteettivarkauksien estämiseksi eivät ole olleet riittäviä. Vaikka lainsäädäntö ei ole asettanut nimenomaisia esteitä, eivät nämä edellä mainitut toimijat ole ottaneet käyttöön vahvaa sähköistä tunnistautumista. (POL-2022-30164, 2.) Tilauspetosten helppoudesta on kirjoittanut muun muassa Yle, jonka vuonna 2021 tekemän testin mukaan ruotsalaisen maksunvälitysfirman Klarnan järjestelmässä oli ongelma, joka mahdollisti asiakkaiden tilin käyttämisen petoksiin ja identiteettivarkauksiin. Testissä tilattiin tavaroita viiden henkilön nimissä viidestä eri verkkokaupasta ja maksutavaksi valittiin Klarnan laskutuspalvelu, jossa tilaus maksetaan 14 päivän kuluessa. Ensimmäisen tilauksen yhteydessä tulee tehdä vahva tunnistautuminen, mutta sen jälkeen tilauksen tekemiseen riittää sähköposti ja postinumero. Tämän vuoksi Klarnalta pystyi tilaamaan tavaraa toisen nimiin, kunhan on vain sähköposti ja postinumero tiedossa. Ylen tietojen mukaan tuotteiden tilaaminen onnistui jopa silloin, vaikka tiliä ei ole Klarnaan luotu, mutta kunhan tilauspetoksen uhri on joskus maksanut Klarnan kautta. Ylen mukaan kymmenen vuoden aikana aikavälillä 2011–2021 Klarna oli ollut asianomistajana tai muussa roolissa yli 1500 rikostapauksessa, joissa yli puolessa oli kyse petosrikoksista. (Hänninen 2021.)

Yle tutki myös alkuvuonna 2021 lähes neljäsataa Helsingin käräjäoikeuden rikossyytettä, jossa oli käytetty vääriä henkilötietoja ja luotto-ostoksia nettikaupoissa. Selvityksen mukaan syytteistä ilmeni, että tavaroiden hankkiminen toisen tiedoilla kävi helposti. Helpoiten tavaraa sai tilattu Klarnan ja Qliron kautta. Klarnan osalta se vaatii vain osalta luottoasiakkaista vahvan tunnistautumisen. Qliron Ylelle antaman vastauksen mukaan henkilökuntaa koulutetaan estämään epäilyttävät tilaukset, mutta Ylen testissä tilaaminen tunnistautumatta onnistui helposti. (Hämäläinen 2021.)

DDV antoi Vastaamon tietomurron jälkeen suosituksen, jonka mukaan kaikissa verkkopalveluissa tulisi käyttää vahvaa sähköistä tunnistamista, jolla voidaan huonontaa identiteettivarkauksien onnistumista (DDV 2020). Kuten voimme huomata, näin ei ole kuitenkaan palveluntarjoajien toimesta toimittu. Vastaamon tietomurron tutkinnanjohtaja Marko Leposen mukaan poliisissa on tietomurron jälkeen seurattu tarkasti, aletaanko tietovuodon uhrien henkilötietoja käyttää esimerkiksi petoksiin. Helmikuussa 2022 Leponen tiedotti, että tällaisia rikoksia on alkanut ilmaantua. Seurannassa oli havaittu noin sadan henkilön henkilötietoja käytetyn väärin erilaisissa rekisteröinneissä. Leposen

mukaan huolena oli erityisesti se, että näitä käytetään jatkossa tilauspetosten tekemiseen. (Leponen 2022.) Henkilötietoja oli käytetty muun muassa kauppapaikkapalveluihin ja pikavippien ottamisessa. Seurannassa havaittiin, että suurin osa väärin tietojen hyväksikäytöistä oli tapahtunut sivustoilla, joissa ei vaadittu vahvaa sähköistä tunnistautumista, vaan tunnistautuminen tapahtui esimerkiksi henkilötunnuksella. Leponen on kommentoinut, että laajentamalla vahvan tunnistautumisen käyttöönottoa voidaan tehostaa tällaisten rikosten torjuntaa. (Leponen 2022.) Toisten tietoja väärinkäyttämällä tehdyt rikokset ovat siis kasvaneet ja palveluntarjoajien riittämättömät tunnistamisvaatimukset ovat olleet näitä mahdollistamassa.

4.2 Kuluttajaluottotyöryhmän perustaminen

Kuluttajaluottosäntely on ollut kokonaisuus, jonka kokonaisvaltaisempaan muuttamiseen on ollut painetta jo pidemmän aikaa. Pääministeri Sanna Marinin hallitusohjelman erityisenä teemana on ollut ylivelkaantumisen ja siihen liittyvien ongelmien vähentäminen. Hallitusohjelman mukaan 2015–2019 hallituskaudella hyväksytyyn kuluttaja- ja pikaluottoja koskevan säntelyn tehokkuutta seurataan. Mikäli siinä havaitaan puutoksia, on hallitusohjelman lausuman mukaan ryhdyttävä toimenpiteisiin säntelyn tehostamiseksi. (Marinin hallitusohjelma 2019, 82.)

Heinäkuussa 2021 oikeusministeriö asettikin asettamispäätöksellä niin sanotun kuluttajaluottotyöryhmän, jonka tarkoituksena oli valmistella kuluttajaluottoja koskeva lainsäädännön muutos. Kuluttajaluottotyöryhmän muodostivat oikeusministeriön lisäksi työ- ja elinkeinoministeriö, valtionvarainministeriö, Finanssivalvonta, Kilpailu- ja kuluttajavirasto / kuluttaja-asiamies, Finanssiala ry, Kaupan Liitto ry, Kuluttajaliitto sekä Suomen Asiakkuusmarkkinointiliitto ry. Pysyvänä asiantuntijana työryhmässä toimi lisäksi tietosuojavaltuutetun toimisto. (HE 218/2022, 5).

Asettamispäätöksen mukaisesti työryhmän tuli valmistella hallituksen esityksen muotoon laadittu ehdotus päätöksessä esitettyjen linjausten mukaisesti. Yksi linjauksista oli henkilöllisyyden todentamisvelvollisuuden laajentaminen koskemaan mahdollisuuksien mukaan kaikkia kuluttajaluottosopimuksia sekä verkkokauppojen laskutuspalveluja sekä säntelyn ajantasaisuuden arviointi muillakin osin. (Kuluttajaluottotyöryhmän asettamispäätös 2021.) Vuonna 2010 voimaantulleen todentamista koskevan säntelymuutoksen katsottiin työryhmän puolesta toimineen suhteellisen hyvin. Kuitenkaan verkkokaupan ja ylipäättään digitaalisessa muodossa käytävän kaupankäynnin lisääntymisen ja kasvun myötä säntelyn ei ole katsottu vastaavan nykyajan tarpeita. (HE 218/2022, 23.) Esityksestä käy mielestäni ilmi se, että säntelyä on tarpeen myös laajentaa. Osana kuluttajaluottosäntelyä otettiin siis käsittelyyn myös todentamista koskeva säntely, joka oli puhututtanut erityisesti Vastaamon tietomurrosta saakka.

Työryhmätyöskentelyn pohjalta valmistui lokakuussa 2022 annettu hallituksen esitys laeiksi kuluttajansuojalain, kuluttajaviranomaisten eräistä toimivaltuuksista annetun lain 13§:n ja oikeudenkäymiskaaren 5 luvun 3§:n muuttamisesta 218/2022 (HE 218/2022, 5). Lakiesitys vahvistettiin 22.3.2023 ja muutos kuluttajansuojalain 7. kappaleeseen (449/2023) tulee voimaan 1.10.2023 alkaen. Muutoksista ja niiden perusteluista kerron tarkemmin seuraavassa kappaleessa.

4.3 Kuluttajansuojalain muutos 2023

4.3.1 Lainanhakijan henkilöllisyyden todentaminen

Tällä hetkellä voimassa olevan kuluttajansuojalain mukaisesti lainanhakija pitää tunnistaa huolellisesti ennen luottosopimuksen tekemistä ja sähköisessä tunnistamisessa pitää käyttää vahvaa tunnistamista. Nyt voimaantulevassa muutoksessa vahvaa tunnistautumista edellytettäisiin myös luottorajaa sekä luoton määrää korottaessa ja uutta luottoa haettaessa. Tämä tarkoittaa siis sitä, että ei ole riittävää, että asiakas tunnistetaan verkkopankkiin kirjautuessa, vaan vahva tunnistautuminen on tehtävä uudelleen vielä luottoa koskevissa muutoksissa. (HE 218/2022, 27.) On arvioitu, että tämä muutos voi ehkäistä väärinkäytöksiä, joissa asiakkaan verkkopankkiin on onnistuttu kertaluontoisesti kirjautumaan oikeudettomasti. Väärinkäyttö voi täten paljastua asiakkaalle luoton muuttamista hakiessa. On kuitenkin huomattava, että tämä ei vähennä sellaisia väärinkäytöksiä, joissa tunnistusvälineet ovat niitä oikeudettomasti hallussa pitävän käytössä jatkuvasti, eikä vain kertaluontoisesti. (HE 218/2022, 35.) Osa luotonantajista vaatii uudelleentunnistautumista jo tälläkin hetkellä, mutta muutos ulottaisi velvollisuuden kaikkiin luotontarjoajiin (HE 218/2022, 35).

Nykyiseen sääntelyyn eivät sisälly hyödykesidonnaiset kertaluotot, koska kuten aiemmin mainittiin, niitä myönnettiin lähinnä postimyynnin yhteydessä eikä niissä esiintynyt väärinkäytöksiä kuten pikaluotoissa. Hyödykesidonnaisilla luotoilla tarkoitetaan sitä, että tavaraa ostetaan netistä velaksi eli myöhemmin maksettavaksi. (Järvinen 2022, 171.) Olennaista on se, että luotto on sidottu tietyn hyödykkeen maksamiseen eikä siten, että luoton käyttötarkoitus on kuluttajan itse määrättävissä (Terämaa 2001, 313). Ehdotuksessa säännösten soveltamisala on laajennettu myös hyödykesidonnaisiin kertaluottoihin.

Muutoksella poistetaan henkilöllisyyden todentaminen ensitunnistamisen jälkeen luodulla henkilökohtaisella tunnisteella, kuten pin-koodilla. Kyseessä on ollut heikko tunnistamismenetelmä, joka on ollut tarpeen, koska tekstiviestilainoja ei olisi voitu muuten myöntää mobiilivarmenteiden vielä puuttuttua. Esityksessä todetaan, että tekstiviestilainoja ei tiettävästi enää myönnetä, joten tätä mahdollisuutta ei ole enää aiheellista laissa säilyttää. (HE 218/2022, 27).

4.3.2 Verkko-osto laskulle

Nykyinen tunnistamista koskeva sääntely ei koske tilanteita, joissa kuluttaja valitsee maksutavaksi laskun, josta ei peritä korkoa tai muita maksuja eli nämä eivät ole edes kuuluneet kuluttajansuojalain luottoja koskevan sääntelyn soveltamisalaan. Tällaisissa maksutilanteissa saatetaan käyttää esimerkiksi henkilötunnusta tai muita tietoja asiakkaan tunnistamiseen, jotka taas esityksen arvion mukaan väärissä käsissä ovat väline verkkokauppapetoksiin. Esityksessä korostetaan, että tosiasiallisesti henkilötunnus voi olla muidenkin henkilöiden tiedossa, jolloin henkilötunnuksia voidaan käyttää verkkokauppapetoksissa. (HE 218/2022, 23). Näin on ollutkin, kuten aiemmin esiin tuomani Ylen testi hyvin tuo esiin.

Tässä kohdin voidaan huomauttaa, että suurimpaan osaa maksutavoista sisältyy jo nykyisinkin velvollisuus tunnistaa asiakas käyttämällä vahvaa tunnistamismenetelmää (HE 281/2022, 51).

14.9.2019 voimaan tullut maksupalveludirektiivi PSD2 (Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/2366, annettu 25 päivänä marraskuuta 2015, maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/110/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta) toi muutoksia henkilöllisyyden todentamisvelvollisuuteen verkkokauppojen ja mobiilimaksamisen osalta, jolloin asiakkaan vahva sähköinen tunnistaminen sähköisissä maksutapahtumissa tuli pakolliseksi. Ennen direktiiviä maksaminen verkkokauppassa saattoi perustua pelkästään kortin tietoihin, eli kortin numeroon, voimassaoloaikaan ja cvc-koodiin (Finanssiala 2019). Muutosten taustalla oli käyttäjien turvallisen tunnistautumisen takaaminen ja petosten riskien vähentäminen (PSD2 johdanto-osa, kohta 95).

Direktiivi pantiin Suomessa täytäntöön maksupalvelulaila (290/2010). Vahva sähköinen tunnistaminen tuli vaatimukseksi kaikkeen sähköiseen maksamiseen 1.1.2021 alkaen siirtymäajan jälkeen (Finanssiala 2019). Maksupalvelulain 10. luvun 85 c §:n mukaan palveluntarjoajan on käytettävä vahvaa tunnistamista, jos maksaja: 1) käyttää maksutiliään tietoverkon välityksellä; 2) käynnistää sähköisen maksutapahtuman; tai 3) toteuttaa etäkanavan kautta toimen, johon voi liittyä väärinkäytöksen riski. Vaatimuksessa on poikkeuksia esimerkiksi pienten maksujen osalta (Finanssiala 2019).

Näin ollen, kun verkossa maksetaan maksukortilla, joutuu käyttäjä tekemään tämän lisäksi vielä vahvan sähköisen tunnistamisen. Sen sijaan laskulle on voinut edelleen tilata vapaasti. (Järvinen 2022, 171). Voimaantulevassa kuluttajansuojalain muutosesityksessä onkin katsottu, että asiakkaan vahvaa tunnistamista koskeva velvollisuus tulee laajentaa myös tilanteisiin, jossa kuluttaja valitsee verkossa maksunlykkäystä tarkoittavan maksutavan ja joissa ei sovelleta jo kuluttajansuojalakia tai maksupalvelulakia. Käytännössä tämä tarkoittaa siis laskua. (HE 218/2022, 27.) Verkossa hyödykkeiden ostamisella tarkoitetaan kaikenlaista sähköisessä ympäristössä harjoitettavaa

etämyyntiä, riippumatta siitä tapahtuuko se esimerkiksi mobiilisivustolla, sosiaalisessa mediassa tai tietyn sovelluksen sisällä (HE 218/2022, 50). Säännös koskee siis vain hyödykkeiden ostamista verkossa ja siten ehdotetun pykälän mukaan, jos kuluttaja ostaessaan hyödykkeitä verkossa valitsee maksutavan, joka merkitsee maksunlykkäystä, kyseistä maksutapaa tarjoavan elinkeinonharjoittajan on todennettava kuluttajan henkilöllisyys maksutavan hyväksymisen yhteydessä käyttämällä tunnistusmenetelmää, joka täyttää tunnistamislain tai maksupalvelulain vahvan tunnistamisen vaatimukset (449/2023).

Säännöksen ulkopuolelle on rajattu tiettyjä tilanteita. Ulkopuolelle jäävät tapaukset, joissa kuluttaja maksaa hinnan vasta tavaran luovuttamisen yhteydessä. Tätä poikkeuksen tuomista säännökseen perusteltiin sillä, että tällaiseen maksutapaan ei liity samalaista väärinkäytösriskiä, kuin laskulla. (HE 218/2022, 51). Toisen poikkeuksena säännöksen soveltamisalan ulkopuolelle rajataan palvelun suorittaminen etäviestimellä, kun laskua tarjotaan suoraan palveluntarjoajan puolesta. Tällaisia palveluita ovat esimerkiksi kotitalouspalvelut ja asianajopalvelut, joissa palvelusta sovitaan etukäteen verkon välityksellä, mutta ne tuotetaan henkilökohtaisena palveluna. Niin ikään näissä tilanteissa väärinkäytösriski on arvioitu pieneksi. (HE 218/2022, 51–52.) Alkuperäisessä kuluttajaluotto-työryhmän muistiossa nämä vielä kuuluivat sääntelyn alaan, mutta esimerkiksi Suomen Yrittäjät lausuiivat, että tunnistamisvelvollisuuden ei tulisi koskea tällaisia tilanteita. Sääntelyä muutettiin lopulliseen hallituksen esitykseen. (HE 218/2022, 47.) Kolmanneksi ulkopuolelle on rajattu hyödykkeen hankkiminen puhelinmyynnissä. Tämä on otettu esille sen vuoksi, että joskus ostoprosessi puhelinmyynnissä voi siirtyä verkkoon, jolloin se muutoin tulisi nyt ehdotetun sääntelyn soveltamisalan piiriin. On kuitenkin katsottu, että riski sellaisille väärinkäytöksille, jossa kuluttaja ei olekaan sanomansa henkilö, on tässäkin hyvin pieni, koska myyjä ottaa yhteyttä kuluttajaan itse. (HE 218/2022, 52.)

4.4 Ehdotusta koskeva lausuntopalaute

Ehdotusta pidettiin lausuntovastauksissa pääosin hyvänä. Takuusäätiön lausunnon mukaan toisen henkilön nimellä ja henkilötunnuksella verkkokaupasta ostaminen on ollut liian helppoa ja yksinkertaista (Takuusäätiö 2022). Poliisihallitus lausui, että tilauspetokset voitaisiin pääosin estää sillä, että ehdotuksessa mainituissa tilanteissa kuten maksunlykkäystä ja luottoa hakiessa vaadittaisiin aina henkilöllisyyden todentamista vahvalla tunnistautumisella (POL-2022-30164, 1). Poliisihallituksen mukaan henkilön vahvojen tunnistautumistietojen hankkiminen on merkittävästi vaikeampaa kuin pelkän henkilötunnuksen ja nimen. Henkilötunnuksia ja nimiä kun on verkossa melko helposti saatavilla ja sitä kautta hyödynnettävissä tilauspetosten aikaansaamiseksi. (POL-2022-30164, 2.) Vaikka Poliisihallitus piti ehdotuksen vaikutuksia rikostorjuntaan ja turvallisuuteen pääosin oikeana, uskoo se, ettei vahva tunnistaminen sinänsä vaikuttaisi kalasteluyritysten kasvuun (POL-2022-30164, 1).

Talousvaliokunnalle annetuissa lausunnoissa kannatettiin pääasiassa tunnistamisvelvollisuuden laajentamista. Klarna oli myös tällä kannalla, mutta lausui, että esityksen myötä vahva asiakastunnistautuminen aktivoitaisiin käytännössä jokaisessa verkko-ostoksessa, johon liittyy minkäänlainen maksunlykkäys, joka taas aiheuttaisi kohtuutonta kitkaa kuluttajalle verkkokaupan ostokokemuksessa ja lisäisi merkittävästi elinkeinoharjoittajien velvoitteita ja siten kustannuksia. Tämän vuoksi Klarna on ehdottanut lausunnoissaan, että vahvalle tunnistautumiselle asetettaisiin jonkinlainen raja-arvo. Klarnan lausunnon mukaan kuluttajalle ei käytännössä synny rahallista riskiä tilattaessa ostokset laskulle, ja vastuu väärinkäytöksistä on viime kädessä verkkokaupalla ja maksupalvelun tarjoajalla. (Klarna 2022.) Myös Medialiitto ja Sanoma Media esittivät euromääräistä rajaa. Hallituksen esitykseen kuitenkin kirjattiin, että tällaista raja-arvoa ei pidetä perusteltuna, koska se synnyttäisi epäselvyyden siitä, miten rajaa tulkittaisiin toistaiseksi voimassa olevissa sopimuksissa ja muutenkin monimutkaistaisi sääntelyä. Lisäksi katsottiin, että pieniä summia tuskin edes maksetaan laskulla. (HE 218/2022, 47.) Oikeusministeriö kiinnitti omassa lausunnossaan huomioita Klarnan lausumaan ja lausui, että vaikka väärinkäytöstilanteessa elinkeinoharjoittaja ei voisiakaan esittää vaateita kuluttajaa kohtaan sellaisten oikeustoimen perusteella, jota hän ei ole tehnyt, aiheutuu tästä kuluttajille joka tapauksessa ylimääräistä vaivaa. Näin ollen oikeusministeriö ei kannattanut poikkeuksien soveltamisalan laajentamista. (Oikeusministeriö 2022a.)

Talousvaliokunta piti ehdotuksen muutoksia perusteltuina ja lausui, että sen saadun selvityksen perusteella väärinkäytökset sekä riskit väärinkäytöksistä ovat selvästi lisääntyneet verkkoasioinnissa. Näin ollen valiokunta katsoi, että niiden estäminen on myös elinkeinoharjoittajien etu. (TaVM 42/2022, 10.)

Eduskunnan lähetekeskustelussa talousvaliokuntaan sekä myöhemmissä eduskunnan käsittelyissä ei kansanedustajien keskuudessa herännyt enempää keskustelua todentamisvelvollisuuden osalta, vaan keskustelu keskittyi korkokaton alentamiseen luotonannossa (PTK 116/2022 vp, PTK 196/2022 vp, PTK 170/2022 vp, PTK 171/2022 vp).

4.5 Vastuu väärinkäytöksistä ja uhrien asema

Seuraamusten osalta ei luottoja koskevaan lukuun ole ehdotettu muutoksia voimassa olevasta sääntelystä. Seuraamuksena säännösten rikkomisesta on kuluttajansuojalain mukaan kielto jatkaa tai uudistaa kyseistä menettelyä. Lisäksi kiellon tehosteeksi voidaan asettaa uhkasakko. (KSL 7:50.) Myöskään vastuukysymykset eivät muuttuneet. Lakiesityksessä on mainittu, että viimesijainen velvollisuus henkilöllisyyden asianmukaisesta todentamisesta säilyy edelleen sillä, joka tarjoaa tunnistamista edellyttävää maksutapaa. Tyypillisesti asiakkaan henkilöllisyyden todentaakin myyjän puolesta erillinen palveluntarjoaja, mutta vastuu todentamisesta säilyy myyjällä. (HE 218/2022, 51.)

Käytännössä taloudelliset tappiot identiteettivarkauksien osalta jäävät kuitenkin usein luotonantajalle tai muulle organisaatiolle. (Informaatio-ohjauksen ja sidosryhmäyhteistyön suunnitelma – Toimenpidesuosituksat 2021, 12)

Vaikka periaatteellinen vastuu henkilöllisyyden oikeasta todentamisesta säilyy myyjällä, ei se poista uhreille aiheutunutta haittaa. Lakiesityksen perusteluissa onkin huomioitu, että rikosten uhrien mahdollisuudet henkilötunnuksen väärinkäyttöön liittyvien rikosten ehkäisemiin ovat rajatut, koska heillä ei useinkaan ole tietoa siitä, että tiedot ovat joutuneet väärin käsiin. Tietoja voidaan käyttää useamman kerran, ennen kuin asia ilmenee henkilötietojen oikealle omistajalle. Väärinkäytösten selvittämisestä aiheutuu haittaa ja jopa kustannuksia, vaikka mahdollisuus irtautua petoksen avulla tehdyistä sopimuksista olisikin mahdollista. (HE 218/2022, 23). Jos luottokortti ei ole esimerkiksi fyysisesti varastettu, ei uhri välttämättä edes hoksaa seurata verkkopankkia, jos sieltä on mennyt väärä maksu.

OP Median haastatteleman identiteettivarkauden uhrin mukaan hän sai viiden vuoden ajan perintäkirjeitä tilauksista, joita hän ei ollut tehnyt. Uhri lähetti laskut tutkintaa johtaneelle poliisille, joka liitti laskun liitteeksi uhrin tekemään rikosilmoitukseen. Sen jälkeen poliisista lähetettiin päivitetty ilmoitus uhrille, joka toimitti sen todisteena laskutusfirmalle, että lasku pantaisiin jäihin. (Mattila 2017). Haastattelun perusteella voidaan mielestäni huomata, että vaikutukset uhrille voivat olla pitkäkestoisia ja jatkuvaa kirjelmointia vaativia. Poliisihallituskin on huomionnut, että asianomistajalle aiheutuu haittaa, kun hän joutuu peruuttamaan nimissään oikeudettomasti otettuja lainoja tai tuotetilauksia, sekä selvittämään ulosottomaksuja. (POL-2022-30164, 3). Uhrit voivat tehdä rikosilmoituksen, mutta kuten yleisessä tiedossa on, niiden käsittelemisessä kestää. Sen sijaan perintätoimet etenevät nopeastikin, joka aiheuttaa uhrille vaikeuksia.

Poliisihallitus on lausunut lakiesitystä kommentoidessaan, että asianomistajan osalta oikeastaan ainoa keino suojautua tällaisia tapauksia vastaan on hakea omaehtoista luottokieltoa. Luottokielto kuitenkin haittaa rikosten uhrien elämää esimerkiksi kuluttajakaupassa tai kun he tekevät muita sopimuksia. (POL-2022-30164, 2–3.) Omaehtoinen luottokielto on maksullinen ja sitä on pitänyt hakea luottotietoyhtiöiltä. Viime vuonna tuli kuitenkin voimaan laki koskien positiivista luottotietorekisteriä (739/2022) ja se otetaan käyttöön vaiheittain kevästä 2024 alkaen. Rekisteriin voi tehdä ilmaiseksi vapaaehtoisen luottokieltoimerkinnän halutessaan. (Oikeusministeriö, 2022b.) Luottokieltojärjestelmää on kaavailtu Suomi.fi-palvelun kautta sähköisen tunnistautumisen kautta hallittavaksi. Finanssiala on kuitenkin lausunut, että mikäli sähköiset tunnistusvälineet ovat jo joutuneet väärin käsiin, pystyy luottoa rikollisin aikoin hakeva kirjautumaan samoilla tunnuksilla Suomi.fi-palveluun ja peruuttamaan luottovaroitus-merkinnän. (Finanssialan 2021). Ongelmaton ei siis ole tämäkään, mutta jos sähköiset tunnistusvälineet ovat väärissä käsissä, ei niiden väärinkäyttöä pysty muutenkaan estämään, ellei niitä sulje väärinkäytöksen huomattuaan.

Ulkomaiden osalta voidaan nostaa esiin esimerkki Tanskasta, jossa otettiin vuonna 2017 käyttöön mahdollisuus tehdä itselleen väestörekisteriin niin kutsuttu varoitusmerkintä, jonka voi tehdä, jos henkilö on hävittänyt esimerkiksi passinsa tai henkilötiedot ovat päätyneet vääriin käsiin. Merkintä kehottaa luotonantajaa tarkistamaan lainanhakijan henkilöllisyyden siten erityisen huolellisesti. Merkintää on voitu toki hyödyntää muuallakin kuin luotonannossa. Elokuuhun 2021 mennessä rekisteriin oli tehty jo 72 000 merkintää. (Informaatio-ohjauksen ja sidosryhmäyhteistyön suunnitelma – Toimenpidesuosituksat 2021, 11–12)

Kuten aiemmin on mainittu, tunnistamisvälineiden joutuminen vääriin käsiinkin on siis ongelma, vaikkakin varmasti paljon harvinaisempi kuin pelkkien tietojen oikeudeton hallussapito. Käytännössä se tarkoittaisi sitä, että jollakin olisi oikeudettomasti hallussaan toisen pankin käyttäjätunnus, salasana sekä avainlukulista taikka puhelin, johon vahva sähköinen tunnistaminen yhdistyy. Henkilötunnusjärjestelmän uudistamista koskevassa lausunnossaan Keskusrikospoliisi tuo esille, että vahvojen tunnistautumisvälineiden myöntämisen tulisi perustua ensimmäisellä kerralla aina henkilökohtaisessa kontaktissa tehtävään henkilön luotettavaan tunnistamiseen. Mikäli havaittaisiin henkilöllisyystodistuksen tai tunnistautumisvälineiden olevan väärän tahon hallussa, vahvan tunnistautumisen välineet olisi tarpeen mitätöidä ja uusia tarpeen vaatiessa. Keskusrikospoliisi korostaa lausunnossaan, että palveluntarjoajalle tulisi säätää lakitasoisesti vastuu varmistua asiakkaan asianmukaisesta vahvasta tunnistautumisesta ja sanktioida velvollisuuden laiminlyönti. (POL-2022-2099, 4)

Kirjallisuudessa on ehdotettu tilauspetosten uhrien suojelemiseksi erilaisia keinoja. Järvisen mukaan, jos tunnistamista ei olisi tehty riittävän turvallisesti, lasku ei olisi perintäkelpoinen. Toisekseen hän ehdottaa, että poliisi voisi ylläpitää tietovuotojen uhrien henkilötunnuksista listaa, josta kauppias voisi tarkistaa onko kyse tällaisen henkilötunnuksen avulla tehdystä tilauksesta. Kolmanneksi hän ehdottaa, että prepaid-numeroista voisi luoda rekisterin, joka tarjoaisi yhden lisäkeinoon petosriskin arviointiin. (Järvinen 2022, 173). Ehdotukset törmäävät käytännössä mielestäni esimerkiksi henkilötietojen suojasta johtuviin ongelmiin. Kauppiasalla tuskin on oikeus tietää, onko uhrin henkilötunnus vuotanut jossakin tietovuodossa.

4.6 Muut aiheeseen liittyvät lainsäädäntöhankkeet

Tällä hetkellä suunnitteilla on useita lainsäädäntömuutoksia, joilla on liittymäpintaa henkilöllisyyden todentamiseen sekä väärillä tiedoilla tehtyjen väärinkäytösten ehkäisemiseen. Valtionvarainministeriössä on ollut käynnissä henkilötunnuksen uudistamista ja valtion takaaman identiteetin hallinnoimista koskeva hanke (VM183:00/2020), jonka tavoitteena on ollut muun muassa uudistaa henkilötunnusjärjestelmää, sujuvoittaa ulkomaalaisten asiointia laajentamalla henkilötunnuksen saajien

piiriä, ehkäistä henkilötunnusten käyttöä tunnistuskäytössä ja ehkäistä identiteettivarkauksia. Hankkeen esittämiä lainsäädäntöehdotuksia ei kuitenkaan ehditty käsitellä edeltävällä hallituskaudella. Hankkeen työryhmä on suositellut, että vahva sähköinen tunnistaminen tulisi ottaa käyttöön erinäisissä palveluissa, mikäli matalamman tasotunnistustavat tai yksilöiminen henkilötunnuksella eivät olisi riittäviä keinoja ehkäistä henkilötunnuksen ja muiden henkilötietojen väärinkäyttöön liittyviä riskejä (Valtionvarainministeriö 2022).

Osana hanketta on käsitelty arviomuistiota henkilötunnuksen muuttamiskynnyksen madaltamisesta. Arviomuistiossa on todettu, että henkilötunnuksen muuttaminen ei suoraan poista petoksen tekemahdollisuuksia varastetulla identiteetillä, sillä kaikki toimijat eivät tarkista henkilötunnuksen voimassaoloa VTJ:stä, joten petosten teko voi jatkua myös vanhalla henkilötunnuksella (Arviomuistio henkilötunnuksen muuttamiskysymyksen madaltamisesta 2021, 12). Arviomuistion perusteella hanke on suosittanut, että henkilötunnuksen muuttamiskynnystä ei madalletaisi nykyisestä, vaan tietovuotojen aiheuttamiin uhkiin tulisi varautua muilla toimenpiteillä. (Arviomuistio henkilötunnuksen muuttamiskysymyksen madaltamisesta 2021, 15).

Tällä hetkellä henkilötunnusta voi muuttaa väestötietojärjestelmä ja Digi- ja väestötietojärjestelmän varmennepalveluista annetun lain (661/2009, VJT-laki) 12§:n mukaisesti henkilötunnuksen väärinkäyttötilanteissa silloin kun muu kuin henkilötunnuksen haltija on toistuvasti väärinkäyttänyt tunnusta ja käytöstä on aiheutunut merkittävää taloudellista tai muuta haittaa tunnuksen oikealle haltijalle ja henkilötunnuksen muuttamisella voidaan tosiasiallisesti estää väärinkäytön haitallisten seurausten jatkuminen.

Valtionvarainministeriössä on ollut myös käynnissä digitaalisen henkilöllisyyden hanke (VM092:00/2021), jonka osana on suunniteltu digitaalista henkilöllisyyttä. Esityksessä on ehdotettu säädettäväksi uusi laki, jossa säädettäisiin digitaalisesta henkilöllisyystodistuksesta, johon kansalaisilla olisi oikeus suoraan oikeus voimassa olevan passin tai henkilökortin nojalla tiettyjä poikkeuksia lukuun ottamatta. Tämän takia myös tunnistamislakiin tulisi muutoksia, sillä digitaalisen henkilöllisyyden avulla tapahtuva sähköinen tunnistaminen luettaisiin myös vahvan tunnistamisen piiriin. (HE 133/2022, 19.) Myöskään tätä ei ehditty käsittelemään edellisellä hallituskaudella, joten asian valmistelu jatkuu.

5 JOHTOPÄÄTÖKSET

Opinnäytetyön tarkoituksena oli ensinnäkin tuoda esiin niitä rikoksia, joita toisten henkilötiedoilla voi luotonannossa ja verkkomaksamisessa tehdä. Toisekseen tarkoituksena oli selvittää mistä syistä

kuluttajansuojalain voimassa olevat luottoja koskevat henkilöllisyyden todentamisvelvollisuutta koskevat säännökset ovat syntyneet ja mitä vaikutuksia niiden voimaantulo toi sekä mitä muutoksia näihin säännöksiin on tulossa.

Toisten henkilöiden tiedoilla luotonantoon ja maksamiseen liittyvissä rikoksissa kyse on useimmiten identiteettivarkaudesta ja petoksesta. Tällöin esimerkiksi tilataan tuotteita verkkokaupasta laskulle tai otetaan pikaluottoja toisen henkilön nimiin. Vaikka uhri ei joutuisi maksuja maksamaan, on rikollinen jo saanut rahallisen hyödyn. Viimeisen vuosikymmenen aikana digitalisaatio, maksamisen tavat ja verkossa tapahtuva kauppa ovat lisääntyneet, ja tätä myötä rikollisuuden muodot ovat kehittyneet ja erilaiset verkossa toisten henkilötiedoilla tapahtuvat väärinkäytökset kasvaneet. Henkilötietoja voidaan oikeudettomasti saada haltuun monilla eri tavoin esimerkiksi varkaudella tai tietomurrolla.

Ennen 2010-luvun taitetta käynnistyi Sisäministeriön identiteettiohjelma, jossa erityisenä painoalueena oli henkilöllisyyden suojaaminen ja identiteettivarkaudet. Työryhmä huomioi verkossa tapahtuneen toimintaympäristön muutoksen ja uhrin huonon aseman. Suunnilleen samaan aikaan identiteettiohjelman kanssa kävi keskustelu pikaluottoihin liittyvistä ongelmista kiivaana. Muiden luottoihin liittyvien ongelmien lisäksi oltiin herätty siihen, että erityisesti vielä siihen aikaan tekstiviestillä haettujen luottojen myöntämisessä oli esiintynyt väärinkäytöksiä. Myös tietosuojavaltuutettu ja kuluttaja-asiamies olivat kiinnittäneet huomiota siihen, että lainaa sai haettua toisen henkilötiedoilla.

Todettiin, että sääntelyä oli siltä osin tiukennettava ja luotonantajille asetettiin kuluttajansuojalain puitteissa velvollisuus tunnistaa lainanhakijat huolellisesti ja vahvan sähköisen tunnistamisen avulla, mikäli lainaa haettiin sähköisesti. Lakimuutos sai osakseen kritiikkiä sen suhteen, oliko väärinkäytöksiä todella sen verran, että tällainen sääntely oli tarpeen ja olisiko esimerkiksi luotonantajien valvontaa voinut toteuttaa enemmän jälkivalvontana, he kuitenkin olivat lopulta vastuussa.

Vaikka tunnistamisvirheiden todettiin olleen lainanmyöntäjien vastuulla, huomioitiin kuitenkin uhrien tilanne. Kun sääntely vähensi tekstiviestilutoissa esiintyneitä huijauksia, paransi se myös samalla uhrien asemaa, joiden ei tarvinnut enää selvittää väärillä tiedoilla myönnettyjä luottoja. Vaikka väärinkäytöksiä ei välttämättä ollut hirvittävän paljon, oli sääntelyllä varmasti myös ennalta estävää vaikutusta, koska ilman oikeudettomasti hankittua sähköistä tunnistamisvälinettä, ei luottoa voinut toisten tiedoilla enää hakea niin helposti. Nyt kun väärinkäytösten määrä on yhä kasvanut ja vahva sähköinen tunnistaminen muutenkin lisääntynyt, voi jälkiviisaana arvioida, että sääntely oli tarpeellinen.

Vaikka tunnistamisvaatimus tuotiin kuluttajansuojalakiin, eivät kaikki luotonantajat ottaneet sitä heti käyttöön. Uskon, että syynä on ollut se, että väärinkäytösten määrä ei ollut suuri ja vahva sähköinen tunnistaminen aiheutti varmasti kustannuksia ja muita haittoja palveluntarjoajille. Hyötyhaitta

suhdetta ei vahvan sähköisen tunnistamisen käyttöönotossa nähty välttämättä siis kovin järkevänä. Vuonna 2021 DDV:n tuottaman selvityksen perusteella, jossa tutkittiin henkilötunnuksen käyttö tunnistamisen välineenä, todettiin vahvan sähköisen tunnistamisen käyttöönoton lisäämisen osalta, että vastaajien mielestä keskimäärin eniten haasteita aiheuttivat järjestelmämuutokset, kustannukset (kuukausimaksut ja siirtomaksut), resurssit ja asiakkaiden valmius ottaa sähköinen tunnistamisväline käyttöön (DDV 2021, 43). Nämä varmasti ovat olleet vaikuttimena jo vuoden 2010 muutoksen jälkeen.

Pikaluotot ylipäättään ovat olleet useiden sääntelymuutosten kohteena vuosien varrella ja noin kymmenen vuotta kuluttajansuojalain muutoksen jälkeen luottoja koskevan sääntelyn katsottiin kaipaavan taas suurempaa päivivitystä. Vuoden 2010 kuluttajansuojalainmuutoksen katsottiin toimineen suhteellisen hyvin, mutta verkkokaupan ja sähköisen kaupankäynnin lisääntymisen myötä lainsäädännön ei katsottu vastavan enää nykytarpeita. Poliisihallitus kritisoi maksupalvelunvälittäjiä ja luotonantajien toimia petosrikollisuuden ja identiteettivarkauksien estämiseksi. Esimerkiksi Klarnan ja Qliron kautta pystyi Ylen tekemän tutkimuksen mukaan tilaamaan helposti tavaraa laskulle toisen tiedoilla.

Kuluttajaluottotyöryhmän ehdotus muutoksista hyväksyttiin eduskunnassa maaliskuussa 2023 ja se tulee voimaan lokakuun alusta 2023. Suurimpana muutoksen nimenomaan tilauspetosten estämiseksi kuluttajansuojalakiin tulee vahvan sähköisen tunnistamisen vaatimus myös silloin kun kuluttaja tilaa tuotteen myöhemmin maksettavaksi eli laskulle. Lain tunnistamisvaatimuksia laajennetaan myös luotonannon osalta, jolloin vahva tunnistaminen tulee vaatimukseksi myös luottorajaa ja luoton määrää korotettaessa sekä vanhan asiakkaan hakiessa uutta luottoa. Nämä muutokset tulevat torjumaan tilanteita, joissa joku pitää oikeudettomasti hallussaan jonkun vahvan tunnistamisen välineitä. Tällaisia väärinkäytöksiä ei uskoakseni ole kovinkaan paljon verrattuna niin kutsuttuihin tilauspetoksiin, jotka olivatkin erityisessä keskiössä tässä lainmuutoksessa. Eri sidosryhmien osalta ei juurikaan esitetty kritiikkiä ehdotusta kohtaan. Vain euromääräistä rajaa laskulle tunnistamisen osalle ehdotettiin, mutta sitä ei lainvalmistelutahon puolelta pidetty järkevänä.

Uskon, että uudistuksella on positiivinen vaikutus rikollisuuden torjunnassa. Poliisihallitus on arvioinut, että vahvan tunnistautumisen edellyttäminen hyödykkeiden hankkimisessa verkossa vähentäisi poliisin tietoon tulleiden identiteetti- ja petosrikosten määrää vuodessa arviolta noin 1000–1500 kappaleella. (POL-2020-84764, 2). Jää nähtäväksi millaiset vaikutukset tosiasiallisesti ovat, mutta ottaen huomioon kyseisten rikosten kasvavan määrän, arvio kuulostaa oikeasuhtaiselta. Vahva sähköinen tunnistaminen on ehdottomasti tehokas keino tällaisten tilauspetosten estämiseksi.

Verkkopetosten määrä on kasvanut huomasti. Tarkkoja määriä tällaisista rikoksista on vaikea saada, sillä identiteettivarkauksia ja petoksia voidaan tehdä monilla muillakin tavoin kuin nostamalla lainaa tai tilaamalla tuotteita toisten henkilötietojen avulla. Lisäksi rikosilmoituksista ei kirjautuvan vuoksi pysty suoraan analysoimaan, että kyse on tällaisista rikoksista vaan ilmoituksia pitäisi pystyä tutkimaan tarkemmin. Myöskään kaikkia tällaisia rikoksia ei ilmoiteta poliisille. Aiemmin esille tuomani Poliisihallitukset tilastot kuitenkin osoittavat, että pelkästään tilauspetoksia, jolla tavaraa on tilattu toisen henkilötunnuksella, on ilmoitettu arviolta vajaa tuhat kappaletta vuosittain muutamana edellisenä vuotena. Arvio oli tässäkin suhteessa todellisuutta pienempi poliisin arvion mukaan. Kyseessä ei siis ole ollut täysin vähäinen ongelma.

Kun mietitään tällaisten rikosten tutkimista poliisin näkökulmasta, tulevat esiin myös resurssikysymykset. Verkkokauppapetosten tutkinta sitoo henkilöresursseja merkittävästi suhteessa siihen, millaisia rangaistuksia tällaisista rikoksista on odotettavissa. (HE 218/2022, 2) Pienessä kuvassa näillä aiheutetut rikosvahingotkaan eivät välttämättä ole suuria, mutta vaihteluväli on kuitenkin muutamista kymmenistä euroista kymmeneen tuhansiin (HE 218/2022, 23). Pelkästään tällaisten rikosten määrän vähentyessä uskon, että muutoksella voi olla myös vaikutusta poliisin työmääriin tutkinnassa, jonka ruuhkautuminen suurten juttumäärien takia on yleisessä tiedossa. Lakiesitystä koskevassa hallituksen esityksessä on muutoksen arvioitu vähentävän poliisin työmäärä hieman, kun mahdollisuus tehdä verkkokauppapetoksia vaikeutuu (HE 218/2022, 29). Uskon, että lainoja koskevien väärinkäytösten osalta muutos ei välttämättä tule ole niin näkyvä, sillä vahva tunnistaminen on ollut luottojen osalta jo laajemmin käytössä.

Lakimuutos voi myös itsessään jo ennalta ehkäistä väärinkäytöksiä, kun rikosten tekeminen toisen tiedolla tehdään yhä vaikeammaksi. Osaltaan samalla tällainen rikollisuus voi myös muuttaa muotoaan ja erilaiset verkossa tapahtuvat väärinkäytökset voivat yhä jatkaa kasvuaan. Poliisihallitus lausuikin ehdotuksen osalta, ettei se usko vahva tunnistaminen vaatimuksen sinänsä vaikuttavan henkilötietojen kalasteluyritysten kasvuun. Lisäksi on huomioitava kansainvälinen verkkokauppa, jossa suomalainen kuluttajansuojalainsäädäntö tulee ainoastaan rajoitetusti sovellettavaksi (Finanssiala 2022). Kuluttajien on siis jatkossa edelleenkin hyvä olla tarkkana maksuvälineidensä, sähköisten tunnistamisvälineiden sekä henkilötietojensa suojaamisessa ja tehdä vapaaehtoinen luottokiello tarvittaessa, jos epäilee tietojensa vuotaneen.

Jatkotutkimusta aiheesta voisi tehdä sen suhteen, kuinka lokakuussa voimaantuleva kuluttajansuojalain muutos on sitten lopulta vaikuttanut tehtyihin väärinkäytöksiin ja mikä merkitys esimerkiksi tulevalla luottokieltorekisterillä tulee olemaan. Lisäksi muut henkilöllisyyden todentamiseen liittyvät muutokset kuten digitaalinen henkilöllisyys tulevat olemaan ajankohtaisia lähitulevaisuudessa ja niihin kohdistuvia tunnistamiseen liittyviä ongelmia voi olla syytä tarkastella lähemmin.

6 POHDINTA

Tässä osiossa tarkoituksena on reflektoida opinnäytetyöprosessia ja sen onnistumista. Opinnäytetyön tekeminen ei tuntunut liian haastavalta, sillä olen ennen Poliisiammattikorkeakoulua opiskellut oikeustiedettä ja tehnyt kaksi opinnäytetyötä jo aikaisemmin. Halusin tehdä tämän opinnäytetyön samasta oikeustieteellisestä näkökulmasta, sillä se on minulle tutuin sekä kiinnostavin näkökulma. Kuluttajansuoja on rikosten ohella kiinnostanut minua ja erityisesti verkossa tapahtuvat väärinkäytökset. Näiden ajatusten pohjalta valikoitui opinnäytetyön aihe henkilöllisyyden todentamisvelvollisuudesta ja siihen liittyvistä väärinkäytöksistä.

Kirjallisuuden ja muun materiaalin löytäminen aiheesta ei ollut kovin vaikeaa, sillä kyseessä oli tutkimuksellinen opinnäytetyö ja paljolti vastauksia tutkimuskysymyksiin löytyi lainvalmisteluaineistosta. Metodina käytin lainopillista sekä oikeushistoriallista metodologiaa, eli pyrin systematisoidaan voimassa olevaa oikeutta sekä esittämään muutosten osalta vastauksia kysymyksiin miksi ja miten. Näitä metodeja olin käyttänyt myös aiemmissa opinnäytetöissäni, joten ne olivat minulle tuttuja. Haasteena tässä oli kuitenkin se, että uudesta lähteestä löytyi aina lisää lähteitä ja uusia ideoita, joita kaikkia ei kuitenkaan ollut aikaa eikä työn laajuus huomioiden järkevä lähteä tutkimaan.

Vaikka lainvalmisteluaineistossa oli suoraan kerrottu syitä muutosten taustalle, pystyi esimerkiksi kirjallisuudesta, lakiesityksestä esitetyistä lausunnoista sekä muista julkisista mielipiteistä tekemään omia johtopäätöksiä sen suhteen, mitkä näiden lausumien taustalla on ollut ja mistä ne ovat johtuneet. Monipuolisuuden vuoksi työhön olisi voinut ottaa myös kansainvälistä materiaalia. Kuitenkin haasteeksi koin opinnäytetyön laajuuden. Kun aiheeseen pääsee sisälle, tulee mieleen yhä enemmän asioita, joita opinnäytteeseen voisi vielä ottaa mukaan. Pyrin kuitenkin pitämään mielessä tutkimuskysymykset ja aiheen rajaukset. Kaiken kaikkiaan opinnäytetyöprosessi oli mielestäni onnistunut ja opinnäytetyössä onnistuin löytämään vastaukset tutkimuskysymyksiin.

LÄHTEET

Arviomuistio henkilötunnuksen muuttamiskysymyksen madaltamisesta 2021: Valtionvarainministeriö 24.11.2021. Luettavissa: <https://vm.fi/hanke?tunnus=VM183:00/2020>. Luettu: 1.3.2023.

Aureärvi, E. & Hemmo, M. 2004: Luotto-oikeus. 3. painos. Jyväskylä, Talentum

DDV 2020: Digi- ja väestötietoviraston vahva suositus vahvan tunnistamisen palveluiden käyttämiselle. Tiedote 2.11.2020. Luettavissa: <https://dvv.fi/-/digi-ja-vaestotietoviraston-vahva-suositus-vahvan-tunnistamisen-palveluiden-kayttamiselle>. Luettu 26.2.2023.

DDV 2021: Henkilötunnuksen käyttö tunnistamisessa. Loppuraportti 18.6.2021. Luettavissa: https://api.hankeikkuna.fi/asiakirjat/e4e7c20c-ab47-480e-b3da-353452c53a1a/39512504-1386-4fc7-aa8a-184d6a8164da/LIITE_20220104084227.PDF. Luettu 20.2.2023.

Edilex 2019: Maksupalveludirektiivi tuli kokonaisuudessaan voimaan 14. syysuuta – verkko-ostoksilla vaaditaan jatkossa vahvaa tunnistautumista. 13.9.2019. Sisäinen lähde. Luettavissa: <https://www.edilex-fi.polamk.idm.oclc.org/uutiset/61256?allWords=maksupalveludirektiivi+tuli&offset=1&per-page=20&sort=relevance&searchSrc=1&advancedSearchKey=824636>. Luettu 23.2.2023.

Finanssiala 2019: Kysymyksiä ja vastauksia toisesta maksupalveludirektiivistä (PSD2). 14.6.2019. Luettavissa: <https://www.finanssiala.fi/uutiset/kysymyksia-ja-vastauksia-toisesta-maksupalveludirektiivista-psd2/>. Luettu: 23.2.2023

Finanssiala 2021: Täydentävä lausuma henkilötunnuksen uudistamishankkeen informaatio-ohjauksen ja sidosryhmäyhteistyön työryhmän toimenpidesuosituksiin: Luottovaroitusjärjestelmän edut luottohijauksen torjunnassa epäselviä. Luettavissa: <https://vm.fi/hanke?tunnus=VM183:00/2020>. Luettu. 1.2.2023.

Finanssiala 2022: Finanssialan lausuntovastaus 29.4.2022 koskien kuluttajaluottotyöryhmän mietintöä 2022:12. Luettavissa: <https://valtioneuvosto.fi/hanke?tunnus=OM085:00/2020>. Luettu: 15.2.2023.

Finlex: Lainvalmistelun prosessiopas. Luettavissa: <http://lainvalmistelu.finlex.fi>. Luettu: 2.3.2023

GE Money 2008: GE Money Oy:n lausunto 31.12.2008 koskien pikavippityöryhmän mietintöä 2008:7. Luettavissa: <https://oikeusministerio.fi/hanke?tunnus=OM038:00/2007>. Luettu: 16.4.2023.

Haasio, A. 2017: Verkkorikokset. Vantaa, BTH Finland Oy

Helsingin käräjäoikeus 2008: Helsingin käräjäoikeuden lausunto 15.12.2008 koskien pikavippityöryhmän mietintöä 2008:7. Luettavissa: <https://oikeusministerio.fi/hanke?tunnus=OM038:00/2007>. Luettu: 16.4.2023.

HE 36/2009. Hallituksen esitys Eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä eräksi siihen liittyviksi laeiksi.

HE 64/2009. Hallituksen esitys Eduskunnalle laeiksi kuluttajansuojalain 7 luvun, rikoslain 36 luvun 6 §:n ja korkolain 4 §:n muuttamisesta.

HE 24/2010. Hallituksen esitys Eduskunnalle laeiksi kuluttajansuojalain muuttamisesta ja eräiden luotonantajien rekisteröinnistä sekä eräksi niihin liittyviksi laeiksi.

HE 133/2022. Hallituksen esitys eduskunnalle digitaalista henkilöllisyyttä koskevaiksi lainsäädännöksi

HE 218/2022. Hallituksen esitys laeiksi kuluttajansuojalain, kuluttajaviranomaisten eräistä toimivaltuuksista annetun lain 13§:n ja oikeudenkäymiskaaren 5 luvun 3§:n muuttamisesta.

Hirvonen, A. 2011: Mitkä metodit? Opas oikeustieteen metodologiaan? Yleisen oikeustieteen julkaisu. Helsinki

Hämäläinen, V. 2021: Osta nyt, älä maksa koskaan. Yle 11.1.2021. Luettavissa: <https://yle.fi/a/3-11690670>. Luettu: 1.3.2023.

Hänninen, J. 2021: Maksufirma Klarnan kautta pystyy tilaamaan tavaraa toisen nimiin – MOT:n testi osoittaa, kuinka pahasti ruotsalaisyhtiön tietoturva osoittaa. Yle 13.7.2021. Luettavissa: <https://yle.fi/a/3-12014974>. Luettu: 1.3.2023.

Identiteettiohjelma 2010: Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma), työryhmän loppuraportti. Sisäasiainministeriön julkaisu 32/2010. Luettavissa: <https://julkaisut.valtioneuvosto.fi/handle/10024/79876>. Luettu: 20.1.2023.

Informaatio-ohjauksen ja sidosryhmäyhteistyön suunnitelma – Toimenpidesuosituksien 2021: Henkilötunnuksen uudistamista ja valtion takaaman identiteetin hallinnoimista koskeva hanke. Informaatio-ohjauksen ja sidosryhmäyhteistyön työryhmä. 7.12.2021. Luettavissa: <https://vm.fi/hanke?tunnus=VM183:00/2020>. Luettu: 2.2.2023.

Järvinen, P. 2022: Digiajan tietosuojat. Tammi.

Kaisto, J. 2005: Lainoppi ja oikeusteoria. Helsinki, Edita

- Kekkonen, J. 1997: Oikeudellisen muutoksen tutkimisesta – minun metodini. Teoksessa Häyhä, J. (toim.) 1997: Minun metodini, 132-150
- Kekkonen, J. 1999: Suomen oikeuden historiallisia kehityslinjoja. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut.
- Keskuskauppakamari 2008: Keskuskauppakamarin lausuntovastaus 23.12.2008 koskien pikaluotto-työryhmän mietintö 2008:7. Luettavissa: <https://oikeusministerio.fi/hanke?tunnus=OM038:00/2007>. Luettu: 30.3.2023.
- Keskusrikospoliisi 2008: Keskusrikospoliisi lausuntovastaus 23.12.2008 koskien pikavippityöryhmän mietintöä 2008:7. Luettavissa: <https://oikeusministerio.fi/hanke?tunnus=OM038:00/2007>. Luettu: 30.3.2023.
- Klarna 2022: Klarna Oy:n lausunto 7.12.2022 eduskunnan talousvaliokunnalle koskien HE 218/2022. 7.12.2022.
- Kuluttajaluottotyöryhmän asettamispäätös 2021: Oikeusministeriön asettamispäätös 2.7.2021 hankkeessa VN/28370/2020. Luettavissa: <https://valtioneuvosto.fi/hanke?tunnus=OM085:00/2020>. 2.2.2023.
- LaVL 12/2009: Lakivaliokunnan lausunto 11.6.2009. Luettavissa: <https://www.eduskunta.fi/FI/Vaski/sivut/trip.aspx?triptype=ValtiopaivaAsiat&docid=he+64/2009>. Luettu: 14.2.2023.
- Leponen, M. 2022: Uusi, huolestuttava ilmiö – rikolliset kohdistava Vastaamon tietovuodon uhreihin raukkamaisia rikoksia. Blogi 11.2.2022. Luettavissa: <https://poliisi.fi/blogi/-/blogs/uusi-huolestuttava-ilmio-rikolliset-kohdistavat-vastaamo-tietovuodon-uhreihin-raukkamaisia-rikoksia>, Luettu 26.2.2023.
- Linnake, T. 2008: Kotimaisessa pikavippihuijauksessa 58 uhria. Iltä-Sanomien 2.12.2008: Saatavilla: <https://www.is.fi/digitoday/tietoturva/art-2000001604675.html>. Luettu 20.2.2023.
- Mattila, R. 2017: Identiteettivarkaus piinasi Mikkoa viisi vuotta: ”Sain kymppitonin laskut ja osoitteeni siirrettiin Kilpisjärvelle”. OP Media. Luettavissa: <https://www.op-media.fi/omat-rahdat/identiteettivarkaus-piinasi-mikkoa-viisi-vuotta-sain-kymppitonin-laskut-ja-osoitteeni-siirrettiin-kilpisjarvelle/>. Luettu 1.3.2023.
- Määttä, K. 2010: Pikaluottojen sääntely oikeustaloustieteellisestä näkökulmasta. Lakimies 3/2010 s. 265–279

Oikeusministeriö 2020: Kuluttajaluottojen sääntelyyn esitetään tiukennuksia. Tiedote 20.10.2022. Luettavissa: <https://oikeusministerio.fi/-/kuluttajaluottojen-saantelyyn-esitetaan-tiukennuksia>. Luettu 29.1.2023.

Oikeusministeriö 2022a: Oikeusministeriön lausuntovastaus 12.1.2023 eduskunnan talousvaliokunnalle koskien HE 218/2022. 12.1.2023.

Oikeusministeriö 2022b: Positiivinen luottotietorekisteri avuksi ylivelkaantumisen toivossa. Luettavissa: <https://oikeusministerio.fi/-/positiivinen-luottotietorekisteri-avuksi-ylivelkaantumisen-torjunnassa>. Luettu: 12.4.2023.

Parkkali, E. & Pönkä, V. 2010: Pikaluottojen oikeudelliset ongelmat. Defensor Legis N:o 5/2010, 585–605.

POL-2020-84764: Poliisihallituksen lausuntovastaus 14.1.2021 koskien luonnosta hallituksen esitykseksi eduskunnalle laiksi väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain muuttamisesta. Luettavissa: https://api.hankeikkuna.fi/asiakirjat/70971366-f3fc-424b-9c3f-54eea05d6271/0f020f64-4004-4d31-a86f-e033df8abad4/LAUSUNTO_20210115084946.PDF. Luettu: 2.3.2023.

POL-2022-2099: Keskusrikospoliisin lausuntovastaus 4.3.2022 koskien henkilötunnusjärjestelmän uudistamista koskevia ehdotuksia (VN/25041/2020-VM-101). Luettavissa: https://api.hankeikkuna.fi/asiakirjat/e4e7c20c-ab47-480e-b3da-353452c53a1a/f1dd9be7-cc48-4c40-811a-ebc34fca7c5f/LAUSUNTO_20220307102440.PDF. Luettu: 1.3.2023.

POL-2022-30164: Poliisihallituksen lausuntovastaus 25.4.2022 koskien kuluttajaluottotyöryhmän mietintöä 2022:12. Luettavissa: <https://valtioneuvosto.fi/hanke?tunnus=OM085:00/2020>. Luettu: 2.2.2023.

PTK 116/2022 vp: Pöytäkirjan asiakohta. Eduskunnan täysistunto 26.10.2022. Luettavissa: https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_218+2022.aspx. Luettu: 16.2.2023.

PTK 169/2022 vp: Pöytäkirjan asiakohta. Eduskunnan täysistunto 16.2.2023. Luettavissa: https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_218+2022.aspx. Luettu: 16.2.2023.

PTK 170/2022 vp: Pöytäkirjan asiakohta. Eduskunnan täysistunto 17.2.2023. Luettavissa: https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_218+2022.aspx. Luettu: 16.2.2023.

PTK 171/2022 vp: Pöytäkirjan asiakohta. Eduskunnan täysistunto 20.2.2023. Luettavissa: https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_218+2022.aspx. Luettu: 16.2.2023.

PTK 91/2009: Täysistunnon pöytäkirja 13.10.2009. Luettavissa: <https://www.edus-kunta.fi/FI/Vaski/sivut/trip.aspx?triptype=ValtiopaivaAsiat&docid=he+64/2009>. Luettu: 14.2.2023.

PTK 92/2009: Täysistunnon pöytäkirja 14.10.2009. Luettavissa: <https://www.edus-kunta.fi/FI/Vaski/sivut/trip.aspx?triptype=ValtiopaivaAsiat&docid=he+64/2009>. Luettu: 14.2.2023.

PTK 95/2009: Täysistunnon pöytäkirja 20.10.2009. Luettavissa: <https://www.edus-kunta.fi/FI/Vaski/sivut/trip.aspx?triptype=ValtiopaivaAsiat&docid=he+64/2009>. Luettu: 14.2.2023.

Riekkinen, J. 2018: Verkkopetoksista ja todistelusta. Lakimies 1/2018, 75-102

Sanna Marinin hallitusohjelma 2019: Pääministeri Sanna Marinin hallituksen ohjelma 10.12.2019. Valtioneuvoston julkaisuja 2019:31.

Savolainen, J. 2009: Petoksenteelijät nostavat joka vuosi satoja pikalainoja toisen nimiin. 13.7.2009. Helsingin Sanomat. Luettavissa: <https://www.hs.fi/kaupunki/art-2000004665659.html>. Luettu 9.4.2023.

Savolainen, J. 2010: Kuluttajavirasto ja tietosuojavaltuutettu jatkavat pikaluottoyritysten seuranta – vasta osa valvontakampanjassa havaituista virheistä korjattu. 13.10.2010. Sisäinen lähde. Edilex. Luettavissa: [https://www-edilex-fi.polamk.idm.oclc.org/uutiset/25514?allWords=pikaluotto%2A&offset=21&perpage=20&sort=timeasc&typelds\[\]=127%3Afi&typelds\[\]=127%3Afi%2C151%3Afi&typelds\[\]=151%3Afi&searchSrc=1&advancedSearchKey=530328](https://www-edilex-fi.polamk.idm.oclc.org/uutiset/25514?allWords=pikaluotto%2A&offset=21&perpage=20&sort=timeasc&typelds[]=127%3Afi&typelds[]=127%3Afi%2C151%3Afi&typelds[]=151%3Afi&searchSrc=1&advancedSearchKey=530328) Luettu: 10.4.2023.

Sisäministeriö 2017: Tietoverkkorikollisuuden torjuntaa koskeva selvitys. Sisäministeriön julkaisu 14/2017. Helsinki

Soininen, H. 2017: Identiteettivarkaus kyberrikoksena – termit ja tunnusmerkistö. Defensor Legis N:o 1/2017, 84-101

Suomen Yrittäjät 2008: Suomen Yrittäjät Ry:n lausuntovastaus koskien 31.12.2008 koskien pikavippi-työryhmän mietintöä 2008:7. Luettavissa: <https://oikeusministerio.fi/hanke?tunnus=OM038:00/2007>. Luettu: 1.3.2023.

Rikos- ja pakkokeinotilasto SVT 2022: Suomen virallinen tilasto. 4. Vuosineljännes 2021. Helsinki: Tilastokeskus. Luettavissa: http://www.stat.fi/til/rpk/2021/04/rpk_2021_04_2022-01-19_tie_001_fi.html. Luettu: 13.2.2023.

Sisäministeriön poliisiosasto 2008: Sisäministeriön poliisiosaston lausuntovastaus 10.12.2008 koskien pikavippi-työryhmän mietintöä 2008:7. Luettavissa: <https://oikeusministerio.fi/hanke?tunnus=OM038:00/2007>. Luettu: 4.3.2023.

Takuusäätiö 2022: Takuusäätiön lausunto 7.12.2022 eduskunnan talousvaliokunnalle koskien HE 218/2022.

TaVM 42/2022: Talousvaliokunnan mietintö koskien HE 281/2022. Luettavissa: https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_218+2022.aspx. Luettu: 16.2.2023.

TaVM 13/2009: Talousvaliokunnan mietintö koskien HE 64/2009

Terämaa, J. 2001: Rahasuoritus ja sähköinen kauppa. Teoksessa Laine ym 2001: Laine, J. (toim). Verkkokauppaoikeus 2001, WSOY. 246-329

Tietosuojalautakunnan päätös nro 1/22.1.2008

Tietosuojavaltuutetun toimisto 2008: Tietosuojavaltuutetun toimisto lausuntovastaus 17.12.2008 koskien pikaluottotyöryhmän mietintöä 2008:7. Luettavissa: <https://oikeusministerio.fi/hanke?tunnus=OM038:00/2007>. Luettu: 3.3.2023.

Traficom 2021: Sähköisen tunnistamisen markkinat – Sähköinen tunnistaminen turvallisen asioinnin mahdollistajana, Traficomin tutkimuksia ja selvityksiä 2/2021

Traficom 2022: Vahvan sähköisen tunnistuksen luotettavuudesta ja turvallisuudesta huolehditaan Suomessa monin tavoin. 15.9.2022. Luettavissa: <https://www.traficom.fi/fi/ajankohtaista/vahvan-sahkoisen-tunnistuksen-luotettavuudesta-ja-turvallisuudesta-huolehditaan>. Luettu: 26.2.2023

Työryhmämietintö 2008:7: Pikaluottoihin liittyvän lainsäädännön uudistaminen. Oikeusministeriö, Helsinki. Luettavissa: <https://oikeusministerio.fi/hanke?tunnus=OM038:00/2007>. Luettu: 1.4.2023.

Valkama, E. & Muttilainen, V. 2008: Maksuvaikeudet luottomarkkinoilla, Oikeuspoliittisen tutkimuslaitoksen tutkimustiedonantoja 86. Helsinki.

Valtioneuvoston periaatepäätös 2009: Valtioneuvoston periaatepäätös sähköisestä tunnistamisesta 5.3.2009

Valtionvarainministeriö 2022: Työryhmä ehdottaa toimenpiteitä henkilötietojen väärinkäytön ehkäisemiseksi. Tiedote 10.1.2022. Luettavissa: <https://vm.fi/web/vm/-/tyoryhma-ehdottaa-toimenpiteita-henkilotietojen-vaarinkayton-ehkaisemiseksi>. Luettu 29.1.2023.