

# Sähköisen maksamisen sääntelyyn liittyvät erityiskysymykset ja vastuunjako

Yritysjuridiikka

Maisterin tutkinnon tutkielma

Janne Kangaspunta

2011

**AALTO-YLIOPISTON KAUPPAKORKEAKOULU – LASKENTATOIMEN LAITOS****Yritysjuridiikka****Tekijä**

Janne Petteri Kangaspunta

**Työn nimi**

Sähköisen maksamisen sääntelyyn liittyvät erityiskysymykset ja vastuunjako

**Työn laji**

Pro Gradu –tutkielma

**Aika**

Kevät 2011

**Sivumäärä**

XIII + 95s.

**Tiivistelmä**

Tutkimuksen kohteena ovat sähköiset maksujärjestelmät, niihin liittyvä sääntely sekä tietyt oikeudelliset kysymykset, joita nousee esille alueen sääntelyn sekä sähköisen toimintaympäristön erityispiirteiden vaikutuksesta. Viime vuosien aikana teknologian kehittymisen, kansainvälisen kaupan merkityksen ja volyymin kasvun sekä toimialojen kasvaneen konvergenssin seurauksena maksutapahtumien suorittaminen on siirtynyt yhä kasvavassa määrin sähköiseen ympäristöön. Nämä kaikki tekijät yhdistettynä maksunvälittäjien kirjon monipuolistumiseen sekä Euroopan unionin integraatiotavoitteisiin ovat johtaneet siihen että myös maksamiseen liittyvän oikeudellisen sääntelyn tarve on lisääntynyt.

Luvussa kolme luodaan yleiskatsaus sähköisen maksamisen toimintaympäristöön ja sen viimeaikaiseen kehitykseen. Luvussa pyritään selvittämään, mitkä tekijät vaikuttavat eri maksutapojen suosioon sekä esitellään tällä hetkellä yleisimmin käytettyjä sähköisiä maksutapoja, havainnollistetaan niiden käyttömahdollisuuksia ja arvioidaan niiden vahvuuksia tai rajoituksia maksamiseen liittyvien moninaisten tavoitteiden toteuttamisessa.

Tutkielman neljännessä luvussa pyritään avaamaan sähköisen maksamisen varsin monitahoista sääntelykehikkoa. Aluksi luvussa käydään läpi, mitä vaikutuksia toimintaympäristön dynaamisuudella sekä rajat ylittävällä luonteella on alueen sääntelyn muodostamiseen. Tämän jälkeen käsitellään maksuympäristön sääntelyä erikseen niin maksujen suorittamiseen, laitosten toimintaedellytyksiin ja maksupalveluiden tarjoamiseen kuin maksujen turvallisuuteenkin liittyen. Luvun lopussa tarkastellaan vielä maksamisen sopimuksia ja niillä vaikuttamisen mahdollisuuksia.

Viidennen luvun ensimmäisessä osiossa käsitellään sähköisen maksamisen turvallisuuteen liittyviä kysymyksiä. Ensin tarkastellaan henkilön tunnistamisen juridisia velvoitteita, identifioimismenetelmien luotettavuuden kriteereitä sekä identiteetin oikeellisen tunnistamisen merkitystä maksutapahtuman sitovuuden kannalta, jonka jälkeen käsitellään identiteettierohdyksen seurauksia ja riskinjakoa erehdystilanteissa. Lisäksi arvioidaan muutamien tällä hetkellä käytössä olevien tunnistusmenetelmien luotettavuutta. Tämän jälkeen käydään läpi tietoturvasuuskysymyksiä ja etenkin sitä, miten sekä yksittäisten maksutapahtumien että tietojen säilyttämisen osalta vastuuriskit jakautuvat osapuolten kesken.

Luvun viisi toisessa osiossa tarkastellaan sähköisten maksutapahtumien suorittamiseen liittyviä kysymyksiä. Aluksi käsitellään tiettyjen virheiden, joko itse maksutapahtumassa tai maksuun liittyvän veloitteen täyttämässä, vaikutusta maksutapahtuman sitovuuteen, joiden osalta nykyinen sääntely voidaan nähdä epäsuhtaisena tai potentiaalisen ongelmallisena. Tämän jälkeen tarkastellaan vielä sääntelyä sekä osapuolten välistä vastuunjakoa maksutapahtumaan liittyvissä teknisissä ongelmatilanteissa.

Viidennen luvun kolmannessa ja viimeisessä osiossa käydään vielä läpi muutamia

sääntelystä, sen puutteellisuudesta tai siitä johtuvasta oikeudellisesta epävarmuudesta aiheutuvia kysymyksiä tietyille intressitahoille.

**Avainsanat**

Sähköinen maksaminen, maksujärjestelmä, maksamisen turvallisuus, maksutapahtuma, vastuunjako

# SISÄLLYSLUETTELO

<b>SISÄLLYSLUETTELO</b> .....	<b>I</b>
<b>LÄHDELUETTELO</b> .....	<b>III</b>
<b>LYHENNELUETTELO</b> .....	<b>XIII</b>
<b>1. JOHDANTO</b> .....	<b>1</b>
1.1 Tutkielman taustaa.....	1
1.2 Tutkielman tavoitteet ja rajaukset.....	3
1.3 Tutkielman rakenne.....	3
<b>2. MÄÄRITELMÄT</b> .....	<b>6</b>
<b>3. SÄHKÖISET MAKSUJÄRJESTELMÄT JA YLEISIMMÄT SÄHKÖISET MAKSUTAVAT</b> .....	<b>8</b>
3.1 Yleistä sähköisestä maksamisesta ja maksujärjestelmistä: maksujärjestelmän valinta .....	8
3.2 Yleisimpiä sähköisiä maksutapoja.....	11
3.2.1 Maksaminen verkossa luotto- tai muun kortin tunnistetietojen avulla .....	11
3.2.2 Pankkiyhteysmaksut .....	12
3.2.2.1 Tilisiirtomaksut.....	13
3.2.2.2 Suoraveloitusmaksut.....	14
3.2.2.3 E-Lasku .....	15
3.2.3 Uudet maksujenvälityspalvelut .....	16
3.2.3.1 Mobiilimaksut.....	17
3.2.3.2 Välityspalvelut (mediating services).....	19
3.2.3.3 Sähköinen raha .....	19
<b>4. SÄHKÖISEN MAKSAMISEN SÄÄNTELY: PÄÄPIIRTEET JA KEHITYS</b> .....	<b>23</b>
4.1 Sähköinen toimintaympäristö ja sen vaikutukset sääntelyyn.....	23
4.2 Maksuympäristön sääntely.....	24
4.2.1 Maksutapahtumaan liittyvä sääntely .....	24
4.2.2 Maksupalveluiden tarjoamiseen liittyvä sääntely .....	26
4.2.3 Maksamisen turvallisuuteen liittyvä sääntely.....	27
4.2.4 Maksamisen sopimukset.....	29
4.2.4.1 Perusvelkasuhteeseen liittyvä sopimus .....	29
4.2.4.2 Maksujärjestelmää koskevat sopimukset.....	31
4.2.4.3 Maksujenvälitystä ja saamisoikeutta koskevat sopimukset.....	31
<b>5. SÄHKÖISEN MAKSAMISEN ERITYISKYSYMYKSET</b> .....	<b>34</b>

<b>5.1 MAKSUJEN TURVALLISUUTEEN LIITTYVÄT KYSYMYKSET</b> .....	34
5.1.1 Identiteetin ja henkilön tunnistamisen merkitys sähköisessä maksuympäristössä .....	34
5.1.1.1 Henkilön tunnistamisen juridiset velvoitteet .....	35
5.1.1.2 Identiteetin oikeudellinen merkitys maksutapahtumassa .....	37
5.1.1.3 Identiteettierohdyksen seuraukset: oikeudettomat maksutapahtumat ja vastuunjako .....	38
5.1.1.4 Yleisesti sähköisessä maksuympäristössä käytössä olevien henkilön tunnistamismenetelmien arviointia .....	43
5.1.1.4.1 Korttimaksujen yhteydessä käytettävät tunnistusmenetelmät .....	43
5.1.1.4.2 Verkkopankkitunnistautuminen .....	45
5.1.1.4.3 Varmenteet.....	46
5.1.1.4.4 Muut tunnistusratkaisut .....	47
5.1.1.5 Anonyymi maksaminen vaihtoehtona .....	49
5.1.2 Tietoturvaluisuus maksamisessa .....	50
5.1.2.1 Yksittäisten maksutapahtumien turvallisuus ja vastuunjako.....	52
5.1.2.2 Tietojen säilyttämisen turvallisuus ja vastuunjako.....	57
<b>5.2 MAKSUJEN SUORITTAMISEEN LIITTYVÄT KYSYMYKSET</b> .....	60
5.2.1 Virheet maksutapahtumassa tai maksuun liittyvän velvoitteen täyttämässä .....	60
5.2.1.1 Yksilöivän tunnisteiden korostunut merkitys maksutapahtumassa.....	60
5.2.1.1.1 Perusteettoman edun palautus oikeuskeinona virheiden korjaamiseksi .....	62
5.2.1.2 Velkoja-aloitteisten maksujen erityinen palautusoikeus .....	67
5.2.1.3 Kuluttajan ja kauppiaan väliset sopimuskiistat: maksutapakohtaiset eroavaisuudet yhteisvastuun osalta myyjää tai palveluksen suorittajaa kohtaan .....	69
5.2.2 Tekniset ongelmatilanteet.....	71
5.2.2.1 Yhteyden katkeaminen / tilapäinen maksuverkon pettäminen.....	72
5.2.2.2 Maksuverkon pettäminen.....	74
<b>5.3 MUUT ERITYISKYSYMYKSET</b> .....	78
5.3.1 Sääntelystä tai muusta toimintaan liittyvästä oikeudellisesta epävarmuudesta aiheutuvat kysymykset.....	78
5.3.1.1 Pienmaksuvälineen määritelmä ja pienmaksuvälineitä koskevien erityissäännösten tarkoituksenmukaisuus.....	78
5.3.1.2 Soveltamisalaan liittyvät epäselvyydet mobiilimaksamisen osalta sekä muut maksupalvelulain vaikutukset mobiilimaksamiseen .....	80
5.3.1.3 Sähköiseen rahaan liittyvät juridiset kysymykset.....	83
5.3.2 Erityisryhmien huomiointi.....	86
5.3.2.1 Tietoyhteiskunnan vaikeasti saavuttavien mahdollisuus sähköisten maksupalveluiden käyttöön .....	87
5.3.2.2 Eriarvoisuus sähköisten tunnisteiden, erityisesti verkkopankkitunnusten osalta.....	88
<b>6. LOPUKSI</b> .....	90

# LÄHDELUETTELO

## Kirjalliset lähteet

Aurejärvi, Erkki – Hemmo, Mika (2007). *Velvoiteoikeuden oppikirja*. 3. Painos. Helsinki: Edita Oy.

Hemmo, Mika (2007). *Velvoiteoikeuden perusteet*. Helsinki: Yliopistopaino.

Hyppönen, Konstantin (2009). *Open Mobile Identity – Secure Identity Management and Mobile Payments Using Hand-Held Devices*. Doctoral dissertation, Kuopio University, Business and Information technology.

Jyrkönen, Hanna – Paunonen, Heli (2003). *Card, internet and mobile payments in Finland*. Suomen pankin keskustelualoitteita 8, 2003. Helsinki: Suomen Pankin monistuskeskus.

Leinonen, Harry (2008). *Payment habits and trends in the changing e-landscape 2010+*. Tutkimuksia/Suomen pankki. A: 111. Helsinki: Multiprint Oy.

Majuri, Tuomas (2005). *Sähköinen raha, asiakastili ja uudet toimijat pankkialalla*. Helsinki: Yliopistopaino.

Saarenpää et al. (1997). Saarenpää Ahti (toim.) – Pöysti Tuomas (toim.) – Sarja Mikko – Still Viveca – Balboa-Alcoreza Ruxandra. *Tietoturvallisuus ja laki: Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä*. Valtiovarainministeriön tutkimusraportti. Helsinki: Edita Oy.

Saarnilehto, Ari – Hemmo, Mika – Kartio, Leena (2001). *Varallisuus oikeus*. Helsinki: WSOY Lakitieto.

Salminen, Markus (2009). *Tietosuoja sähköisessä liiketoiminnassa*. Talentum/Kariston kirjapaino Oy.

Schaub, Martien (2004). *European Legal Aspects of E-Commerce*. Groningen: Europa Law Publishing.

Terämaa, Jyri (2001). *Rahasuoritus ja sähköinen kauppa* teoksessa Laine, Juha (toim.): *Verkkokauppa-oikeus*. Porvoo. WSOY – Kirjapainoyksikkö.

Turban et al. (2010). Turban, Efraim – King, David – Lee, Jae – Liang, Ting-Peng – Turban, Deborah. *Electronic Commerce 2010: A managerial perspective*. 6<sup>th</sup> edition. NJ: Pearson education inc. publishing as Prentice Hall.

Viemerö, Mikko (2009). *Tietosuoja sähköisessä kaupassa ja sähköisessä viestinnässä*. Yritysjuridiikka / Licensiaatintutkimus. Helsingin kauppakorkeakoulu, Laskentatoimen ja rahoituksen laitos.

## **Virallislähteet**

### ***Euroopan Unioni***

- EY/95/46 Euroopan parlamentin ja neuvoston direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta. (Tietosuojadirektiivi)
- EY/2007/64 Euroopan parlamentin ja neuvoston direktiivi maksupalveluista sisämarkkinoilla, direktiivien 97/7/EY, 2002/65/EY, 2005/60/EY ja 2006/48/EY muuttamisesta ja direktiivin 97/5/EY kumoamisesta. (Maksupalveludirektiivi)
- EY/2009/110 Euroopan parlamentin ja neuvoston direktiivi sähköisen rahan liikkeeseenlaskijalaitosten liiketoiminnan aloittamisesta, harjoittamisesta ja toiminnan vakauden valvonnasta, direktiivien 2005/60/EY ja 2006/48/EY muuttamisesta sekä direktiivin 2000/46/EY kumoamisesta. (Sähkörahadirektiivi)
- KOM (2001)66 Euroopan yhteisöjen komissio: Komission tiedonanto. Sähköinen kaupankäynti ja rahoituspalvelut.
- KOM (2003)718 Euroopan yhteisöjen komissio: Komission tiedonanto. Maksualan uusi oikeudellinen kehys sisämarkkinoilla.
- KOM (2004)679 Euroopan yhteisöjen komissio: Komission tiedonanto. EU:n uusi toimintasuunnitelma vuosiksi 2004–2007 muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten torjumiseksi.
- KOM (2008)627 Euroopan yhteisöjen komissio: Ehdotus. Euroopan parlamentin ja neuvoston direktiivi sähköisen rahan liikkeeseenlaskijoiden liiketoiminnan aloittamisesta, harjoittamisesta ja toiminnan vakauden valvonnasta, direktiivien 2005/60/EY ja 2006/48/EY muuttamisesta sekä direktiivin 2000/46/EY kumoamisesta. (2008/0190 COD)

- KOM (2010)245 Euroopan yhteisöjen komissio. Komission tiedonanto. Euroopan digitaalistrategia.
- MARKT/208/2001 Euroopan yhteisöjen komissio: Valmisteluasiakirja. Sisämarkkinoiden yhtenäisen maksualueen mahdolliset sääntelypuitteet MARKT/208/2001 – Rev.1. 7.5.2002.

### ***Suomi***

#### **Lait**

- 38/1978 Kuluttajansuojalaki
- 523/1999 Henkilötietolaki
- 121/2007 Laki luottolaitostoiminnasta
- 503/2008 Laki rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä
- 617/2009 Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista
- 290/2010 Maksupalvelulaki

#### **Muut**

- 21.8.2008/539 Valtioneuvoston päätös huoltovarmuuden tavoitteista
- HE 33/2002vp Hallituksen esitys Eduskunnalle laeiksi luottolaitostoiminnasta annetun lain ja eräiden siihen liittyvien lakien muuttamisesta.
- HE 169/2009vp Hallituksen esitys Eduskunnalle maksupalvelulaiksi ja eräiksi siihen liittyviksi laeiksi.
- KK 564/2010vp Eduskunta, Valtiopäiväasiakirjat. *Kirjallinen kysymys: Vanhusten pankkipalvelut yhtenäisen euromaksualueen käyttöönoton jälkeen.* Kysymys: Pauliina Viitamies/sd, 23.6.2010. Vastaus: Tapani Tölli, 15.7.2010.
- KK 620/2010vp Eduskunta, Valtiopäiväasiakirjat. *Kirjallinen kysymys: Sähköisen tunnistautumisen eriarvoisuuden korjaaminen.* Kysymys: Mikko Alatalo/kesk., 1.7.2010. Vastaus: Tapani Tölli, 23.7.2010.



Liikenne- ja viestintäministeriö (2003 <sup>a</sup> )	<i>Mobiili lähimaksaminen – nykykäyttö ja tulevaisuus.</i> Liikenne- ja viestintäministeriön julkaisuja 22/2003/V.
Liikenne- ja viestintäministeriö (2003 <sup>b</sup> )	<i>Sähköisen tunnistamisen menetelmät ja niiden sääntelyn tarve.</i> Liikenne- ja viestintäministeriön julkaisuja 44/2003.
Liikenne- ja viestintäministeriö (2007)	<i>Uusien sähköisten liiketoimintamallien kartoitus Eurooppa-USA-Aasia.</i> Liikenne- ja viestintäministeriön julkaisuja 40/2007.
Liikenne- ja viestintäministeriö (2008 <sup>a</sup> )	Sähköisen tunnistamisen kehittämissuostun 1. väliraportti arjen tietoyhteiskunnan neuvottelukunnalle: <i>Sähköisen tunnistamisen nykytila Suomessa.</i> 15.1.2008. Saatavilla osoitteessa <a href="http://www.arjentietoyhteiskunta.fi/files/36/Sahkoisen_tunnistamisen_nykytila_lopullinen_080115.pdf">http://www.arjentietoyhteiskunta.fi/files/36/Sahkoisen_tunnistamisen_nykytila_lopullinen_080115.pdf</a>
Liikenne- ja viestintäministeriö (2008 <sup>b</sup> )	Arjen tietoyhteiskunnan neuvottelukunta: <i>Vahvan sähköisen tunnistamisen kansalliset linjaukset.</i> 15.10.2008.
Liikenne- ja viestintäministeriö (2010)	<i>NFC- työryhmän väliraportti.</i> Kesäkuu 2010. Saatavilla osoitteessa <a href="http://www.arjentietoyhteiskunta.fi/files/290/Valiraportti-kesa2010_final_pdf.pdf">http://www.arjentietoyhteiskunta.fi/files/290/Valiraportti-kesa2010_final_pdf.pdf</a>
Oikeusministeriö (2008)	Oikeusministeriö: Työryhmämietintö 2008:11 – Maksupalvelut.
Valtioneuvosto (2009)	U4/2009vp. Valtioneuvoston kirjelmä eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi (sähkörahadirektiivi).
VM (2004)	E29/2004vp. Valtionvarainministeriö: E-kirjelmä koskien komission tiedonantoa KOM 2003(718). 30.3.2004.
VM (2010)	Valtiovarainministeriön tiedote 24.8.2010, Vaalikauden lopulla annettavat hallituksen esitykset. ID 71677.
<b><i>Ruotsi</i></b>	
Regeringskansliet (2010)	Genomförande av det nya e-penningdirektivet, DS 2010:27. Stockholm: Elanders Sverige AB.

## Lausunnot

- Euroopan talous- ja sosiaalikomitea (2004) *Euroopan Talous- ja sosiaalikomitean lausunto aiheesta Komission tiedonanto neuvostolle ja Euroopan parlamentille maksualan uudesta oikeudellisesta kehyksestä sisämarkkinoilla. (KOM(2003(718)). 2004/c302/03. Julkaistu Euroopan Unionin virallisessa lehdessä 7.12.2004.*
- Euroopan talous- ja sosiaalikomitea (2009) *Euroopan talous- ja sosiaalikomitean lausunto aiheesta ehdotus: Euroopan parlamentin ja neuvoston direktiivi sähköisen rahan liikkeeseenlaskijoiden liiketoiminnan aloittamisesta, harjoittamisesta ja toiminnan vakauden valvonnasta, direktiivien 2005/60/EY ja 2006/48/EY muuttamisesta sekä direktiivin 2000/46/EY kumoamisesta. (KOM2008(627)). 2009/c218/06. Julkaistu Euroopan Unionin virallisessa lehdessä 11.9.2009.*
- FiCom (2009<sup>a</sup>) Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry: *FiComin lausunto Valtioneuvoston sähkörahadirektiiviehdotuksesta laatimaan U-kirjelmään.* 24.2.2009. Saatavilla osoitteessa [http://www.ficom.fi/lausunnot/index\\_1.html?Id=1235473697.html](http://www.ficom.fi/lausunnot/index_1.html?Id=1235473697.html)
- FiCom (2009<sup>b</sup>) Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry: *FiComin lausunto maksupalvelulakia koskevasta HE-luonnoksesta.* 27.5.2009. Saatavilla osoitteessa [http://www.ficom.fi/lausunnot/index\\_1.html?Id=1243960481.html](http://www.ficom.fi/lausunnot/index_1.html?Id=1243960481.html)
- FiCom (2010) Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry: *FiComin lausunto liikennevaliokunnalle maksupalvelulaista HE 169/2009 ja eräistä siihen liittyvistä laeista.* 4.2.2010. Saatavilla osoitteessa [http://www.ficom.fi/lausunnot/index\\_1.html?Id=1265701806.html](http://www.ficom.fi/lausunnot/index_1.html?Id=1265701806.html)
- Gauriloff (2009) Gauriloff, Jouni: *Maksupalvelulaki, lausuntotiivistelmä.* Oikeusministeriön lausuntoja ja selvityksiä 2009:18.

- Keskuskauppa-  
kamari (2006) *Lausunto valtionvarainministeriölle ehdotuksesta maksupalveluita koskevaksi direktiiviksi KOM(205)603 final. 25.1.2006.* Saatavilla osoitteessa <http://www.keskuskauppakamari.fi/Eduunvalvonta/Lausunnot/Maksupalveluita-koskeva-direktiiviehdotus>
- Kuluttajavirasto (2004) *Lausunto Euroopan Komissiolle tiedonannosta KOM(2003)718. 13.2.2004. Dnro 2002/79/4783.* Saatavilla osoitteessa [http://www.kuluttajavirasto.fi/File/a8c9d3f5-92e1-4290-99be-e6970c5d94bd/041213\\_lausunto.pdf](http://www.kuluttajavirasto.fi/File/a8c9d3f5-92e1-4290-99be-e6970c5d94bd/041213_lausunto.pdf)
- LiVL 2/2010vp *Liikenne- ja viestintävaliokunnan lausunto HE 169/2009vp:stä (HE maksupalvelulainsäädännön muuttamisesta ja eräiksi siihen liittyviksi laeiksi).* 25.2.2010.

## **Lehti- ja internet-artikkelit**

- Aikavuori, Erja (2009). *Lainsäädännöllä sähköisen tunnistamisen kimppeun.* Tilisanomat 2/2009, s.67 - 69.
- Hämäläinen, Pertti (2010). *Mobiilivarmenne tulee taas.* Tietokone 8/2010, s.50 - 51.
- Kajantie, Sari (2010). *Miksi joku haluaa varastaa identiteetin?* Tiedosta 4/2010, s.16 - 17.
- Korhonen, Kari (2009). *Verkkomaksu kaipaa turvallisuutta.* Talouselämä 40/2009, s.8.
- Lehto, Tero (2010<sup>a</sup>). *”Norjassa ja Ruotsissa ei kukaan kysele, annetaanko keppiä vai porkkanaa”.* Tietokone 3/2010, s.18.
- Lehto, Tero (2010<sup>b</sup>). *Näin verkkopankkiin hyökätään.* Tietokone 3/2010, s.19.
- Lehto, Tero (2010<sup>c</sup>). *RSA: Verkkopankkien tietoturvaa voisi parantaa.* Tietokone 27.1.2010. Saatavilla osoitteessa [http://www.tietokone.fi/uutiset/rsa\\_verkkopankkien\\_tietoturvaa\\_voisi\\_parantaa](http://www.tietokone.fi/uutiset/rsa_verkkopankkien_tietoturvaa_voisi_parantaa)
- Linnake, Tuomas (2009). *Sähköinen tunnistus yrittää uudestaan.* IT Viikko 1.9.2009. Saatavilla osoitteessa <http://www.itviikko.fi/tietoturva/2009/09/01/sahkoinen-tunnistus-yrittää-uudestaan/200919216/7>
- Nikulainen, Kalevi (2005). *Pankkien mobiilimaksaminen matalalennossa: palvelujen ja käyttäjien määrä junnaa paikallaan.* IT Viikko 14/2005, s.6.

Nupponen, Sakari (2010). *Kännykkälippu uudistuu vapuksi*. Taloussanomat 27.4.2010. Saatavilla osoitteessa <http://www.taloussanomat.fi/liikenne/2010/04/27/kannykkalippu-uudistuu-vapuksi/20105991/12>

## **Muut lähteet**

ASIC (2008). Australian Securities & Investments Commission: *Consultation paper 90 - Review of the Electronic Funds Transfer Code of Conduct 2007/2008*. ASIC proposals, October 2008. Saatavilla osoitteessa [http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/CP-90-Review-of-Electronic-Funds-Transfer-Code-v1.pdf/\\$file/CP-90-Review-of-Electronic-Funds-Transfer-Code-v1.pdf](http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/CP-90-Review-of-Electronic-Funds-Transfer-Code-v1.pdf/$file/CP-90-Review-of-Electronic-Funds-Transfer-Code-v1.pdf)

European Payments Council (2009). *Customer-to-bank security good practices guide*. 397-08v1.1. Saatavilla osoitteessa [http://www.europeanpaymentscouncil.eu/knowledge\\_bank\\_download.cfm?file=EPC397-08%20v1%201%20C2Bsecurity%20good%20practices%20guide.pdf](http://www.europeanpaymentscouncil.eu/knowledge_bank_download.cfm?file=EPC397-08%20v1%201%20C2Bsecurity%20good%20practices%20guide.pdf)

Euroopan komissio: Sähköinen raha. Euroopan komission internetsivut, [http://ec.europa.eu/internal\\_market/payments/emoney/index\\_en.htm](http://ec.europa.eu/internal_market/payments/emoney/index_en.htm)

Euroopan komissio (2010). *Digitaalistrategia: komissiolta toimintasuunnitelma Euroopan elintason ja hyvinvoinnin tueksi*. IP/10/581. Lehdistötiedote [verkojulkaisu], 19.5.2010. Saatavilla osoitteessa <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/581&format=PDF&aged=1&language=FI>

FiCom (2008). Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry: Tietoa toimialasta. Langattomat lähiverkot ja tietoturvallisuus. 28.4.2008. Saatavilla osoitteessa [http://www.ficom.fi/tietoa/tietoa\\_4\\_1.html?Id=1156845988.html](http://www.ficom.fi/tietoa/tietoa_4_1.html?Id=1156845988.html)

Finanssialan Keskusliitto (2008). *Maksaminen suomessa ja Euroopassa*. 7.7.2008. Saatavilla osoitteessa [http://www.fkl.fi/materiaalipankki/julkaisut/Julkaisut/Maksaminen\\_Suomessa\\_ja\\_Euroopassa\\_07072008.pdf](http://www.fkl.fi/materiaalipankki/julkaisut/Julkaisut/Maksaminen_Suomessa_ja_Euroopassa_07072008.pdf)

Finanssialan Keskusliitto (2009). *Yhtenäinen Euromaksualue yrityksille*. 2/2009. Saatavilla osoitteessa [http://www.fkl.fi/teemasivut/sepa/vaikutukset\\_yritystoimintaan/Dokumentit/Sepa\\_yrityksille.pdf](http://www.fkl.fi/teemasivut/sepa/vaikutukset_yritystoimintaan/Dokumentit/Sepa_yrityksille.pdf)

- Finanssialan Keskusliitto (2010<sup>a</sup>). *Yhtenäisen euromaksualueen toteutuminen suomessa, Suomen kansallinen siirtymäsuunnitelma, versio 4*. 17.2.2010. Saatavilla osoitteessa [http://www.fkl.fi/teemasivut/sepa/tekninen\\_dokumentaatio/Dokumentit/SEPA\\_siirtymasuunnitelma\\_helmikuu\\_2010.pdf](http://www.fkl.fi/teemasivut/sepa/tekninen_dokumentaatio/Dokumentit/SEPA_siirtymasuunnitelma_helmikuu_2010.pdf)
- Finanssialan Keskusliitto (2010<sup>b</sup>). *Pankit suomessa 2009*. 20.4.2010. Saatavilla osoitteessa [http://www.fkl.fi/materiaalipankki/julkaisut/Julkaisut/Pankit\\_Suomessa\\_2009.pdf](http://www.fkl.fi/materiaalipankki/julkaisut/Julkaisut/Pankit_Suomessa_2009.pdf)
- Finanssialan Keskusliitto (2011). *Pankit suomessa 2010*. 5.4.2011. Saatavilla osoitteessa <http://www.fkl.fi/materiaalipankki/julkaisut/Julkaisut/Pankit%20Suomessa%202010.pdf>
- Finanssialan Keskusliiton ylläpitämä E-Lasku –sivusto, [www.e-lasku.info](http://www.e-lasku.info)
- Finanssivalvonnan internetsivut, <http://www.finanssivalvonta.fi/fi/Fiva/Valvottavat/Pages/Valvottavat.aspx>
- Karnouskos, Stamatis (2004). *Mobile payment: A journey through existing procedures and standardization initiatives*. IEEE Communication surveys 6(4): 44-66. Saatavilla osoitteessa [www.comsoc.org/livepubs/surveys/public/2004/oct/pdf/KARNOUSKOS.pdf](http://www.comsoc.org/livepubs/surveys/public/2004/oct/pdf/KARNOUSKOS.pdf)
- Kauppalehti (2010). *Kännykkälompakolle paha takapakki*. 3.6.2010. Saatavilla osoitteessa <http://www.kauppalehti.fi/5/i/talous/uutiset/etusivu/uutinen.jsp?oid=2010/06/34073&sort=false>
- Keskusrikospoliisi (2009). *Yrityksiin kohdistuvan rikollisuuden tilannekuva: Tietoturvallisuus ja maksuteknologia, 3.4.2009*. Julkaisun numero: RTP 164/213/09. Saatavilla osoitteessa [http://www.poliisi.fi/poliisi/krp/home.nsf/files/Teematilannekuva\\_kev%C3%A4t2009/\\$file/Teematilannekuva\\_kev%C3%A4t2009.pdf](http://www.poliisi.fi/poliisi/krp/home.nsf/files/Teematilannekuva_kev%C3%A4t2009/$file/Teematilannekuva_kev%C3%A4t2009.pdf)
- Kuluttajavirasto (2010). *Ajankohtaista kuluttajaoikeudesta 7/2010 - Teemana rahoituspalvelut*. [verkkolehti] 13.9.2010. Saatavilla osoitteessa [http://www.kuluttajavirasto.fi/File/a98d9c96-f579-4f3b-96dc-5542089d5f5e/1007\\_Rahoituspalvelut.pdf](http://www.kuluttajavirasto.fi/File/a98d9c96-f579-4f3b-96dc-5542089d5f5e/1007_Rahoituspalvelut.pdf)
- Lehto, Tero (2010<sup>d</sup>). *Verkkopankkirosvo vei rahat. Kuka maksaa?* [blogi]. Tietokone: 3.2.2010. Saatavilla osoitteessa <http://blogit.tietokone.fi/tietojakoneesta/2010/02/verkkopankkirosvo-vei-rah-at-kuka-maksaa/>
- Luottokunta (2010). *Kauppiasohje: Maksukorttialan tietoturvastandardin (PCI DSS) noudattaminen ja kauppiiaan velvollisuudet 1.5.2010 lukien*. Saatavilla osoitteessa <http://www.luottokunta.fi/portal/page/portal/9449A22994427105E044001B787C0255>

Luottokunta: Maksaminen internetissä. Luottokunnan internetsivut,  
[http://www.luottokunta.fi/fi/kortit\\_ja\\_setelit/ohjeita\\_kortinhaltijalle/maksaminen\\_internetissa#portal-rewrite?a=1:e=0:p=0/portal-rewrite#](http://www.luottokunta.fi/fi/kortit_ja_setelit/ohjeita_kortinhaltijalle/maksaminen_internetissa#portal-rewrite?a=1:e=0:p=0/portal-rewrite#)

Luottokunta: Verified By Visa. Luottokunnan internetsivut,  
[http://www.luottokunta.fi/fi/kortit\\_ja\\_setelit/visa/verified\\_by\\_visa](http://www.luottokunta.fi/fi/kortit_ja_setelit/visa/verified_by_visa)

Mobiilivarmenne.fi (2010). Mobiilivarmennus käynnistyy suomessa. Tiedote, 30.11.2010. Saatavilla osoitteessa: [http://www.mobiilivarmenne.fi/fi/fi\\_7.html#2](http://www.mobiilivarmenne.fi/fi/fi_7.html#2)

Nordea (2010<sup>a</sup>). Korttien sisältämät toiminnot ja sovellettavat ehdot 5/2010. Saatavilla osoitteessa [http://www.nordea.fi/sitemod/upload/root/fi\\_org/appx/fin/ehdot/MKYE900dl.pdf](http://www.nordea.fi/sitemod/upload/root/fi_org/appx/fin/ehdot/MKYE900dl.pdf)

Nordea (2010<sup>b</sup>). Pankkitunnuksilla käytettävien palveluiden yleiset sopimusehdot 5.2010. Saatavilla osoitteessa [http://www.nordea.fi/sitemod/upload/Root/fi\\_org/appx/fin/ehdot/MMST960DL.pdf](http://www.nordea.fi/sitemod/upload/Root/fi_org/appx/fin/ehdot/MMST960DL.pdf)

OECD (2006). *Online payment systems for E-Commerce, 2006*. DSTI/ICCP/IE(2004)18/FINAL. Saatavilla osoitteessa <http://www.oecd.org/dataoecd/37/19/36736056.pdf>

OP-Pohjola (2011). *Häiriö osuuspankin verkkopalveluissa*. Osuuspankin tiedote. Saatavilla osoitteessa <https://www.op.fi/op?cid=151424569&srcpl=4>

PayPalin internetsivut. *PayPal: Q4 2010 FastFacts*. Saatavilla osoitteessa [https://www.paypal-media.com/assets/pdf/fact\\_sheet/PP\\_FastFacts\\_Q410\\_0111.pdf](https://www.paypal-media.com/assets/pdf/fact_sheet/PP_FastFacts_Q410_0111.pdf)

Poliisi (2008). *Kelan tekemän tutkintapyynnön esitutkinta päättynyt*. Poliisin tiedotteet, 5/2008. Saatavilla osoitteessa <http://www.poliisi.fi/poliisi/bulletin.nsf/vwSearchView/161EC35E75C233BCC2257455003ECB03>

Ripatti, Kirsi – Iivarinen, Timo (2010). *SEPA- infrastruktuurin syntyminen suomessa*. BoF Online 6/2010. [verkkajulkaisu] Suomen pankki. Saatavilla osoitteessa [http://www.suomenpankki.fi/fi/julkaisut/selvitykset\\_ja\\_raportit/bof\\_online/Documents/BoF\\_Online\\_06\\_2010.pdf](http://www.suomenpankki.fi/fi/julkaisut/selvitykset_ja_raportit/bof_online/Documents/BoF_Online_06_2010.pdf)

Suomen Asiakastieto Oy (2011). *Rekisterimuutos paljasti maksuhäiriövelkojen todellisen määrän.*

Lehdistötiedote, 12.1.2011. Saatavilla osoitteessa

<http://www.asiakastieto.fi/asiakastieto/ajankohtaista/index.jsp?T=nu&A=422>

Tilastokeskus (2010). Suomen virallinen tilasto (SVT): Tieto- ja viestintätekniiikan käyttö [verkkajulkaisu].

Helsinki: Tilastokeskus. Saatavilla osoitteessa: [http://tilastokeskus.fi/til/sutivi/2010/sutivi\\_2010\\_2010-10-26\\_tie\\_001\\_fi.html](http://tilastokeskus.fi/til/sutivi/2010/sutivi_2010_2010-10-26_tie_001_fi.html)

Tilastokeskus (2011). Suomen virallinen tilasto (SVT): Kuluttajabarometri. Liitekuvio 16. Matkapuhelimien lukumäärät kotitalouksissa, helmikuu 2011 [verkkajulkaisu]. Helsinki: Tilastokeskus. Saatavilla osoitteessa:

[http://tilastokeskus.fi/til/kbar/2011/03/kbar\\_2011\\_03\\_2011-03-28\\_kuv\\_016\\_fi.html](http://tilastokeskus.fi/til/kbar/2011/03/kbar_2011_03_2011-03-28_kuv_016_fi.html)

Tyree, Alan L. (2003). *Mistaken internet payments* [online]. 3/2003. Saatavilla osoitteessa

<http://www2.austlii.edu.au/~alan/mistaken-epayments.html>

Visa:n internetsivut, <http://www.visa.fi>

Väestörekisterikeskus: Varmenteet. Väestörekisterikeskuksen internetsivut,

<http://www.vaestorekisterikeskus.fi/default.aspx?id=145>

Väestörekisterikeskuksen tiedote: Marraskuun loppuun mennessä kansalaisvarmenteita oli myönnetty yhteensä 341.800:lle henkilölle. Väestörekisterikeskuksen FINEID.FI -internetsivut,

<http://fineid.fi/default.aspx?site=9&docid=4035>

## **Oikeuskäytäntö**

KKO 1989:98

KKO 2006:81

KKO 2007:6

## LYHENNELUETTELO

ASIC	Australian Securities & Investments Commission
EPC	European Payments Council
EU	Euroopan Unioni
EY	Euroopan yhteisö
HE	Hallituksen esitys
HSL	Helsingin seudun liikenne
HO	Hovioikeus
IT	Information Technology
KK	Kirjallinen kysymys
KKO	Korkein oikeus
KSL	Kuluttajansuojalaki (38/1978)
KOM	Euroopan yhteisöjen komissio
LiV	Liikenne- ja viestintävaliokunta
LuottoIL	Laki luottolaitostoiminnasta (121/2007)
MPL	Maksupalvelulaki (290/2010)
NFC	Near Field Communication
OECD	Organization for Economic Co-operation and Development
OM	Oikeusministeriö
PCI	Peripheral Component Interconnect
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification
SEPA	Single European Payment Area
SSL	Secure Sockets Layer
TUPAS	Tunnistuspalvelu asiointipalveluntuottajille
VM	Valtionvarainministeriö



# 1. JOHDANTO

## 1.1 Tutkielman taustaa

Niin globaalissa, eurooppalaisessa kuin myös kotimaisessa maksuympäristössä on viime vuosikymmenten aikana tapahtunut useita merkittäviä muutoksia. Teknologinen kehitys ja sen yhteydessä tapahtuneet innovaatiot myös maksamisen alueella ovat olleet suurin yksittäinen tekijä sille, että perinteisten fyysisten maksutapahtumien rinnalle on kehittynyt monia muitakin maksamisen muotoja. Maksaminen on siirtynyt yhä kasvavassa määrin sähköiseen ympäristöön: nykyään maksutapahtumat suoritetaan niiden luonteesta riippumatta entistä useammin elektronisissa maksuliikejärjestelmissä tietokoneen tai muun päätelaitteen avulla. Ottaen huomioon sen, että esimerkiksi pelkästään Euroopassa yli 250 miljoonaa ihmistä käyttää internetiä päivittäin ja käytännössä katsoen kaikilla on käytössään matkapuhelin,<sup>1</sup> tämä on varsin ymmärrettävää.

Verrattuna perinteisiin fyysisiin maksutapahtumiin, sähköinen maksaminen on nopeampaa, vaivattomampaa sekä kustannustehokkaampaa useimmille maksuverkoston toimijoille. Nämä ovat tärkeimpiä syitä sille, että paine ja halu sähköisen maksamisen kehittämiseen on kasvanut entisestään. Myös kaupankäynnin kansainvälistyminen sekä toimialojen lisääntynyt konvergenssi ovat omalta osaltaan vaikuttaneet maksukäytäntöjen muuttumiseen. Lisäksi Eurooppalaisesta näkökulmasta myös unionin integraatitavoitteet ovat muokanneet vahvasti maksuympäristön kehityssuuntaa. Euroalueella ollaan oltu sähköistä maksamista tukevan ja edesauttavan politiikan kannalla, samalla tavoitteena kuitenkin se, että jäsenmaiden maksukäytännöt muodostuvat mahdollisimman yhtenäisiksi rajat ylittävän kilpailun edistämiseksi.

Nämä kaikki tekijät yhdistettynä maksunvälittäjien kirjon monipuolistumiseen ovat samalla johtaneet kuitenkin siihen, että myös maksamiseen liittyvän oikeudellisen sääntelyn tarve on kasvanut. Taloudelliseen merkitykseen verrattuna rahasuorituksen tekemistä koskevia säännöksiä on historiallisesti ollut vähän.<sup>2</sup> Tämän lisäksi sääntely on ollut melko hajanaista sekä alueellisesti että myös eri maksujärjestelmien välillä. Maksuympäristön kehittyessä kuitenkin yhä vahvemmin globaalimpaan suuntaan tarvitaan aiempaa yhtenäisempi oikeudellinen kehys pelisääntöjen varmistamiseksi. Lainsäädännön ohella keskeinen merkitys toimivan kokonaisuuden

---

<sup>1</sup> KOM (2010)245, s.4.

<sup>2</sup> Terämaa, 2001, s.249.

muodostamiseksi on osaltaan myös tehokkaalla itsesääntelyllä, yhtenäisillä maksuliikennealan standardeilla sekä maksujärjestelmän osapuolten välisillä sopimuksilla.

Euroopan komissio on viime aikoina ottanut johtavan roolin yhtenäisen Eurooppalaisen maksuinfrastruktuurin luomisessa, joka on johtanut siihen että ylikansallisen lainsäädännön määrä maksamisen alueella on viime aikoina lisääntynyt. Mm. maksupalveludirektiivi (2007/64/EY) on implementoitu jo suurimpaan osaan jäsenmaista ja uusi sähkörahadirektiivi (2009/110/EY) on saatettava jäsenmaissa voimaan vielä myöhemmin tänä vuonna. Lisäksi komissio on pyrkinyt kannanotoissaan ottamaan huomioon myös muut maksuympäristöön ja maksamiseen liittyvät merkittävät oikeudelliset kysymykset. Yhtenäinen maksualan sääntely on osa SEPA:a, uutta yhtenäistä eurooppalaista maksualueetta, jonka tarkoituksena on edistää kaupankäyntiä sisämarkkinoilla. Sääntelyn lähtökohtana on komission ja jäsenmaiden pyrkimys koordinoituihin sekä toimiviin maksupalveluihin koko unionin alueella.<sup>3</sup>

Kokonaisuutena nämä uudet pelisäännöt selkeyttävät ja yhtenäistävät oikeudellista kehystä maksumarkkinoilla. Kuitenkin ne toisaalta myös nostavat esiin kysymyksiä aiheuttaessaan sellaisia muutoksia vallitsevaan tilanteeseen, jotka eivät välttämättä ole lähtökohtaisesti suosiollisia kaikille sähköisen maksuympäristön toimijoille. Toivottavaa olisi, ettei sääntely muodostuisi esteeksi uusille innovaatioille, hidastaisi paikallista kehitystä, vaikeuttaisi uusien toimijoiden tuloa markkinoille tai myöskään olisi epätasapainossa markkinoiden osapuolten, eli tässä tapauksessa palveluntarjoajien ja maksupalvelun käyttäjien, erityisesti kuluttajien osalta, kunkin ryhmän neuvotteluaseman huomioiden. Lisäksi, vaikka sääntelyn tulisi olla em. joustavaa, toisaalta yksityiskohtiin mentäessä olisi tärkeää että se olisi toisaalta myös riittävän selkeää, jotta tarpeettomalta tulkinnanvaraisuudelta sekä oikeudelliselta epävarmuudelta pystyttäisiin välttymään.

Sähköisen maksamisen alueella on sääntely-ympäristössä tapahtuneiden muutosten lisäksi ollut viime aikoina havaittavissa muutamia muitakin epävarmuustekijöitä. Jatkuva verkkorikollisuuden kasvu ja rikollisten käyttämien tekniikoiden kehittyminen on nähty yhdeksi suurimmista sähköistä kaupankäyntiä ja -maksuliikennettä haittaavista yksittäisistä tekijöistä. Tästä syystä tietoturvallisuuden merkitys maksuympäristössä on viime aikoina noussut korostuneen keskeiseen asemaan. Lisäksi, vaikka maksuliikenteen sähköistyminen on nähty pääasiassa positiivisena ilmiönä sekä maksupalvelujen käyttäjien kuin palveluntarjoajienkin kannalta, joidenkin erityisryhmien

---

<sup>3</sup> Regeringskansliet, 2010, s. 166.

osalta on noussut toisaalta esiin huolia siitä onko ko. ryhmien asemaa otettu alueen kehityksessä riittävästi huomioon.

## **1.2 Tutkielman tavoitteet ja rajaukset**

Työni tarkoituksena on tehdä selvitys yleisimmin käytössä olevista sähköisistä maksutavoista ja maksuympäristössä vallitsevasta oikeudellisesta tilanteesta sekä sen mahdollisista puutteista tai siitä johtuvista käytännön ongelmista ja niiden seurauksista sähköisen maksamisen alueella. Pyrin punnitsemaan kokonaisuutta siitä näkökulmasta, miten tämänhetkinen sääntelykehys ottaa maksumarkkinoiden eri osapuolten intressit huomioon heidän sopimusoikeudellisen neuvotteluasemansa huomioiden. Lisäksi pyrin selvittämään, miten vastuu osapuolten välillä jakautuu erityisesti sähköiseen maksamiseen liittyvissä erityiskysymyksissä. Lähtökohtani on tuottaa mahdollisimman objektiivinen ja alueen olennaisimpia kysymyksiä kattavasti tarkasteleva kokonaisuus.

Käsittelen aihetta ensisijaisesti kotimaisesta näkökulmasta. Erityisesti sääntelyn osalta pyrin lähtökohtaisesti pitäytymään kansallisen tai vaihtoehtoisesti sen perustana olevan ylikansallisen oikeuden alueella. Kuitenkin esimerkiksi mahdollisissa ristiriitatilanteissa sekä tulkinnallisissa kysymyksissä pyrin mahdollisuuksien mukaan hakemaan tukea myös kansainväliseltä alueelta. Maksuvälineiden ja maksamisen kehityssuuntausten osalta tarkasteluni on osittain myös laajalaisempaa. Maksamisen teknistä toimintaympäristöä käsittelen varsin pintapuolisesti: tämä toisaalta osittain työn juridisesta luonteesta sekä toisaalta työn laajuudelle asetettujen kriteerien olemassaolosta johtuen. Lisäksi, useimmiten sähköiseen maksamiseen liittyvässä sääntelyssä pyrkimyksenä on myös teknologianeutraaliuden periaate, jolloin käytettävien teknologisten ratkaisujen ei pitäisi lähtökohtaisesti vaikuttaa olennaisesti oikeudelliseen tulkintaan. Rajaan käsittelyni ulkopuolelle myös maksamiseen liittyvät rikosoikeudelliset seuraamukset, huolimatta siitä että ne saattavat olla varsin merkittävässäkin roolissa tiettyjen käsiteltävien kokonaisuuksien alueella.

## **1.3 Tutkielman rakenne**

Johdannon ja käsitteiden määrittelyn jälkeen luon luvussa kolme yleiskatsauksen sähköisen maksamisen toimintaympäristöön ja sen viimeaikaiseen kehitykseen. Pyrin luvussa havainnollistamaan, mitkä tekijät vaikuttavat sähköisen maksutavan valintaan maksupalvelun

käyttäjien näkökulmasta. Tämän jälkeen esittelen joitakin tällä hetkellä yleisimmin käytössä olevia tai muuten tutkimukseni kannalta merkittävimpänä pitämiäni sähköisiä maksutapoja sekä pyrin arvioimaan niiden vahvuuksia ja rajoituksia sähköisen maksamisen moninaisten tavoitteiden toteuttamisessa. Tämä on mielestäni olennaista aiheen kokonaisvaltaisen hahmottamisen kannalta.

Luvussa neljä tarkastelen sähköisen maksamisen varsin monitahoista sääntelykehikkoa kotimaisesta näkökulmasta, ylikansalliset suuntaviivat kuitenkin huomioiden. Arvioin ensin sääntelytavoitteiden moninaisuuden sekä toimintaympäristön erityispiirteiden vaikutusta sääntelykehikon muodostumiseen. Tämän jälkeen pyrin hahmottamaan sähköisten maksujen kannalta tärkeimpiin osa-alueisiin liittyvän sääntelyn kehitystä ja nykytilaa sekä sen mahdollisia puutteita. Lainsäädännön lisäksi pyrin ottamaan huomioon myös muun merkittävän sääntelyn, kuten erilaisten maksuyhteisöjen tai valvontaelinten laatimien standardien vaikutuksen kullakin osa-alueella. Viimeiseksi arvioin vielä luvussa maksusuorituksen taustalla olevan perussuhteen sekä maksupalvelusta mahdollisesti tehtyjen sopimusten merkitystä ja niillä vaikuttamisen mahdollisuutta osapuolten välisten vastuiden määrittelyssä.

Luvussa viisi nostan esiin kysymyksiä, jotka ovat mielestäni ongelmallisia tai muuten korostuneen mielenkiintoisia sähköisessä maksamisen alueella. Ensimmäisenä käsittelen luvussa maksamisen turvallisuutta ja siihen liittyviä kysymyksiä. Näistä sähköisessä maksamisessa korostuvat maksujärjestelmän osapuolten identifioimisen eli tunnistamisen merkitys sekä tietoturvallisuuskysymykset. Selvitän ensin luvussa 5.1.1 henkilön tunnistamisen juridisia velvoitteita, eri identifioimismenetelmien luotettavuuden kriteereitä sekä identiteetin tunnistamisen merkitystä maksutapahtuman sitovuuden kannalta. Tämän jälkeen käsittelen identiteettierohdyksen seurauksia ja riskinjakoa erehdystilanteissa sekä pyrin arvioimaan erilaisia tunnistamismenetelmiä maksujärjestelmittäin niiden tämänhetkisten yleisesti käytössä olevien tunnistamiskäytäntöjen osalta. Seuraavaksi siirryn luvussa 5.1.2 käsittelemään tietoturvallisuutta: otan esille pääkohtia tietoturvallisuuteen ja luotettavaan maksamisen tekniikkaan liittyvistä asioista ja etenkin siitä, miten sekä yksittäisten maksutapahtumien että tietojen säilyttämisen osalta vastuuriskit jakautuvat osapuolten kesken.

Toinen kokonaisuus viidennessä luvussa on itse maksutapahtumaan ja sen sääntelyyn liittyvät erityiskysymykset. Näistä käsittelen aluksi luvussa 5.2.1 tiettyjen virheiden, joko itse maksutapahtumassa tai siihen liittyvän velvoitteen täyttämässä, vaikutusta maksutapahtuman sitovuuteen, joiden osalta nykyinen sääntely voidaan nähdä epäsuhtaisena tai potentiaalisen

ongelmallisena. Ensin otan esille yksilöivän tunnisteiden korostuneen merkityksen suhteessa perusteettoman edun palautuksen käytön hankaluuteen oikeuskeinona virheen sattuessa. Sen jälkeen tarkastelen maksupalveludirektiivin myötä implementoitua velkoja-aloitteisten maksujen erityistä palautusoikeutta, josta siirryn punnitsemaan maksutyypikohtaisia eroavaisuuksia maksutapahtumiin liittyvissä yhteisvastuukysymyksissä. Tämän jälkeen tarkastelen vielä luvussa 5.2.2 sääntelyä sekä osapuolten välistä vastuunjakoa teknisissä ongelmatilanteissa, kuten esimerkiksi silloin kun maksuyhteys katkeaa tai maksuverkko pettää joko tilapäisesti tai pitemmällä aikavälillä.

Viidennen luvun kolmannessa ja viimeisessä osiossa tarkastelen vielä sääntelystä, toisaalta sen tiukkuudesta ja toisaalta puutteellisuudesta tai siitä johtuvasta oikeudellisesta epävarmuudesta aiheutuvia ongelmia tietyille intressitahoille. Ensin käsittelen luvussa 5.3.1 lähinnä ylikansallisen sääntelyn ohjaavaa vaikutusta muun muassa ns. uudempien maksutapojen käyttöönottoa sekä käyttötarkoitusta silmällä pitäen. Tämän jälkeen pohdin vielä luvussa 5.3.2 sähköisen maksamisen ja sen vahvistuneen aseman merkitystä tiettyjen yhteiskuntaryhmien näkökulmasta, joiden osalta maksamisen kokonaisvaltainen sähköistymiskehitys uhkaa hankaloittaa tai on jo hankaloittanut asiointia sekä maksuliikenteen suorittamista aina peruspankkipalveluista lähtien.

Tutkielman viimeisessä, kuudennessa luvussa käyn vielä läpi aiempien kappaleiden pääkohdat, erityisesti osapuolten välistä vastuunjakoa silmällä pitäen. Tarkastelen erityisesti sitä, miten nykyinen lainsäädäntö onnistuu kokonaisuutena ottamaan alueen moninaiset tavoitteet huomioon. Viimeinen luku toimii kokoavana osiona, josta on nähtävissä teoksen keskeinen sisältö.

## 2. MÄÄRITELMÄT

*Maksu* on velvoiteoikeuden yleisen määritelmän mukaan rahavelvoitteeseen liittyvä täyttämistoimi. Maksutapahtuma on varainsiirtotapahtuma, jolla rahavelvoitteen olemassaolo saadaan velallisen ja velkojan välillä lopullisesti lakkaamaan. Maksu katsotaan täten oikeustoimeksi. Oikeudellisesti maksun kannalta ei ole merkitystä sillä, kenen välillä varainsiirtotapahtuma suoritetaan: maksun määritelmän täyttää myös täten varojen siirto maksujenvälitysjärjestelmässä ilman, että varojen omistaja vaihtuu, esimerkkinä tästä henkilön varojen siirto omien tiliensä välillä luottolaitoksesta toiseen.<sup>4</sup>

*Maksujärjestelmä* tai maksujenvälitysjärjestelmä on sellaisten menetelmien, välineiden ja järjestelmien kokonaisuus, joiden avulla suoritetaan maksuja. Maksupalvelulaissa (290/2010) maksujärjestelmä määritellään ”*sääntöihin perustuvaksi järjestelmäksi, jossa määritetään tai toteutetaan rahamääräisiä velvoitteita, taikka siirretään maksutapahtumien katteet*”. Maksujärjestelmällä on maksunvälityksessä osapuolten välillä kaksi päätehtävää, maksun kohteena olevan varallisuuden siirtäminen saajalle sekä suoritusta koskevan tiedon välittäminen saajalle. Maksujärjestelmät voivat olla joko suljettuja yhden välittäjän järjestelmiä tai avoimia järjestelmiä, joissa voi olla useitakin välittäjiä osallisena. Suljetuille järjestelmille on usein ominaista yhteensopimattomuus muihin järjestelmiin. Niistä esimerkkinä monet sähköisen rahan järjestelmät. Joka tapauksessa, maksujärjestelmässä on oltava maksajan ja vastaanottajan lisäksi aina vähintään yksi perusvelkasuhteen ulkopuolinen taho, joka huolehtii maksun välittämiseen liittyvistä tehtävistä. Käytetyt maksujärjestelmät liittyvät usein kansallisiin rahajärjestelmiin ja palvelevat kunkin valtion yleisesti käytettävissä olevia maksutapoja. Tämän takia eri maksujärjestelmien rakenne ja jopa perusteiltaan samanlaisten maksumuotojen käytännön toteutustapa vaihtelee maittain. Kansainväliset rajat ylittävissä maksuissa erot kansallisten maksujärjestelmien välillä vaativatkin usein käsittely- ja muunnostehtäviä, jotka vievät aikaa sekä lisäävät kuluja ja virheiden mahdollisuutta.<sup>5</sup>

*Sähköinen maksujärjestelmä* on maksujärjestelmä, jossa maksutapahtuma sekä sitä seuraavat rahan liikkeet suoritetaan sähköisessä ympäristössä.

---

<sup>4</sup> Terämaa, 2001, s.251.

<sup>5</sup> Terämaa, 2001, s.274 - 277.

*Palveluntarjoaja* on luonnollinen henkilö, yksityishenkilö tai julkinen oikeushenkilö, joka tuloa tai muuta taloudellista hyötyä saadakseen ammattimaisesti tarjoaa maksupalveluita.<sup>6</sup>

*Maksuväline* on maksukortti tai muu käyttäjäkohtainen väline tai menettelytapa tai näiden yhdistelmä, jonka käyttämisestä maksutoimeksiantoihin maksupalvelun käyttäjä ja palveluntarjoaja ovat sopineet.<sup>7</sup>

---

<sup>6</sup> 290/2010, 8.2§

<sup>7</sup> 290/2010, 8.9§

### 3. SÄHKÖISET MAKSUJÄRJESTELMÄT JA YLEISIMMÄT SÄHKÖISET MAKSUTAVAT

#### 3.1 Yleistä sähköisestä maksamisesta ja maksujärjestelmistä: maksujärjestelmän valinta

Maksujärjestelmien tärkein tehtävä on tarjota keino siirtää varallisuutta talouden eri osapuolten välillä. Huolimatta maksun funktion tärkeydestä, yhtä kaikkiin maksutapahtumiin optimaalisesti soveltuvaa maksujärjestelmää ei ole kehitetty vaan markkinoilla on useita toisistaan poikkeavia järjestelmäratkaisuja. Maksujärjestelmä joka soveltuu tiettyyn tilanteeseen voi olla vastaavasti sopimaton toisen tyyppisen maksun suorittamiseen. Se, mikä järjestelmä soveltuu kunkin tyyppiseen varallisuuden siirtoon ja kullekin käyttäjälle parhaiten, riippuu useista seikoista: itse maksujärjestelmän ominaisuuksista, sen käyttöön liittyvistä kustannuksista sekä toisaalta myös käyttötarkoituksesta.

Mm. Turban et. al ovat yksilöineet Evansin ja Schmalenseen <sup>8</sup> julkaisun pohjalta keskeisiä, joskus menestymisen kannalta jopa ratkaisevia yksittäisiä sähköisten maksujärjestelmien ominaisuuksia. <sup>9</sup>

Näitä ovat muun muassa:

- *Itsenäisyys*: Järjestelmät, jotka velvoittavat käyttäjän asentamaan erityisiä lisäkomponentteja, kuten ohjelmistoja tai laitteistoja toimiakseen, menestyvät epätodennäköisemmin.
- *Yhteentoimivuus*: Sähköisen maksujärjestelmän täytyy olla teknisesti yhteensopiva jo olemassa olevien järjestelmien kanssa sekä tukea yleisimpiä käyttöalustoja.
- *Käytön helppous*: Maksujärjestelmän täytyy olla riittävän helppokäyttöinen, jotta se voisi saavuttaa suurten massojen suosion.
- *Turvallisuus*: Kuinka turvallinen järjestelmä on ja mitkä ovat turvallisuusrikkomuksen seuraukset osapuolille? Jos riski maksajalle on suurempi kuin maksun vastaanottajalle (kauppiaalle), maksaja ei välttämättä halua käyttää ko. järjestelmää.
- *Anonymiteetti*: Jotkut ostajat haluavat heidän henkilöllisyytensä ja transaktioidensa pysyvän anonyymeinä.
- *Kansainvälisyys*: Sähköinen maksuympäristö on maailmanlaajuinen. Ideaalina maksutavan olisi hyvä olla helposti sovitettavissa sekä paikallisiin toimintamalleihin että täyttää myös kansainväliset vaatimukset.

---

<sup>8</sup> Ks. Evans, David S. – Schmalensee, Richard (2005). *Paying with Plastic: The digital revolution in buying and borrowing*. Cambridge, MA: MIT Press, cop.

<sup>9</sup> Turban et al., 2010, s.525.



Kuitenkaan edes sinänsä ominaisuuksiltaan hyvänkään maksujärjestelmän suosio ei ole vielä taattu. Vaikka perustoiminnot olisivatkin olemassa, tarvitaan myös käyttömahdollisuuksien kasvua.<sup>10</sup> Maksujärjestelmän menestyksen esteeksi tai ainakin hidasteeksi voi koitua ns. Muna-ja-kana – ongelma käyttäjien ja maksupalvelujen välillä: uusien innovaatioiden täytyy menestyäkseen hyödyttää kaikkia osapuolia. Kauppiat eivät omaksu maksutapaa, jota vain harva ostaja käyttää. Toisaalta ostajat taas eivät ota vastaavasti uusia maksutapoja käyttöön, jos niiden käyttömahdollisuudet kauppiaiden palveluissa ovat rajoitetut. Useimmiten viekin vuosia, ennen kuin mikään maksujärjestelmä saavuttaa yleisen hyväksynnän.<sup>11</sup> Osittain tästä syystä perinteisemmät maksutavat ovat säilyttäneet suosionsa siitä huolimatta, että sähköisen maksamisen vaihtoehdot ovat monipuolistuneet.<sup>12</sup>

Minkä tahansa maksujärjestelmän käyttöön liittyy sekä suoria että epäsuoria kustannuksia sen käyttäjille. Suoria kustannuksia ovat palveluntarjoajien tai vaihtoehtoisesti kauppiaiden veloittamat palkkiot maksujärjestelmän käytöstä, epäsuorat kustannukset liittyvät mm. transaktioiden kompleksisuuteen, nopeuteen, riskitekijöihin sekä vaihtoehtoiskustannuksiin.<sup>13</sup> Myös kaikki nämä tekijät vaikuttavat maksutavan valintaan.

Ominaisuuksien sekä kustannustekijöiden ohella olennaista on myös se, minkä tyyppiseen maksamiseen maksujärjestelmää on tarkoitus käyttää. Maksamisetäisyyden perusteella sähköiset maksut voidaan jakaa lähi- ja etämaksamiseen. Perinteisesti sähköinen maksaminen on ollut etämaksamista, jossa transaktiot tukeutuvat maksutietojen välittämiseen ulkoisen tietoliikenneverkon kautta. Etämaksuissa maksun vastaanottaja voi olla hyvinkin jopa täysin toisella puolella maailmaa. Sen vastakohta, (kontaktiton) lähimaksaminen on transaktioiden tekemistä lähikommunikaatiotekniikan<sup>14</sup> avulla.<sup>15</sup> Ko. transaktiot voivat perustua suoraan arvon siirtämiseen päätelaitteesta kauppiaan maksupäätteeseen tai vastaavasti käyttäjän identifiointiin ja taustajärjestelmissä tapahtuvaan arvon siirtoon. Kontaktittomien tekniikoiden käyttö on ollut suosituinta pieniarvoisten ostosten kuten matkalippujen maksamisessa, jossa lähimaksamista on

---

<sup>10</sup> Nikulainen, IT Viikko 7.4.2005.

<sup>11</sup> Esimerkiksi luottokortit esiteltiin yleisölle 1950-luvulla mutta otettiin laajamittaiseen käyttöön vasta 1980-luvulla.

<sup>12</sup> Turban et al., 2010, s.525.

<sup>13</sup> OECD, 2006, s.6.

<sup>14</sup> Maksamista jossa kaupan maksupäätteen ja ostajan päätelaitteen välillä ei käytetä ulkoista tietoliikenneverkkoa, esimerkiksi mm. RFID-, Bluetooth- sekä infrapunateknologiaa käyttävät lähikommunikaatiotekniikat.

<sup>15</sup> Liikenne- ja viestintäministeriö, 2003<sup>a</sup>, s.2.

käytetty korvaamaan aikaa vieviä, vähäarvoisia käteismaksuja.<sup>16 17</sup> Sillä voisi yleistyessään olla kuitenkin runsaasti muitakin potentiaalisia sovellusmahdollisuuksia sähköisen maksamisen sekä tunnistamisen alueella.

Maksut voidaan jakaa maksun luonteen mukaan myös yksittäisen maksutapahtuman *suuruuden* perusteella mikro- tai nanomaksuihin ja niitä suurempiin maksuihin. Maksujen rajoille ei ole standardimääritelmää vaan se, mitä pidetään mikromaksun rahamääräisenä rajana, vaihtelee: esimerkiksi OECD:n julkaisussa mikromaksut määritellään alle 5€ suuruisiksi, joissain lähteissä rajana käytetään vaihtoehtoisesti myös muita summia.<sup>18</sup> Yleisenä lähtökohdana voidaan kuitenkin pitää sitä, että mikromaksut ovat rahamääräisesti pieniä maksuja.<sup>19</sup> Niitä käytetään esim. digitaalisen sisällön, kuten mm. musiikkiraitojen, pelien, lehtiartikkelien ym. ostamiseen. Kun suurissa maksuissa käyttäjien kannalta tärkeimpiä ovat turvallisuuteen liittyvät seikat, pienissä maksuissa korostuvat taas erityisesti maksamiseen liittyvät kulut, maksujärjestelmän käytön helppous sekä mahdollisesti myös maksajan anonymiteetti. Perinteiset maksujärjestelmät soveltuvat varsin heikosti kertaluontoisiin mikromaksuihin niiden suhteellisen korkeiden transaktiokustannusten (30 - 40 % ostoksen hinnasta) tai vaihtoehtoisesti raskaiden tunnistusmenetelmien takia. Sekä erilaisia maksutilejä että myös aivan uusia maksujenvälityspalveluita on kehitelty vastaamaan mikromaksujen tarpeisiin. Kuitenkaan kustannustehokkaita, kansainvälisiä maksujärjestelmiä erittäin pieniin maksutapahtumiin ei ole vielä kehitetty, vaan sovellukset ovat tällä hetkellä paikallisia.<sup>20</sup>

---

<sup>16</sup> Liikenne- ja viestintäministeriö, 2010, s.6.

<sup>17</sup> Tämän takia kontaktiton lähimaksaminen on kehittynyt keskimääräistä paremmin maissa, jossa käteisen käyttö on ollut keskimääräistä yleisempää. Sen sijaan Pohjoismaiden kaltaisissa, runsaasti luottokortteja käyttävissä maissa se on kehittynyt hitaammin. (Liikenne- ja viestintäministeriö, 2010, s.6.)

<sup>18</sup> Esimerkiksi Turban et al. (2010) luokittelee mikromaksuiksi alle \$5 maksutapahtumat. Hyppönen (2009, s.33) puolestaan katsoo peukalosääntönä olevan, että \$2 ja sitä pienemmät maksut ovat mikromaksuja.

<sup>19</sup> KOM (2003)718, s.10.

<sup>20</sup> OECD, 2006, s.5.

## 3.2 Yleisimpiä sähköisiä maksutapoja

Sähköisestä kaupasta puhuttaessa on usein esitetty näkemys siitä, ettei täydellistä verkkomaksamiseen soveltuvaa maksutapaa toistaiseksi ole.<sup>21</sup> Lisäksi ihmisten maksutottumukset ovat erilaisia sekä kehittyvät hitaasti, joka vaikuttaa osaltaan uusien maksutapojen omaksumiseen. Eri maksutapoja onkin perinteisesti käytetty erilaisiin maksamisen tarpeisiin ja käyttö vaihtelee suurestikin maakohtaisten tai alueellisten tapojen sekä toimialojen ominaisuuksien mukaan.<sup>22</sup> Seuraavassa on esitelty tällä hetkellä yleisimpiä sähköisiä maksutapoja, niiden käyttömahdollisuuksia sekä etuja ja rajoituksia.

### 3.2.1 Maksaminen verkossa luotto- tai muun kortin tunnistetietojen avulla

Luottokortin ja sen tunnistetietojen käyttö sähköisessä maksamisessa perustuu vakiintuneeseen käytäntöön. Luottokorttimaksaminen onkin edelleen kansainvälisesti *sähköisen kaupan selvästi yleisin maksutapa* menettelyn puutteellisuudesta huolimatta. Se on käytännöllinen maksutapa erityisesti sellaisissa etämaksutapahtumissa, joissa maksu suoritetaan kansallisten rajojen yli ja muut maksutapahtuman osapuolten käyttämät maksujärjestelmät eivät ole yhteensopivia keskenään. Joidenkin arvioiden mukaan luottokorttimaksun käyttämistä on maailmanlaajuisesti jopa yli 90 % tasolla kaikista verkkokaupankäynnin transaktioista.<sup>23</sup> Euroopassa ko. käyttöaste on keskimäärin jonkun verran matalampi, vaikkakin toisaalta erot valtioiden sisäisten maksukäytäntöjen välillä ovat merkittäviä.<sup>24</sup> Myös muiden korttien suosio verkkomaksamisessa on kasvanut viime aikoina, ja joissain maissa esimerkiksi debit -kortti onkin nykyisin laajalti käytetty vaihtoehto verkkomaksamiseen.<sup>25</sup>

Teknisesti korttimaksu verkossa tapahtuu siten, että maksun suorittaja ilmoittaa maksun vastaanottajalle korttinsa numeron ja maksun vastaanottaja muodostaa veloitustapahtuman tämän numeron sekä muiden maksuvelvoitetta koskevien tietojen perusteella. Maksun vastaanottaja

---

<sup>21</sup> Terämaa, 2001, s.248.

<sup>22</sup> OECD, 2006, s.12.

<sup>23</sup> OECD, 2006, s.5.

<sup>24</sup> OECD, 2006, s.12 - 13.

<sup>25</sup> OECD, 2006, s.5.

tarkistaa tietojen oikeellisuuden joko manuaalisesti ottamalla yhteyttä kortinantajaan tai automatisoidusti välittäjäosapuolen avulla.<sup>26</sup>

Suurimpia etuja käyttäjilleen luottokorttimaksamisessa ovat sen helppous sekä maksutavan laajalle levinnyt käyttäjä- ja kauppiaaverkosto.<sup>27</sup> Myös luottokorttitekniikan mahdollistama takaisinveloitusmahdollisuus<sup>28</sup> on useiden toimialan asiantuntijoiden mukaan yksi luottokorttien avainhyödyistä muihin maksujärjestelmiin verrattuna, joissa ei tällaista mahdollisuutta useinkaan ole.<sup>29</sup> Kaikkeen verkkomaksamiseen kortit eivät kuitenkaan välttämättä sovellu: maksutapahtumien yhteydessä palveluntarjoajien veloittamat provisiot kortin käytöstä ovat etenkin pienten maksujen näkökulmasta usein suhteellisen korkeita. Kortteja ei voida myöskään käyttää henkilöiden välisiin maksuihin, jonka lisäksi luottokortin myöntäminen edellyttää käyttäjiltä myös tiettyjen taloudellisten edellytysten täyttymistä.<sup>30</sup> Myös asiointiturvallisuuden saralla on parannettavaa: huolimatta parantuneista turvallisuus- sekä henkilön tunnistamiskäytännöistä kortin väärinkäyttö globaalissa verkkoympäristössä on ainakin vielä tällä hetkellä suhteellisen helppoa.

### 3.2.2 Pankkiyhteismaksut

Sähköisiin pankkiyhteismaksuihin kuuluvat mm. tilisiirtomaksut, suoraveloituskäytöt sekä uusimpana tulokkaana e-lasku. Sähköisten pankkiyhteismaksujen markkinat jakautuvat edelleen pääasiassa kansallisten rajojen mukaan:<sup>31</sup> etenkin Suomessa ja Pohjoismaissa pankkien verkkomaksujärjestelmät ovat perinteisesti olleet erittäin kehittyneet, ja niitä käytetään paljon osana sähköistä liiketoimintaa.<sup>32</sup> Muualla maailmassa, muutamaa poikkeusta<sup>33</sup> lukuun ottamatta pankkiyhteismaksujen käyttö ei ole ollut vastaavalla tasolla. Kuitenkin osana Eurooppalaisia integraatiotavoitteita nyt myös pankkiyhteismaksujen osalta on tähdätty rakenteellisiin ja

---

<sup>26</sup> Terämaa, 2001, s.302.

<sup>27</sup> OECD, 2006, s.16.

<sup>28</sup> Ts. "Chargeback option"

<sup>29</sup> OECD, 2006, s.19.

<sup>30</sup> OECD, 2006, s.16.

<sup>31</sup> KOM (2010)245, s.12.

<sup>32</sup> Suomessa oltiin solmittu vuonna 2009 yhteensä noin 4,9 miljoonaa verkkopankkisopimusta. Ruotsissa oli vuonna 2007 noin 7 miljoonaa ja Norjassa noin 4,4 miljoonaa henkilöasiakkaiden verkkopankkisopimusta. Euroopan keskuspankki ei ole kerännyt verkkopankkisopimuksiin ja verkkopankin käyttöön liittyvää tietoa, joten vertailutietoja muista maista on vaikea löytää. (Finanssialan keskusliitto, 2008, s.2) Tilastokeskuksen lokakuussa tekemän tutkimuksen mukaan viimeisten 3kk aikana suomalaisista 76% oli käyttänyt verkkopankkia. (Tilastokeskus, 2010)

<sup>33</sup> Esim. Portugali, Hollanti. (OECD, 2006, s.13)

lainsäädännöllisiin muutoksiin Euroalueella, jotka lisäävät niiden käyttöä maksuliikenteessä. Yhtenäistä eurooppalaista maksualuetta kehitettäessä pankkiyhteysmaksujen merkitys on olennainen. EPC:n SEPA- tilisiirtoja koskevan sopimuksen on allekirjoittanut tähän mennessä noin 4500 eurooppalaista pankkia, kuluttajille suunnattuja suoraveloitustapahtumia tulee marraskuun 2010 alussa vastaanottamaan 2600 pankkia ja yritysten välisiä suoraveloitustapahtumia vajaan 2400 pankkia.<sup>34</sup>

Etuina pankkiyhteyden kautta tapahtuvassa verkkomaksamisessa kaikkien osapuolten kannalta ovat erityisesti kustannustehokkuus ja verrattain korkea turvataso.<sup>35</sup> Maksutoimeksiannoissa raha siirtyy verkkopankin maksuissa reaaliaikaisesti tililtä toiselle, joka on ilmeisen toivottava ominaisuus kaikkien järjestelmän käyttäjien kannalta. Kuluttajien turvallisuuden kannalta tärkeä ominaisuus on myös se, etteivät kauppiat saa asiakkaan tilitietoja maksutapahtuman yhteydessä. Myös asiakkaan tunnistaminen on pankkiyhteysmaksuissa yleensä järjestetty varsin luotettavasti.

### 3.2.2.1 Tilisiirtomaksut

*Tilisiirto* määritellään uudessa maksupalvelulaissa ”maksajan maksutilin veloittamisena maksajan aloitteesta varojen siirtämiseksi maksunsaajan maksutilille.” Tilisiirron perustana on siis maksajan aloite, jolla maksaja antaa tiedot maksusta luottolaitokselle, joka suorittaa tilisiirron maksunsaajan tilille tai hänen luottolaitokselleen maksun vastaanottajan saataville. Maksaja vastaa lähtökohtaisesti siitä, että annetut tiedot ovat oikeita. Tilisiirto on näin ollen pohjimmiltaan talletusmuotoisen pankkisaamisen siirtämistä maksun saajalle. Useamman luottolaitoksen välillä tapahtuvassa siirrossa vaihtuu myös tallettusaamisen velallinen, pankki.<sup>36</sup>

Tilisiirrot soveltuvat erinomaisesti esimerkiksi yksityishenkilöiden tai yritysten välisiin rahansiirtoihin sekä laskujen maksamiseen. Suoraan sähköiseen kaupankäyntiin tilisiirrot eivät ole perinteisesti soveltuneet sellaisenaan sen tosiaikaisuusvaatimuksen takia. Kuitenkin nyttemmin on kehitetty sovelluksia, joissa maksun suorittaminen liittyy osana myyjän ja ostajan väliseen kauppaan: Myyjän ilmoitettua suoritettavan maksun määrän maksaja muodostaa yhteyden pankin maksujenvälityspalveluun, jossa tilisiirto suoritetaan tosiaikaisena kirjauksena. Tämän jälkeen

---

<sup>34</sup> Ripatti – Iivarinen, 2010, s.9.

<sup>35</sup> Liikenne- ja viestintäministeriö, 2007, s.20.

<sup>36</sup> Terämaa, 2001, s.263.

maksaja palaa myyjän palveluun. Myyjä saa tiedon maksajan suorituksesta tosiaikaisesti, jonka jälkeen hän voi vahvistaa tilauksen sekä maksun vastaanottamisen ostajalle.<sup>37</sup>

Verkkopankkien tilisiirtomaksut ovat olleet jo pitkään suosittuja Suomessa, etenkin niiden helppokäyttöisyyden takia. TNS Gallupin vuonna 2009 tekemän selvityksen mukaan suomalaiset maksavat mieluiten verkko-ostoksensa verkkopankin kautta: 60 % verkko-ostoksia tehneistä oli käyttänyt kyseistä maksutapaa. Kuitenkin useissa maissa tilisiirtomaksujen käyttö on marginaalista. Tämä johtuu ensisijaisesti järjestelmien integroinnin sekä yhteisten maksusäännösten puutteista.

### 3.2.2.2 Suoraveloituskasut

Suoraveloitus määritellään maksupalvelulaissa maksajan maksutilin veloittamisena *maksunsaajan* aloitteesta varojen siirtämiseksi maksunsaajan maksutilille, kun maksaja on antanut suostumuksensa maksutapahtumaan joko maksunsaajalle tai maksunsaajan palveluntarjoajalle taikka omalle palveluntarjoajalleen. Olennaista suoraveloitustyyppisen maksusuhteen osalta on siis maksajan suostumus hänen tilinsä veloittamiseen. Kuitenkin aloitteen yksittäisen maksu- tai veloitustapahtuman toteuttamisesta käynnistää maksunsaaja.<sup>38</sup> Veloituksen määrää ja veloitusaikaa koskevat ehdot määräytyvät perussuhteen perusteella, veloitustapaa koskevat ehdot taas perustuvat maksunvälittäjän tarjoaman palvelun ehtoihin.

Suoraveloitusta, kuten muitakin ns. velkoja-aloitteisia maksutapoja käytetään lähinnä asiakassuhteissa, joihin liittyy toistuvaluonteisia veloitustapahtumia samojen osapuolten välillä. Suoraveloitustekniikkoja käytetäänkin enimmäkseen yleishyödyllisen laitoksen (sähkölaitos, puhelinyhtiö jne.), vakuutusyhtiön tai luotonantajan veloittamiin toistuviin maksuihin.<sup>39</sup> Suoraveloituksen käyttö sähköisen kaupan yhteydessä on rajoitettua sen etukäteen edellyttämän valtuutuksen takia.<sup>40</sup>

---

<sup>37</sup> Terämaa, 2001, s.264.

<sup>38</sup> Terämaa, 2001, s.264.

<sup>39</sup> KOM (2003)718, liite 16.

<sup>40</sup> Terämaa, 2001, s.264-265.

Suoraveloitus on ollut käytössä yleisesti monissa maissa <sup>41</sup>, mutta on sen käyttö on rajoittunut useimmiten kansallisten rajojen sisäisiin siirtoihin. Tämä on johtunut osittain oikeudellisista eroista ja osittain teknisen yhteentoimivuuden puutteesta kansallisten suoraveloitujärjestelmien välillä. Yhtenäisen eurooppalaisen maksualueen myötä tilanne on kuitenkin nyt muuttunut: suomalainen suoraveloitussmalli tulee sellaisenaan poistumaan käytöstä <sup>42</sup> ja se korvataan yleiseurooppalaisella SEPA -suoraveloitussmaksulla. Tämä tulee vaikuttamaan huomattavasti ko. maksutyypin tekniseen toteutukseen: aikaisemmin suoraveloituksessa maksaja antoi suoraveloitussvaltuutuksen omalle pankilleen, SEPA- suoraveloituksessa taas maksaja antaa valtakirjan suoraan laskuttajalle. Riskit laskuttajan ja maksajan kannalta ovat näin erilaiset. <sup>43</sup>

Suomalaiset pankit ja laskuttajat ovat suhtautuneet varauksellisesti uuden suoraveloitustavan sopivuuteen kansallisen suoraveloituksen korvaavana maksutapana. Erilaisen toteutuksen lisäksi maksupalvelulakiin on velkoja-aloitteisten maksujen osalta tullut myös erityinen palautusoikeussäännös, mikä lisää edelleen maksutapaan liittyvää epävarmuutta. Pankit ovatkin suositelleet asiakkailleen vanhan kotimaisen suoraveloituksen korvaamista mieluummin e-laskun ja tilisiirron yhdistelmällä. SEPA -suoraveloituksen epäillään näin jäävän kapean laskuttajaryhmän palveluksi, koska suoraveloitus lisää yritysten työtä valtakirjojen hallinnoinnissa ja luo epävarmuutta saatavien saamisessa peruutusmahdollisuuden takia.

### 3.2.2.3 E-Lasku

E-lasku on Suomessa voimakkaasti kehittyvä palvelu, johon liittyy koko ajan entistä enemmän käyttäjiä. Myös Euroopan tasolla on vahva tahto e-laskutuksen edistämiseen. <sup>44</sup> Kaikkien laskujen kokonaismäärän on arvioitu Suomessa olevan noin 450 miljoonaa kappaletta vuodessa, joista yritysten välillä e-laskuja on viidennes ja kuluttajalaskutuksessa alle kymmenesosa. <sup>45</sup> On arvioitu,

---

<sup>41</sup> Suoraveloituksen käyttäminen EU-alueen maissa vaihtelee suuresti. Ruotsissa suoraveloituksen osuus maksuliikenteestä on samaa suuruusluokkaa kuin Suomessa. Saksassa suoraveloituksen suhteellinen osuus maksuliikenteestä on korkea, 42 %, ja Englannissa 21 %. Saksan suoraveloitusten korkeaa osuutta selittää osittain se, että osa korttimaksuista välitetään suoraveloituksina. Euroopassa on joitakin maita, joissa suoraveloituksella ei ole maksutapana käytännössä juuri mitään merkitystä, vaan sen suhteellinen osuus on alle 4 % (esimerkiksi Puola, Malta, Latvia). (Finanssialan Keskusliitto, 2008, s.7.)

<sup>42</sup> Finanssialan Keskusliitto, 2010<sup>a</sup>, s.14. Suomalaisen suoraveloituksen päättymisajankohdasta ei ole kuitenkaan tehty vielä päätöstä, ja palvelun käyttö tulee jatkumaan vuoden 2010 jälkeenkin.

<sup>43</sup> Finanssialan Keskusliitto 2010<sup>a</sup>, s.3

<sup>44</sup> Finanssialan Keskusliitto, 2010<sup>a</sup>, s.3.

<sup>45</sup> Lehto, 2010<sup>a</sup>, s.18.

että paperisten laskujen korvaaminen sähköisillä toisi suomalaisille yrityksille ja yhteiskunnalle jopa miljardien vuosittaiset säännöt. Pankit suosittelevat myös kansallisen suoraveloituksen korvaamista e-laskuun perustuvilla maksupalveluilla.<sup>46</sup> Ko. muutosprosessi on kuitenkin synnyttänyt myös vastarintaa kansalaisten ja median keskuudessa, joten jää nähtäväksi, millä aikataululla palvelu saadaan laajamittaiseen käyttöön.<sup>47</sup> Finanssialan keskusliiton huhtikuussa 2011 tekemän selvityksen mukaan noin 20 prosenttia kuluttajista on siirtynyt e-laskun käyttäjiksi.<sup>48</sup>

Teknisesti E-lasku on lainvoimainen sähköinen versio tai esitysmuoto paperilaskusta. Se sisältää saman informaation kuin paperinenkin versio ja toimii samalla tavalla, erotuksena että siihen liittyy käyttäjien kannalta vähemmän manuaalisia toimenpiteitä.<sup>49</sup>

E-laskun käyttö voi tuoda sekä laskuttajille että kuluttajille merkittäviä hyötyjä. Laskuttajalle syntyy kustannussäästöjä, maksajan kannalta suurimmat edut ovat nopeus ja vaivattomuus. Lisäksi maksaja voi valtuuttaa pankkinsa maksamaan laskuttajakohtaisesti tietyt maksut automaattisesti niiden eräpäivänä, jolloin palvelu muistuttaa vahvasti vanhaa suoraveloituspalvelua. Sähköinen laskujen maksaminen luo käyttäjilleen myös turvallisuuteen liittyviä etuja. Pankit tunnistavat tarkkaan e-laskun osapuolet: verkkolaskua on erittäin vaikea väärentää, eikä verkkopankkiin voi lähettää e-laskuja muu kuin sopimuksen tehnyt yritys. Laskuihin ei pääse käsiksi ilman pankkitunnuksia, joten myöskään muut tahot eivät pääse katsomaan tai hyväksymään toisten laskuja. Verkkopankkiin tulleita laskuja ei voi myöskään esim. varastaa esimerkiksi henkilötietojen väärinkäytöksiä varten.<sup>50</sup>

### 3.2.3 Uudet maksujenvälityspalvelut

Erityisesti internetissä ja matkapuhelinverkoissa harjoitettavan sähköisen kaupankäynnin lisääntyminen on luonut tarpeen kehittää vastaavasti myös ko. toimintaympäristöön soveltuvia maksutapoja.<sup>51</sup> Tällaisia ns. uusia maksujenvälityspalveluita on kehitetty erityisesti sentyyppisiä maksutapahtumia varten, joihin ns. vakiintuneet maksutavat, kuten käteismaksu, tilisiirto tai

---

<sup>46</sup> Finanssialan Keskusliitto, 2009, s.7.

<sup>47</sup> Lehto, 2010<sup>a</sup>, s.18.

<sup>48</sup> Finanssialan Keskusliitto, 2011, s.12.

<sup>49</sup> Turban et al., 2010, s.536.

<sup>50</sup> Finanssialan Keskusliiton ylläpitämä E-lasku – sivusto [www.e-lasku.info](http://www.e-lasku.info). Haettu 16.1.2011.

<sup>51</sup> Majuri, 2005, s.2.



korttimaksu eivät syystä tai toisesta sovellu tai soveltuvat heikosti esimerkiksi korkeiden transaktiokustannusten tai tiettyjen maksun suorittamiseen liittyvien vaatimusten takia. Vaihtoehtoisille maksujärjestelmille on nähty tilaus sekä potentiaalia vastata tiettyjen maksamisen erityisalueiden, kuten yksityishenkilöiden välisten maksumarkkinoiden tai mikromaksujen tarpeisiin.<sup>52</sup>

### 3.2.3.1 Mobiilimaksut

*Mobiilimaksaminen* on matkapuhelimen avulla suoritettavaa maksamista. Alun perin viestintävälineeksi kehitetystä matkapuhelimesta on tullut viime aikoina myös yhä tärkeämpi maksuväline.<sup>53</sup> Mobiileja maksujärjestelmiä on viimeisen kymmenen vuoden aikana kehitetty tuotteiden, palveluiden ja sisällön maksamiseen elektronisessa ja mobiilissa kaupankäynnissä sekä kassatoimipisteissä ja automaateilla. Sovellukset ovat kuitenkin olleet vielä varsin paikallisia, ja kokonaisuutena ajatellen mobiilipalvelut eivät kilpaile pankkien tai luottokorttiyhtiöiden maksunvälityksen kanssa.<sup>54</sup> Toisaalta, esimerkiksi Japanissa matkapuhelinta käytetään maksamiseen enemmän kuin tietokonetta ja myös joissain muissa maissa matkapuhelimella maksaminen on mahdollista monessa yhteydessä.<sup>55</sup> Suomessa matkapuhelimen käyttö vaihtoehtoisena maksuvälineenä on edennyt vahvimmin mm. matkalippujen ostossa ja pysäköinnissä. Koko Euroopan tasolla mobiilimaksujen volyymi on keskimäärin vielä todella pieni.<sup>56</sup>

Karnouskos määrittelee mobiilimaksun ”*miksi tahansa maksuksi, jossa matkaviestinvälinettä käytetään maksun aloittamiseksi, aktivoimiseksi ja/tai vahvistamiseksi*”.<sup>57</sup> Teknisesti matkapuhelinta voidaan käyttää varsin monipuolisesti maksamisessa niin internetin-, matkapuhelinverkon kuin lähitunnistamisteknologiankin avulla. Mobiilimaksamisen sovelluksia ovat olleet esimerkiksi puhelinlaskulla laskutus, prepaid-ratkaisut, mobiilikukkarosovellukset sekä perinteisten maksuvälineiden, kuten luottokortin ja pankkiyhteyden käyttö matkapuhelimen avulla. Suuri osa käytetyistä ratkaisuista on ollut ns. etämaksusovelluksia, eli ne tukeutuvat

---

<sup>52</sup> OECD, 2006, s.5.

<sup>53</sup> Kuluttajavirasto, 2010, s.6.

<sup>54</sup> Gauriloff, 2009, s.15.

<sup>55</sup> OECD, 2006, s.12.

<sup>56</sup> Leinonen, 2008, s.98.

<sup>57</sup> Karnouskos, 2004, s.44 - 66.

tietoliikenneverkkoihin ostajan ja myyjän välisessä transaktiotiedon siirrossa. Tulevaisuudessa nykyistä vahvemmin tulee mitä todennäköisimmin yleistymään kuitenkin myös mobiili lähimaksaminen, jossa maksutapahtuma välitetään suoraan ostajan matkapuhelimen myyjän maksutai kassapäätteeseen ilman yleistä tietoliikenneverkkoa jonkun lähimaksuteknologian, kuten NFC-tekniikan<sup>58</sup> avulla. Tämänäköisistä sovelluksista on saatu jo varsin lupaavia kokemuksia. Lisäksi matkapuhelinta on myös pidetty potentiaalisena apuvälineenä muiden sähköisten maksuvälineiden varmennusongelmiin ns. kahden kanavan tunnistussysteemin mahdollistajana.

Mobiilimaksamisen potentiaalista ja lukuisista markkinoille tuoduista ratkaisuista huolimatta mitään laajempaa tai yhtenäistä mobiilimaksamiskulttuuria ei ole vielä tähän mennessä kuitenkaan syntynyt, vaan useimmat sovellukset ovat olleet paikallisia. Käyttöä ovat rajoittaneet erityisesti operaattoreiden perimä suhteellisen korkea hinta ja sitä kautta soveltumattomuus suurempiin maksuihin. Myös matkapuhelinoperaattorien rinnastaminen muihin maksupalveluntarjoajiin ja sitä kautta suhteellisen raskaat pääomavaatimukset maksupalvelujen tarjoamiselle ovat hidastaneet ratkaisujen käyttöönottoa. Suurempien maksujen hoitaminen edellyttää lisäksi operaattorilta luottolaitoksen toimilupaa, ja sitä kautta samoja edellytyksiä kuin pankeilta. Myös kuluttajien tottumattomuudella matkapuhelinten käyttöön sähköisenä maksuvälineenä on varmasti ollut oma vaikutuksensa.<sup>59</sup>

Ominaisuuksiltaan matkapuhelin soveltuu kuitenkin varsin hyvin maksamiseen. Suurimpia hyötyjä mm. Leinosen mukaan ovat välineen kannettavuus, sen riittävät näppäimistö- ja näyttöominaisuudet sekä käyttö- ja tallennuskapasiteetti maksutapahtumien toteutusta ajatellen, sirukorttipaikan olemassaolo asiakkaiden tunnistamista ja maksutapahtumien salausta ajatellen sekä em. lähi- ja etäkäyttömahdollisuudet.<sup>60</sup> Tämän lisäksi sillä on myös suosittuna matkaviestinvälineenä valmiiksi kansainvälisesti laaja käyttäjäverkosto: maailmanlaajuisesti yli puolella maailman väestöstä on matkapuhelin ja Euroopan tasolla mitattuna matkapuhelimia on jopa enemmän kuin ihmisiä.<sup>61</sup> Tilastokeskuksen mukaan myös 99 prosentilla suomalaisista kotitalouksista on ainakin yksi matkapuhelin käytössään, yleensä useampia.<sup>62</sup> Suurimmat haasteet teknisellä puolella ovat

---

<sup>58</sup> NFC, Near Field Communication. Ks. lisää esim. [www.nfc-forum.org](http://www.nfc-forum.org)

<sup>59</sup> OECD, 2006, s.22.

<sup>60</sup> Leinonen, 2008, s.181.

<sup>61</sup> Leinonen, 2008, s.181.

<sup>62</sup> Tilastokeskus, 2011. [http://tilastokeskus.fi/til/kbar/2011/03/kbar\\_2011\\_03\\_2011-03-28\\_kuv\\_016\\_fi.html](http://tilastokeskus.fi/til/kbar/2011/03/kbar_2011_03_2011-03-28_kuv_016_fi.html) Haettu 31.3.2011.

tarpeeksi helppojen käyttösovellusten sekä riittävän luotettavan tunnistamismenetelmän liittäminen mobiilimaksutapahtumiin.<sup>63</sup>

### 3.2.3.2 Välityspalvelut (mediating services)

Välityspalvelujärjestelmät käyttävät hyödykseen perinteisiä maksutapoja, kuten luottokortti- ja pankkiyhteysmaksuja, kuitenkin lisäämällä niihin uuden tason. Esimerkki ko. palveluista on PayPal, jolla on maailmanlaajuisesti jopa yli 94 miljoonaa aktiivista käyttäjää.<sup>64</sup> Maksaakseen ko. palvelussa käyttäjien tarvitsee vain tietää toistensa sähköpostiosoitteet, jotka ovat varmistettuja ja yhdistettyinä käyttäjien henkilökohtaisiin maksutileihin. Maksun määrä veloitetaan ko. tililtä, eikä muuta taloudellista informaatiota lähetetä maksun vastaanottajalle.

Voidakseen käyttää ko. järjestelmiä, käyttäjien on välttämätöntä rekisteröityä tarjoamalla luottokortti- tai pankkitilitietonsa maksujen lähteeksi. Ne hyödyntävät jo olemassa olevia maksuverkostoja, joten palveluiden käyttöönotto on varsin vaivatonta. Välityspalvelut soveltuvat kuitenkin pikemminkin tiettyihin markkinarakoihin kuin tarjoavat yleisen maksuvaihtoehdon. Ne tarjoavat esimerkiksi vartenotettavan vaihtoehdon sellaisille tahoille, jotka haluavat käydä kauppaa verkossa rekisteröitymättä kauppiaksi: esimerkiksi yksityishenkilöiden välisiin rahansiirtoihin kansainvälisissä verkkohuutokaupoissa tai pienten myyjien verkkokauppoihin. Kustannuksiltaan ne eivät välttämättä kuitenkaan sovellu esimerkiksi mikromaksuihin. Myöskään turvallisuustasoltaan niitä ei voi suunnitella raskaammiksi kuin järjestelmät joihin ne perustuvat, joka rajoittaa maksutavan itsenäistä kehitystä.<sup>65</sup>

### 3.2.3.3 Sähköinen raha

Sähköinen raha on ensisijaisesti mikromaksamisen tarpeiden pohjalta kehittynyt maksuväline. Se on etukäteen sen liikkeeseenlaskijalta ostettavaa haltijaluontoista sähköistä raha-arvoa, jota voidaan käyttää maksamiseen erilaisissa elektronisissa maksuympäristöissä, kuten myyntipisteissä tai verkossa mobiili- tai internetyhteyden avulla. Sähköisen rahan järjestelmien on suunniteltu tuovan

---

<sup>63</sup> Leinonen, 2008, s.65 ja 181.

<sup>64</sup> Ks. PayPalin internetsivut: *PayPal: Q4 2010 FastFacts*. [https://www.paypal-media.com/assets/pdf/fact\\_sheet/PP\\_FastFacts\\_Q410\\_0111.pdf](https://www.paypal-media.com/assets/pdf/fact_sheet/PP_FastFacts_Q410_0111.pdf) Haettu 31.3.2011.

<sup>65</sup> OECD, 2006, s.20 - 21.

elektronisen vaihtoehdon käteisen rahan käytölle.<sup>66</sup> Verrattuna käteisen rahan käyttöön sähköisen rahan liikkeessä olevat määrät ovat olleet kuitenkin vielä pieniä.<sup>67</sup> Vaikka sähköisen rahan on odotettu teknologian ja tietoyhteiskunnan kehittymisen myötä vähitellen kasvattavan suosiotaan, järjestelmät eivät ole ainakaan vielä saaneet odotetun vahvaa asemaa sähköisessä kaupankäynnissä: Vuoden 2007 lopussa sähköisen rahan liikkeeseenlaskijoita oli globaalilla tasolla ainoastaan 20, jonka lisäksi 127 yritykselle oli myönnetty poikkeuslupa liikkeeseenlaskuun.<sup>68</sup>

Sähköisen rahan sovellukset voivat lähtökohtaisesti olla varsin erilaisia keskenään. Näin ollen juridisen määritelmän<sup>69</sup> vaikutus rajanvetoon sille mitä pidetään sähköisenä rahana, on olennainen.<sup>70</sup> Yleensä sähköinen raha on tallennettu joko sähköiselle laitteelle, kuten esim. mikrosirullisen toimikortin muistiin (korttiraha) tai joko etäpalvelimelle tai tietokoneen muistiin sähköiseen kukkaraan (verkkoraha).<sup>71</sup> Verkkorahaa voi käyttää täysin virtuaalisesti, korttiraha vaatii yleensä erillisen lukulaitteen, joka tosin on mahdollista liittää käytettävään päätelaitteeseen, kuten esim. tietokoneeseen tai matkapuhelimeen. Nytemmin on kuitenkin kehitetty myös täysin kontaktittomia maksutekniikoita ko. maksuja silmällä pitäen.

Sähköisellä rahalla on joitakin muista sähköisistä maksuvälineistä eroavia ominaisuuksia. Ensinnäkin, on syytä huomioida että sähköinen raha ei ole laillinen maksuväline<sup>72</sup>, vaan raha-arvoa, jota kansallisten järjestelmien ylläpitäjät vaihtavat oman maansa valuuttaan yleensä 1:1 suhteessa. Toiseksi, kuten setelit ja kolikot, myös sähköinen raha on usein anonyymiä. Sähköistä rahaa ei myöskään lähtökohtaisesti tallenneta yksilöidyille tileille, vaan se on luonteeltaan haltijarahaa,

---

<sup>66</sup> Jo vuonna 1999 julkaistun VM:n sähköisen käteisen sääntelytyöryhmä II: muistion näkemyksen mukaan sähköisestä rahasta piti kehittyä todennäköisesti ”pitkällä aikavälillä merkittävä maksuväline”. Ks. Valtionvarainministeriön Työryhmämuistioita 4/99: Sähköisen käteisen sääntelytyöryhmä II:n muistio, s.27.

<sup>67</sup> EU:ssa liikkeessä olevan sähköisen rahan määrä on nykyään noin miljardi euroa, kun käteistä on liikkeellä yli 637 miljardia euroa. (Euroopan talous -ja sosiaalikomitea, 2009, s.6.)

<sup>68</sup> KOM (2008)627, s.2.

<sup>69</sup> Sähköinen raha määritellään uudessa sähkörahadirektiivissä (2009/110/EY) seuraavasti: ”Sähköisellä rahalla tarkoitetaan sähköisesti tai magneettisesti tallennettua rahallista arvoa, joka ilmenee liikkeeseenlaskijaan kohdistuvana saatavana, joka on laskettu liikkeeseen vastaanotettuja varoja vastaan direktiivin 2007/64/EY 4. Artiklan 5.kohdassa määriteltyjä maksutapahtumia varten ja jonka muu luonnollinen henkilö tai oikeushenkilö kuin sähköisen rahan liikkeeseenlaskija itse ottaa vastaan. (Yleisellä tasolla määriteltynä) Sähköisellä rahalla tarkoitetaan siis sähköistä raha-arvoa, jota voidaan käyttää elektronisessa maksuympäristössä myös muiden kuin sen liikkeeseenlaskijan palveluissa.

<sup>70</sup> Majuri, 2005, s.119 - 120.

<sup>71</sup> Euroopan komission internetsivut, [http://ec.europa.eu/internal\\_market/payments/emoney/index\\_en.htm](http://ec.europa.eu/internal_market/payments/emoney/index_en.htm) Haettu 5.2.2011

<sup>72</sup> Laillisia maksuvälineitä ovat rahalain mukaisella tavalla liikkeelle lasketut *setelit ja kolikot*.

toisin kuin talletustileillä olevat varat. Hallituksen esityksen mukaan sähköisenä rahana ei pidetä sellaista maksuvälinettä, joka on liitetty talletuspankissa olevaan talletussuojan alaiseen tiliin. Siten esimerkiksi sellainen maksukortti, jonka avulla kauppialle voi pankin ja asiakkaan kanssa tekemänsä sopimuksen nojalla suoraan veloittaa asiakkaan pankkitiliä maksuksi asiakkaan ostoista, ei ole laissa tarkoitettua sähköistä rahaa.<sup>73</sup> Oikeusteknisesti sähköinen raha on siis eräänlainen laillisten maksuvälineiden ja tilirahan välimuoto.<sup>74</sup> Lisäksi sähköiselle rahalle ei lähtökohtaisesti makseta korkoa, vaan mahdollinen korkohyöty tulee täysimääräisesti liikkeeseenlaskijan hyväksi. Sähköisen rahan aitouden varmistamiseen käytetään yleensä sähköistä salakirjoitusta fyysisten aitoustekijöiden sijasta.

Sähköisen rahan tarjoajien markkinat eivät koskaan ole olleet erityisen integroituneet vaan sähkörahamarkkinoilla on esiintynyt useita toisistaan riippumattomia järjestelmiä, jotka ovat toimineet pääasiassa kansallisella tasolla. Uusien maksutottumusten hitaan yhteiskunnallisen omaksumisen lisäksi tähän ovat olleet syinä pieni käyttäjäkunta niin kauppioiden kuin kuluttajienkin keskuudessa, sähköisen rahan liikkeeseenlaskijoiden menetelmien eroavaisuudet, korkeat kustannukset ja ennen kaikkea se, että sähköisen rahan järjestelmillä ei ole usein myöskään ollut liittymiä muihin maksujenvälitysjärjestelmiin. Lisäksi useiden kannanottojen mukaan iso osuus tähän odotettua hitaampaan kehitykseen on ollut myös vanhan sähkörahamarkkinan asettamalla vaatimuksilla, jotka ovat merkittävästi rajoittaneet innovointia ja toimijoiden markkinoille pääsyä. Viime aikoina lainsäädännön kehittyessä sähköisen rahan järjestelmät ovat nousseet uudestaan esille keskusteluissa, sillä sähköisellä rahalla voidaan nähdä sen aiemmista epäonnistumisista huolimatta varsin huomattavaa käyttöpotentiaalia, esimerkiksi tiettyjen yhteiskuntaryhmien, joilla ei ole mahdollisuuksia täyttää luottokelpoisuuden vaatimuksia, sähköiseen talouteen osallistumisen mahdollistajana.<sup>75</sup> Sekä RFID- teknologian että internetin avulla toimivista sovelluksista on saatu maailmalla muutenkin hyviä kokemuksia.<sup>76 77</sup> Pitää

---

<sup>73</sup> HE 33/2002vp, s.50.

<sup>74</sup> Terämaa, 2001, s.259.

<sup>75</sup> Euroopan talous- ja sosiaalikomitea, 2009, s.1,11. Esimerkkeinä em. ryhmistä mm. maahanmuuttajat, pankkipalveluverkoston ulkopuolella olevat tai sitä vain vähän käyttävät, sekä eräissä tapauksissa myös nuoret ja vammaiset.

<sup>76</sup> RFID -pohjaisia sovelluksia on hyödynnetty mm. erilaisissa kontaktittomissa älykorteissa. Onnistuneena esimerkkinä tästä on Hongkongissa jo vuonna 97 käyttöön otettu Octopus -kortti. Sitä voi käyttää paikallisesti lähes kaikkien julkisen liikenteen matkojen maksamiseen, jonka lisäksi se toimii maksuvälineenä elintarvikemyymälöissä, supermarketissa, pikaruokaravintoloissa, pysäköintimittareissa, myyntiautomaateissa jne. 95 prosenttia Hongkongin 16 - 65 vuotiaista käyttää ko. korttia maksamisessa. Myös Euroopassa on otettu käyttöön joitain vastaavia, vielä varsin paikallisia ja käyttökohteiltaan varsin rajallisia sovelluksia. Talous- ja sosiaalikomitean lausunnon mukaan on kuitenkin todennäköistä, että RFID -korttien käyttökohteet tulevat lisääntymään ja monipuolistumaan kun ko. kortit otetaan laajalti käyttöön. (Euroopan talous- ja sosiaalikomitea, 2009, s.5.)

kuitenkin muistaa, että niin kauan kun kuluttajat eivät pidä ko. järjestelmistä saatavia etuja riittävän suurina muihin vaihtoehtoisiiin järjestelmiin verrattuna, he eivät muuta maksutottumuksiaan.<sup>78</sup>

---

<sup>77</sup> Myös internetissä voidaan hyötyä sähköisen rahan käytöstä. Ensinnäkin, sähköinen raha mahdollistaa myös pankkipalveluverkoston ulkopuolisille asiakkaille erilaisten maksullisten internetsovellusten käytön. Toiseksi, erilaiset E-Bayn kaltaiset verkkohuutokauppapalvelut ovat lisänneet merkittävästi kuluttajien välisiä rahasiirtoja internetissä. Useissa järjestelmissä kansainväliset pankkien väliset rahansiirrot eivät ole mahdollisia tai niistä aiheutuu huomattavia kustannuksia käyttäjille. Sähköinen raha antaa riittävän luotettavan ja kustannustehokkaan maksamisen vaihtoehdon näissä tapauksissa. Kolmanneksi, on keskusteltu siitä, että usein pienten, muutamien senttien suuruisten verkko-ostosten maksaminen esimerkiksi luottokortin tai pankkitunnisteiden avulla nähdään liian raskaana. Tässä onkin tilaus erilaisille vaivattomammille sähkörahamuotoisille sovelluksille, jossa erillistä tunnistautumista ei tarvitsisi joka kerta suorittaa. (Euroopan talous- ja sosiaalikomitea, 2009, s.5-6.)

<sup>78</sup> OECD, 2006, s.24.

## 4. SÄHKÖISEN MAKSAMISEN SÄÄNTELY: PÄÄPIIRTEET JA KEHITYS

Sähköisen kaupan toteuttamisen kannalta eräs keskeisimmistä kysymyksistä on, miten kauppaan liittyvä rahavelvoite, maksu, voidaan suorittaa kaupan osapuolten kannalta oikein ja turvallisesti.<sup>79</sup> Varsinkin viime aikoina maksamisen vaihtoehtojen monipuolistuessa myös oikeudellisen sääntelyn tarve maksumarkkinoilla on lisääntynyt. Lukuisat kansainväliset, kansalliset ja alueelliset säännökset ohjaavat kaikkia maksutapoja.<sup>80</sup> Toimintaympäristöstä johtuvien erityispiirteiden takia kuitenkin myös toimijoiden välisen itsesääntelyn sekä erilaisten maksuyhteisöjen laatimien standardien merkitys yhtenäisen lainsäädännön ohella on olennainen. Lisääntyneestä sääntelystä huolimatta myös sopimuksilla sekä velvoiteoikeuden yleisillä suoritusta koskevilla periaatteilla on merkitystä maksuun liittyvien oikeudellisten kysymysten arvioinnissa.<sup>81</sup>

### 4.1 Sähköinen toimintaympäristö ja sen vaikutukset sääntelyyn

Sähköinen toimintaympäristö luo merkittäviä haasteita maksamiseen liittyvän sääntelyn ja lainsäätäjien kannalta. Ensinnäkin, suurin osa lainsäädännöstä on perinteisesti kansallista tai sidottu maantieteellisiin alueisiin. Sen sijaan sähköisellä toimintaympäristöllä on rajat ylittävä, kansainvälinen luonne.<sup>82</sup> Tämä tekee yhtenäisen sääntelykehikon muodostamisesta sähköiseen toimintaympäristöön varsin haasteellista, etenkin alueelliset eroavaisuudet huomioon ottaen. Voimassa oleva lainsäädäntö on lisäksi alun perin suunniteltu fyysisen toimintaympäristön vaatimuksia silmällä pitäen, joten toimintaympäristö luo myös haasteita siltä osin, kun ko. aiemmin tuotettua lainsäädäntöä tulisi soveltaa tasapuolisesti elektronisessa ympäristössä.

Toiseksi, lakien kehittäminen, valmistelu ja täytäntöönpano on kokonaisuutena useimmiten hidas ja jäykkä prosessi.<sup>83</sup> Vastaavasti, teknologia ja sähköisen maksamisen toimintaympäristö kehittyvät nopeasti: palvelut ovat lähentyneet teknisesti toisiaan ja ovat saavutettavissa useilla vaihtoehtoisilla laitteilla.<sup>84</sup> Jopa uusien lakien kohdalla on näin ollen riski, että ne vanhentuvat muutaman vuoden sisällä nopean teknologisen kehityksen takia.<sup>85</sup> Lainsäätäjien haasteena onkin täten muodostaa

---

<sup>79</sup> Terämaa, 2001, s.248.

<sup>80</sup> Efrain et al., 2010, s.525.

<sup>81</sup> Terämaa, 2001, s.251.

<sup>82</sup> Schaub, 2004, s.16.

<sup>83</sup> Schaub, 2004, s.16.

<sup>84</sup> KOM (2010)245, s.4.

<sup>85</sup> Schaub, 2004, s.16.

teknologianeutraalia lainsäädäntöä, joka olisi sovellettavissa käytetystä teknologiasta tai käytetystä maksupäätteestä riippumatta. Monesti tämäntyyppisen ratkaisun tavoittelu kuitenkin johtaa liian avoimeen, epätäsmälliseen ja tulkinnanvaraiseen sääntelyyn, joka ei tarjoa riittävää lain suojaa kaikille toimintaympäristön osapuolille.<sup>86</sup> Vastaavasti jos sääntely muodostetaan liian jäykäksi, se voi rajoittaa innovaatioita sekä tiettyjen maksupalveluiden kehittämistä joka puolestaan hidastaa tarpeettomasti maksuympäristön muuttumista kulloinkin vallitsevan teknologian mukana ja samalla myös rajoittaa yhteiskunnallista kehitystä. Alueen lainsäädännöllä onkin varsin haastava, useiden tavoitteiden välillä tasapainotteleva tehtävä toimintaympäristössään: sen pitäisi olla samalla riittävän tiukkaa ja yksityiskohtaista toimijoiden turvallisuuden ja oikeuksien varmistamiseksi sekä epäselvyyksien välttämiseksi, mutta toisaalta myös riittävän teknologiariippumatonta ja joustavaa maksualan kehityksen edesauttamiseksi.

## **4.2 Maksuympäristön sääntely**

Sähköisen maksamisen sääntelykehikko on rakentunut vähitellen ja se on varsin monitahoinen. Aiemmin sääntely eri maksuvälineiden välillä oli varsin hajanaista. Viime aikoina, sähköisen kaupankäynnin lisääntymisen sekä Euroopan Unionin integraatiotavoitteiden myötä ylikansallisen lainsäädännön määrä on kuitenkin lisääntynyt ja sääntely näin ollen kokonaisuutena jonkin verran yhtenäistynyt. Euroopan maksuneuvosto (EPC) on laatinut yhtenäisen sääntelykehikon euroalueen sisällä tapahtumia maksutapahtumia varten, mukaan lukien sähköiset maksut. Kuitenkin, vaikka mm. sähköisestä kaupankäynnistä, sähköisestä laskutuksesta ja sähköisistä allekirjoituksista on annettu keskeistä yhteismarkkinalainsäädäntöä, kauppatapahtumat ovat edelleen liian monimutkaisia digitaalisessa ympäristössä, ja ko. sääntöjä sovelletaan eri tavoin eri jäsenvaltioissa. Komissio katsookin tiedonannossaan, että kuluttajien ja yritysten keskuudessa on vielä huomattavaa epävarmuutta kunkin tahon oikeuksista ja oikeudellisesta suojasta verkkokaupankäynnissä.<sup>87</sup>

### **4.2.1 Maksutapahtumaan liittyvä sääntely**

Sähköisen maksamisen asteittaisen kehittymisen sekä sähköisen maksukentän pirstaleisuuden takia sähköiseen maksamiseen ja erityisesti itse maksutapahtumaan liittyvä sääntely on perinteisesti ollut varsin hajanaista. Keskeisin kotimaisista säädöksistä oli aina vuoteen 2010 asti tilisiirtolaki

---

<sup>86</sup> Schaub, 2004, s.16.

<sup>87</sup> KOM (2010)245, s.8.



(821/1999), jossa säädettiin luottolaitosten tai muiden maksujenvälittäjien velvollisuudesta antaa tietoja tilisiirrosta sekä ko. tahojen vähimmäisvelvoitteista tilisiirron toteuttamisessa. Lisäksi tilisiirtolaki sisälsi säännökset tilisiirtomaksun sitovuudesta sivullisiin nähden, maksumääräyksen peruuttamisesta sekä maksumääräyksen antajan vapautumisesta suoritusvelvoitteestaan saajaan nähden. Tilisiirtolain lisäksi sähköiseen maksamiseen liittyviä säännöksiä sisältyi mm. kuluttajansuojalakiin (38/1978), jossa määrättiin a) tilinhaltijan vastuusta tapauksissa joissa luottokorttia tai tililuoton käyttöön oikeuttavaa muuta tunnistetta oli käytetty oikeudettomasti ja b) luotonantajan vastuusta myyjän sopimusrikkomusten osalta, sekä viestintämarkkina-laissa (393/2003), jonka 79a§ soveltui matkapuhelimella suoritettuun oikeudettomaan maksutapahtumaan.<sup>88</sup> Suoraveloituskäytön osalta ei ollut erillistä lainsäädäntöä, vaan niiden käyttö perustui lähinnä palvelusta tehtyihin sopimuksiin ja valtuutusta koskeviin oppeihin.<sup>89</sup> Myöskään sähköisen rahan osalta ei maksun suorittamiseen liittyviä säännöksiä juurikaan ollut.<sup>90</sup>

Maksuympäristössä tapahtuneen teknisen kehityksen seurauksena maksaminen on muuttunut yhä monimuotoisemmaksi. Maksutapojen ja -tottumusten sekä toimintaympäristön muuttuessa sähköisen maksamisen sääntelyä erityisesti juuri maksutapahtumien toteuttamiseen liittyen on ollut välttämätöntä tarkistaa ja yhtenäistää. Näin tapahtuikin, kun Euroopan komissio antoi 13. marraskuuta 2007 maksupalveludirektiivin, joka implementoitiin kotimaan lainsäädäntöön maksupalvelulaille huhtikuussa 2010. Maksupalvelulaki kumosi tilisiirtolain, ja toi kaikki sähköiset maksutapahtumat yhtenäisen sääntelyn piiriin. Maksupalveludirektiivin vaatimat reunaehdot on implementoitu myös muihin kotimaisiin maksusäännöksiä sisältäviin lakeihin.

Lain soveltamisalamääritelmän mukaan sillä säännellään maksupalveluja koskevista tiedonantovelvollisuuksista, sopimusehdoista sekä maksupalvelujen toteuttamisesta. Se sisältää määräyksiä mm. palveluntarjoajien tiedonantovelvollisuuksista, puitesopimusten solmimisesta, maksutapahtumien toteuttamisesta, maksujen sivullissitovuudesta sekä erinäisistä maksupalvelun käyttäjien ja palveluntarjoajien velvollisuuksista ja oikeuksista maksuvälineiden käyttöön liittyen. Maksupalvelulain säännökset ovat pääosin pakottavia. Maksupalveludirektiivi ja maksupalvelulaki yhtenäistävät maksutapahtumiin liittyvää sääntelyä kaikkien maksuvälineiden osalta, sekä selventävät vallitsevaa oikeudentilaa.

---

<sup>88</sup> HE 169/2009, s.11,12.

<sup>89</sup> Terämaa, 2001, s.264-265.

<sup>90</sup> Terämaa, 2001, s.269.

Maksutapahtumaan liittyen oikeudellista sääntelyä täydennetään erilaisilla yleisluontoisilla ehdoilla ja standardeilla.<sup>91</sup> Lisäksi joissain tapauksissa, kuten virheellisten tilisiirtomaksujen palautusvelvollisuuden osalta, joudutaan turvautumaan myös osittain yleisiin velvoiteoikeudellisiin periaatteisiin.

#### 4.2.2 Maksupalveluiden tarjoamiseen liittyvä sääntely

Toisen kokonaisuuden maksamisen sääntelyssä muodostaa maksulaitosten toimintaedellytyksiin ja maksuvälineiden liikkeeseenlaskuun liittyvä sääntely. Luottolaitosdirektiivin (2006/48/EY) pohjalta säädettyssä laissa luottolaitostoiminnasta (121/2007) säädetään oikeudesta harjoittaa luottolaitostoimintaa sekä tällaiselle toiminnalle asetettavista vaatimuksista ja niiden noudattamisen valvonnasta. Lisäksi laissa säädetään oikeudesta harjoittaa muuta liiketoimintaa, jossa yleisöltä hankitaan takaisinmaksettavia varoja. Uudessa maksupalveludirektiivin pohjalta säädettyssä maksulaitoslaissa (297/2010) taas säädetään oikeudesta tarjota maksupalvelua. Sen mukaan maksupalvelua saa pääsääntöisesti tarjota vain toimiluvan saanut maksulaitos. Laissa säädettyjen vaatimusten täytyessä Finanssivalvonta voi kuitenkin päättää, että suomalainen luonnollinen henkilö tai oikeushenkilö saa tarjota maksupalvelua myös ilman toimilupaa. Tämän lisäksi keskeisiä lakeja alueella ovat myös laki finanssivalvonnasta (878/2008), joka sisältää säännöksiä finanssivalvonnan toiminnasta ja sen valvontavaltuuksista, sekä laki rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä (503/2008), joka sisältää säännöksiä rahoitusjärjestelmien käytön estämisestä ko. tarkoituksiin.

Toimintaedellytyksiin ja liikkeeseenlaskuun liittyvä sääntely on herättänyt keskustelua erityisesti uusien maksujenvälityspalveluiden, kuten mobiilimaksupalveluiden sekä sähköisen rahan osalta. Lakien tiukkoja säännöksiä on osittain pidetty syynä sille, etteivät ko. maksutavat ole kehittyneet odotetunlaisesti, siitä huolimatta että niiden lähtökohta olisikin ollut juuri päinvastainen.

Esimerkiksi mobiilimaksualan liikkeeseenlaskijoita on säännelty luottolaitoslailla, joka vaatii yleisövarojen vastaanottajalta eli prepaid- ratkaisun tarjoajalta vähintään maksuliikkeyhteisön toimiluvan, jonka ehtona maksuliikkeyritykseltä vaaditaan vähintään miljoonan euron vähimmäispääomaa. Operaattorista riippumattomien palvelujen laskuttaminen operaattorin

---

<sup>91</sup> Esimerkiksi pankkiyhteysmaksujen osalta lainsäädäntöä täydentävät Finanssialan keskusliiton laatimat Euromaksualueella välitettävien euromaksujen yleiset ehdot. Nämä pankkien yleiset sopimusehdot noudattavat suurelta osin maksupalvelulain pääpiirteitä.

puhelinlaskulla vaatii taas luottoyhteisön toimiluvan, jolta vaadittava vähimmäispääoma on viisi miljoonaa euroa. Nämä vähimmäisvaatimukset ovat esim. liikenne- ja viestintäministeriön kannanoton<sup>92</sup> mukaan melko suuria, jotta ne palvelisivat mobiilimaksualan vapaata kehitystä.

Myös sähköisen rahan liikkeeseenlaskijoita on säädelty luottolaitoslilla siihen erikseen implementoidun sähkörahadirektiivin (2000/46/EY) pohjalta. Direktiivin tarkoituksena oli ensisijaisesti helpottaa muiden kuin luottolaitosten pääsyä sähköisen rahan markkinoille. Sillä pyrittiin luomaan sääntelyjärjestelmä, joka olisi sekä huomioon otanut sähköisen rahan uusien liikkeeseenlaskijoiden toimintaan liittyvät riskit että toisaalta myös mahdollistanut teknologiset innovaatiot sähköisen maksamisen alueella<sup>93</sup> ja helpottanut pienempien palveluntarjoajien markkinoille pääsyä. Kuitenkin direktiivin täytäntöönpanon arvioinnissa paljastui, että osa ko. direktiivin säännöksistä päinvastoin on näyttänyt haitanneen sähköisen rahan markkinoiden kasvua.

Ko. sääntelyn aiheuttamaa epätasapainoa on onneksi osittain pyritty viime aikoina kuitenkin korjaamaan. Esimerkiksi sähköisen rahan käyttöä pyritään lisäämään uuden sähkörahadirektiivin (2009/110/EY) avulla, joka selkeyttää vallitsevaa oikeudentilaa ja keventää liikkeeseenlaskijoilta edellytettäviä vaatimuksia. Myös mobiilimaksaminen kehittyisi parhaiten avoimemman sääntelyn ja vapaan kilpailuympäristön turvin. Keskuskauppakamarin mukaan lainsäädännöllä ei pitäisi asettaa myöskään mobiilimaksuja koskevien palvelujen tarjoajille vaatimuksia, jotka käytännössä estävät palvelujen tarjoamisen jatkamisen ja kehittämisen.<sup>94</sup> Käsittelen lainsäädännön aiheuttamia ongelmia uusille maksuvälineille tarkemmin vielä myöhemmin teoksessa.

#### **4.2.3 Maksamisen turvallisuuteen liittyvä sääntely**

Maksamisen turvallisuuteen liittyvä sääntely jakautuu useiden lakien kesken, joita täydennetään lisäksi useilla toimialakohtaisilla standardeilla. Sähköisen maksamisen näkökulmasta on syytä tarkastella erityisesti asiakkaiden tunnistamiseen ja tietoturvaan liittyvää sääntelyä.

Henkilön tunnistamisvelvollisuuksista sähköisessä ympäristössä säädetään nykyään ensisijaisesti laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009). Laki on

---

<sup>92</sup> Liikenne- ja viestintäministeriö, 2003<sup>a</sup>, s.26.

<sup>93</sup> Euroopan talous- ja sosiaalikomitea, 2009, s.2.

<sup>94</sup> Keskuskauppakamari, 2006. <http://www.keskuskauppakamari.fi/Eduunvalvonta/Lausunnot/Maksupalveluita-koskeva-direktiiviehdotus> Haettu 19.1.2011

sinänsä poikkeuksellinen, että vahvaa sähköistä tunnistamista suoranaisesti koskevaa lainsäädäntöä ei muualla Euroopassa ole vielä voimassa.<sup>95</sup> Sen säädökset koskevat luotettavan sähköisen tunnistamisen keskeisiä edellytyksiä ja tunnistamispalveluiden tarjoajien valvontaa. Ko. lain lisäksi asiakkaiden tunnistamisesta on joitakin säännöksiä myös muissa laeissa, kuten mm. laissa luottolaitostoiminnasta sekä laissa rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä.

Suomessa ei ole erillistä tietoturvalakia, vaan tietosuojaa ja tietoturvaa koskevat yleisluontoiset säännökset on sisällytetty lähinnä henkilötietolakiin (523/1999) ja sähköisen viestinnän tietosuojalakiin (516/2004).<sup>96</sup> Keskeiset periaatteet niin yksittäisen maksutapahtuman turvallisuudesta huolehtimisessa kuin myös tietojen säilyttämisen turvallisuuden kannalta voidaan johtaa tietosuojadirektiivin (95/46/EY) 17 artiklasta, jonka henkilötietojen keräämistä ja käsittelyä koskevia ehtoja sovelletaan myös tietojen vaihtoon maksumarkkinoilla. Artiklan mukaan ”henkilötietoja käsittelevän henkilöllä (rekisterinpitäjällä) on velvollisuus huolehtia henkilötietojen käsittelyn turvallisuudesta. Jäsenvaltioiden on säädettävä rekisterinpitäjän velvollisuudesta toteuttaa tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi kaikelta laittomalta tietojen käsittelyltä, muun muassa luvattomalta tietojen luovuttamiselta.” Tämä tietosuojadirektiivin säännös on implementoitu Suomessa henkilötietolain 7. Lukuun. Nyttemmin viittaussäännös ko. lakiin henkilötietojen käsittelystä maksupalveluiden tarjoajien osalta on sisällytetty myös maksupalvelulakiin. MPL 86§:ssa ilmoitetaan että henkilötietojen käsittelyyn maksupalvelutoiminnassa sovelletaan, mitä henkilötietolaissa säädetään. Lisäksi mainitaan, että jos tietojen käsittely on välttämätöntä maksupalveluihin liittyvien rikosten estämiseksi tai selvittämiseksi, palveluntarjoajat saavat luovuttaa tietoja keskenään sen jälkeen kun rikoksesta on ilmoitettu poliisille. Jos se on välttämätöntä maksupalvelutoimintaan kohdistuvan vakavan tai laaja-alaisen uhkan torjumiseksi, tiedon saa kuitenkin rekisteröidä ja luovuttaa jo ennen poliisille ilmoitusta.

Henkilötietolaki on teknologiariippumatonta lainsäädäntöä, joka jättää rekisterinpitäjille mahdollisuuden hyvinkin vapaaseen teknologioiden valintaan ja itseohjautuvaan toiminnan suunnitteluun. Tällaisen avoimen lainsäädännön toinen puoli on sen tulkinnanvaraisuus.<sup>97</sup> Näin

---

<sup>95</sup> Linnake, IT Viikko 1.9.2009. <http://www.itviikko.fi/tietoturva/2009/09/01/sahkoinen-tunnistus-yrittaa-uudestaan/200919216/7> Haettu 20.1.2011

<sup>96</sup> Salminen, 2009, s.81.

<sup>97</sup> Salminen, 2009, s.49.

ollen lainsäädäntöä onkin täydennetty erillisillä maksuyhteisöjen laatimilla tietoturvaa koskevilla säännöksillä ja periaatteilla, kuten mm. pankkiyhteysmaksujen osalta euroalueen pankkeihin sovellettavalla Euroopan maksuneuvoston (EPC) turvallisuusohjeilla ja korttimaksujen osalta Kansainvälisen korttimaksamisen yhteisön (PCI) antamilla standardeilla. EPC on luonut sääntökirjat, jotka sisältävät perusasiat yhtenäisen euroalueen maksutuotteiden turvallisuuteen liittyvistä järjestelyistä, jonka lisäksi se on panostanut verkkoturvallisuuden edistämiseen myös julkaisemalla erilaisia periaatteita ja menettelytapoja joita tulisi käyttää maksamisessa, kuten kuvauksen hyvistä käytännöistä ja ohjeet asiakkaan ja pankin väliseen rajapintaan kun käytetään elektronisia yhteystapoja <sup>98</sup> sekä julkaisun puhelimella tapahtuvan maksamisen periaatteista ja turvallisuudesta. <sup>99</sup> PCI:n standardit taas määrittelevät korttimaksamisen turvallisuuden teknisten vaatimusten minimitason, ja ne koskevat palveluntarjoajien lisäksi myös kauppiaita, järjestelmätoimittajia ja -valmistajia.

#### **4.2.4 Maksamisen sopimukset**

Vaikka lainsäädäntö onkin tärkeä osa sähköisen maksamisen kokonaisuutta, sähköisen maksamisen ja siihen liittyvien vastuiden määrittelyssä tärkeä rooli on myös maksutapahtumaan osallistuvien tahojen välisillä sopimuksilla. Sähköisen kaupan maksutapahtumissa maksajan ja maksun saajan välisen perusvelkasuhdetta koskevan sopimuksen lisäksi yksilöitävissä ovat sopimukset maksajan ja hänen maksunvälittäjänsä, maksajan ja saajan maksunvälittäjien- sekä saajan ja hänen maksunvälittäjänsä välillä.

##### **4.2.4.1 Perusvelkasuhteeseen liittyvä sopimus**

*Perusvelkasuhde* solmitaan siis maksajan ja maksun saajan välillä. Maksutapahtumien taustalla oleva ko. suhde osapuolten välillä voi olla luonteeltaan joko kerta- eli yksittäisluontoinen tai vastaavasti jatkuva eli kestopuoltonen, jolloin siihen liittyvän velvoitteen täyttäminen edellyttää useita toistuvia maksusuorituksia sidonnaisuuden voimassaoloaikana. Kestovelkasuhteille on ominaista, että kysymys oikeasta maksusuorituksesta saattaa tulla samassa oikeussuhteessa ajankohtaiseksi useita kertoja. Aurejärven ja Hemmon näkemyksen mukaan ko. tapauksissa

---

<sup>98</sup> Saatavilla osoitteessa <http://www.europeanpaymentscouncil.eu/documents/EPC397-08%20v1%201%20C2Bsecurity%20good%20practices%20guide.pdf>

<sup>99</sup> Saatavilla osoitteessa <http://www.europeanpaymentscouncil.eu/documents/EPC220-08%20EPC%20GSM%20TSM%20WP%20V1.pdf>

suoritusten oikeellisuuden arvioinnin olisi oltava toisaalta yksilöllistä, mutta toisaalta kuitenkin myös sopimuskokonaisuuden huomioon ottavaa.<sup>100</sup>

Itse varsinaisen maksunvälityksen kannalta ei perusvelkasuhteeseen liittyvällä sopimuksella ole yleensä kuitenkaan suurempaa merkitystä. Velvoiteoikeudellisesti rahan maksaminen on pikemminkin yleistäyttöisluontoinen suoritus, jonka voi *de facto* tehdä myös joku muu velallisen puolesta: vaikka velallinen pysyy samana, suorituksen sisältöön nähden on yleensä merkityksetöntä, kuka täyttää siihen liittyvän maksuvelvoitteen.<sup>101</sup> Jos maksunvälitystä koskevat edellytykset ovat olemassa, yksittäiset maksut toteutetaan maksujärjestelmässä huolimatta siitä onko perusvelkasuhde pätevä vai ei.<sup>102</sup> Esimerkiksi sähköisen rahan maksuissa tai tilisiirtojen välityksessä perusvelkasuhteen yksityiskohdat eivät ole maksunvälittäjien tiedossa, ja näin ollen maksunvälittäjä eli pankki tai sähkörahayhteisö ei vastaa esimerkiksi siitä, jos maksaja suorittaa maksun epähuomiossa väärälle vastaanottajalle.

Maksupalvelun tarjoajat eivät kuitenkaan ole täysin vailla vastuuta myöskään perusvelkasuhteen osalta, vaan tietyissä tilanteissa myös palveluntarjoajat voivat joutua arvioimaan asiakkaidensa välisen suhteen vaikutusta heidän omaan toimintaansa. Esimerkiksi luottoon perustuvassa maksujenvälityksessä perusvelkasuhteen merkitys voi korostua, jos perusvelkasuhteessa tapahtuu sopimusrikkomus osapuolten välillä. Tämän lisäksi on myös muitakin tilanteita, joissa maksujenvälittäjillä voidaan katsoa olevan tietty korostettu vastuu välittämistään maksuista. Nämä liittyvät useimmiten lainvastaiseen tai rikolliseen toimintaan. Esimerkiksi Terämaan mielestä maksujenvälittäjällä on rahanpesulain perusteella yleiseen huolellisuusvelvollisuuteen liittyvä velvollisuus jättää lainvastaiseen toimintaan perustuvat maksut välittämättä silloin, kun välittäjällä on tästä tieto.<sup>103</sup> Lisäksi maksupalvelulaissa on jätetty palveluntarjoajille mahdollisuus kieltäytyä maksutoimeksiannoista myös muista syistä. Tällainen tilanne voisi tulla kysymykseen esimerkiksi jos maksujenvälittäjällä olisi tieto tai vähintäänkin vahva oletus siitä, että annettu maksutoimeksianto on virheellinen. Käytännössä maksuun liittyvän perusvelkasuhteen vaikutus tulee pankkien harjoittamassa toiminnassa arvioitavaksi kuitenkin hyvin harvoin.<sup>104</sup>

---

<sup>100</sup> Aurejärvi – Hemmo, 2007, s.12.

<sup>101</sup> Aurejärvi – Hemmo, 2007, s.12-13.

<sup>102</sup> Terämaa, 2001, s.282.

<sup>103</sup> Terämaa, 2001, s.283.

<sup>104</sup> Terämaa, 2001, s.283.

#### 4.2.4.2 Maksujärjestelmää koskevat sopimukset

*Maksujärjestelmää koskevia sopimuksia* taas solmitaan maksun välittävien palveluntarjoajien kesken. Ne ovat olennainen osa sopimusketjua, kun maksaja ja saaja käyttävät eri maksunvälittäjiä. Pankkien välillä tapahtuvaa maksujensiirtoa koskevilta osilta maksujenvälityssopimukset ovat yleensä sisällöltään yhteneviä.<sup>105</sup> Nämä sopimukset ovat kuitenkin sinänsä merkittäviä, että ne muodostavat perusedellytykset yhtenäisen maksujärjestelmän luomiselle.

Finanssialan keskusliiton laatimien maksujenvälityksen yleisten ehtojen lisäksi myös maksupalvelulaissa on joitain pakottavia määräyksiä koskien palveluntarjoajien välisiä rahansiirtoja. Nämä liittyvät mm. maksutoimeksiantojen toteuttamisaikoihin, palveluntarjoajien välisiin vastuihin maksutapahtumien suhteen sekä joihinkin tiedonanto-oikeuksiin ja -velvollisuuksiin, joista palveluntarjoajat eivät voi sopia toisin. Ko. ehdot ja määräykset rajoittavat palveluntarjoajien keskinäistä sopimusvapautta maksujenvälityksen suhteen.

#### 4.2.4.3 Maksujenvälitystä ja saamisoikeutta koskevat sopimukset

Merkittävimpiä sopimuksia maksunvälitykseen liittyvien vastuiden kannalta ovat kuitenkin *sopimukset maksajan ja maksajan välittäjän sekä maksun saajan ja välittäjän välillä*. Maksajan ja hänen maksunvälittäjänsä välisen oikeustilan sääntelyssä on useimmiten peruslähtökohtana saamisoikeutta koskeva sopimus, kuten pankin talletussopimus, luottokorttisopimus tai sähköistä rahaa koskeva sopimus.<sup>106</sup> Kyseisten sopimusten ehdot sovitaan yleensä puiteluontoisesti velkojan (tallettaja tai luottokorttiyhtiö) ja velallisen (pankki-, luottokortinhaltija tai e-rahamarkkinan osittaja) kesken. Näiden sopimusten sisältö vaihtelee pääasiallisesti siitä riippuen, onko kyse talletuksesta vai luottomuotoisesta saamisesta.

Maksupalvelun käyttäjien asema suhteessa palveluntarjoajiin on varsin suojattu myös maksamiseen liittyvien sopimusten solmimisen osalta. Maksupalvelulaissa säädetään pakottavasti tietyistä maksupalveluissa käytettävistä sopimusehdoista. Sen 7§:ssa säädetään, että sopimusehto jolla poiketaan lain säännöksistä maksupalvelun käyttäjän, eli maksajan tai maksun vastaanottajan vahingoksi, on mitätön, ellei ko. laissa jäljempänä säädetä toisin. Kuitenkin tilanteissa jossa

---

<sup>105</sup> Terämaa, 2001, s.286.

<sup>106</sup> Terämaa, 2001, s.283.

maksupalvelun käyttäjä ei ole kuluttaja, maksupalvelun käyttäjä ja palveluntarjoaja voivat sopia toisin useista seikoista kuten mm. tiedonantovelvollisuuksista, puitesopimuksesta, maksutoimeksiannon toteuttamisesta sekä erinäisistä muista vastuista ja velvollisuuksista maksutapahtumiin liittyen. Näin ollen maksupalvelulain pakottavat säännökset rajaavat toisaalta sopimusten vaikutusmahdollisuuksia sähköisessä maksamisessa varsin perusteellisesti kuluttajien osalta, mutta toisaalta sallivat laajemman sopimusvapauden muiden maksupalvelun käyttäjien, kuten esim. yritysten osalta.

Toisaalta myös pienmaksuvälineiden käytöstä tehtävien sopimusten osalta maksupalvelulaki mahdollistaa tavallista laajemman sopimusvapauden. Toisin voidaan sopia mm. tiedonantovelvollisuuksista, maksutoimeksiannon peruuttamisesta, maksutapahtuman toteuttamisajasta, katoamisilmoituksen teosta, sekä erinäisistä lievemmistä vastuista sekä velvollisuuksista. Tämä laajempi sopimusvapaus on säädetty lähtökohtaisesti pienmaksuvälineiden teknisten ominaisuuksien ja käyttötarkoituksen sekä toisaalta niiden käytön edistämistarkoituksen vuoksi. Se kuitenkin myös lisää maksupalvelun käyttäjien omaa vastuuta ko. maksupalvelun sopimusehtoihin tutustumisen osalta.

Maksupalvelulain ohella myös luottolaitoslaissa on asetettu joitakin rajoituksia ko. sopimusten sisällölle. LuottolL126§:ssa määrätään että Luottolaitos ei saa toiminnassaan käyttää sopimusehtoa, joka ei kuulu luottolaitoksen toimintaan tai jota on pidettävä asiakkaan kannalta kohtuuttomana. Kyseinen kohtuullisuusvaatimus koskee kaikkia luottolaitoksen tekemiä sopimuksia eikä esim. edellytä, että asiakas on kuluttaja. Saman pykälän toisessa momentissa määrätään, että luottolaitoksen on toimitettava Finanssivalvonnalle (ent. Rahoitustarkastus) sen toiminnassa käytettävien vakioehtoisten sopimusten ehdot. Fiva valvoo ko. sopimusehtojen käyttöä ja markkinointia.

Näiden saamisoikeutta koskevien sopimusten ohella etämuotoisten ja elektronisten maksumuotojen toteuttamistavan takia on talletusvaatimukseen perustuvien maksuliikepalvelujen osalta tarpeellista erikseen sopia tavoista, joilla ko. saamisoikeutta käytetään maksamiseen. Näiden ns. maksujenvälitys sopimusten<sup>107</sup> on oikeuskirjallisuudessa katsottu muodostavan aivan oman sopimustyyppinsä.<sup>108</sup>

---

<sup>107</sup> Esim. Verkkopankkisopimus, Sähköisen rahan käyttösopimus.

<sup>108</sup> Terämaa, 2001, s.284.



Pankkiyhteysmaksamisessa tilin verkkokäytöstä tehdään lähes poikkeuksetta erillinen sopimus. Luottokortin käyttöön perustuvassa maksamisessa erillinen sopimus maksukäytöstä tehdään harvoin.<sup>109</sup> Etämaksamiseen liittyviä ehtoja sisällytetäänkin nykyään useimmiten varsinaisiin korttisopimuksiin. Näidenkin ehtojen osalta palveluntarjoajien on kuitenkin huomioitava että myös niiden laatimiseen liittyy tiettyjä kohtuullisuusvaatimuksia. On esiintynyt ainakin yksi tapaus, jossa voidaan katsoa että maksunvälityssopimuksella yritettiin rajoittaa maksupalveluyrityksen vastuuta etämaksamisessa kohtuuttomasti suhteessa käyttäjiin: Nordean vanhojen korttiehtojen<sup>110</sup> kohdassa 3.7 täsmennettiin, että ”Kortinhaltija saa kortillaan maksaa ostoksia *ainoastaan* sellaiselle Internet-kauppiaalle, joka on mukana Verified by Visa- tai MasterCard SecureCode- palvelussa”. Kuitenkin luottokunnan, joka koordinoi ko. sopimusten ehtoja, käyttöehdoissa tällaista edellytystä ei ole eikä ollut, vaan ainoastaan edellytys siitä, että asiakas huolehtii maksamisen tietoturvasta. Myös kuluttajansuojalaki alleviivaa luotonantajan vastuuta kaupan peruuntuessa. Nordean em. ehdon voidaan katsoa olleen vähintäänkin kyseenalainen. Uusissa yrityksen korttiehdoissa<sup>111</sup> mainitaankin internet-maksamisen osalta ainoastaan, että ”Kortinhaltijan *suositellaan* maksavan kortillaan ostoksia ainoastaan sellaiselle Internet-kauppiaalle, joka on mukana Verified by Visa- tai MasterCard SecureCode- palvelussa *tai* jonka kortinhaltija tietää muuten olevan turvallinen.”

Kokonaisuutena maksamisesta tehtyjen osapuolten välisten sopimusten osalta voidaan sanoa, että palveluntarjoajien mahdollisuus rajoittaa lakiin perustuvaa vastuutaan maksamiseen liittyvillä sopimuksilla vaihtelee jonkin verran käytettävän sähköisen maksuvälineen ja sen perusteella, onko maksupalvelun käyttäjä kuluttaja vai muu taho. Maksuvälineistä eniten sopimusperusteista liikkumavaraa on mikromaksujen, kuten tiettyjen mobiilimaksujen ja sähköisen rahan maksujen osalta, käyttäjien osalta etenkin kuluttajien asema on yleensä varsin hyvin suojattu.

---

<sup>109</sup> Terämaa, 2001, s.284.

<sup>110</sup> Nordea, Korttiehdot 21.4.2008.

<sup>111</sup> Ks. Nordea, 2010<sup>a</sup>, s.3. [http://www.nordea.fi/sitemod/upload/root/fi\\_org/appx/fin/ehdot/MKYE900dl.pdf](http://www.nordea.fi/sitemod/upload/root/fi_org/appx/fin/ehdot/MKYE900dl.pdf)

## **5. SÄHKÖISEN MAKSAMISEN ERITYISKYSYMYKSET**

Verrattuna fyysisen maksutapahtuman sisältävään maksamiseen, sähköisessä ympäristössä maksaminen sisältää useita, ensisijaisesti maksuympäristöön liittyviä erityispiirteitä, jotka on otettava huomioon kaikessa sähköisessä maksamisessa niin maksujenvälittäjien, maksujärjestelmiä käyttävien osapuolten kuin lainsäätäjänkin taholta toimivan ja turvallisen maksuympäristön aikaansaamiseksi. Kysymykset sähköisen maksamiseen liittyen, joihin on syytä kiinnittää erityistä huomiota, voidaan jakaa pääpiirteittäin varsin luontevasti kolmeen osa-alueeseen: maksamisen turvallisuuteen, maksutapahtumaan ja sen toteuttamiseen sekä muihin, kuten alueen lainsäädännöstä tai yhteiskunnallisista tavoitteista aiheutuviin kysymyksiin.

### **5.1 MAKSUJEN TURVALLISUUTEEN LIITTYVÄT KYSYMYKSET**

Ensimmäinen käsittelemistäni aihekokonaisuuksista sähköiseen maksamiseen liittyen on sähköisen maksuympäristön turvallisuus. Sähköisessä maksuympäristössä turvallisuusriskit korostuvat, koska osapuolet eivät maksutapahtuman yhteydessä tapaa fyysisesti toisiaan. Tämän lisäksi sähköinen ympäristö on myös fyysistä ympäristöä houkuttelevampi kanava erilaiselle rikolliselle toiminnalle huomattavasti pienemmän kiinni jäämisen riskin takia. Heikko luottamus verkkoympäristöön haittaa vakavasti verkkotalouden kehitystä: komission tiedonannon mukaan huolet maksujen turvallisuudesta ja yksityisyydestä sekä puuttuva luottamus ovat keskeisiä syitä verkkopalveluiden käytön rajoittamiseen.<sup>112</sup> Näin ollen erityisesti henkilön oikeelliseen tunnistamiseen, maksutapahtuman tietoturvallisuuteen sekä näissä tapahtuviin ongelmatilanteisiin liittyvään osapuolten väliseen vastuunjakoon onkin sähköisessä ympäristössä syytä kiinnittää erityistä huomiota.

#### **5.1.1 Identiteetin ja henkilön tunnistamisen merkitys sähköisessä maksuympäristössä**

Henkilön tunnistamisella tarkoitetaan henkilön identiteetin todentamista. Tämä on oikeustointen pätevyyteen ja asiointiturvallisuuteen liittyvä perusedellytys.<sup>113</sup> Vertailtaessa perinteiseen, fyysiseen osapuolten kohtaamiseen perustuvaan maksamiseen, sähköisiä maksujärjestelmiä käytettäessä oikeustoimen tekijän identiteetin todentamisen merkitys korostuu, koska on mahdollista että oikeustoimen osapuolet eivät tapaa missään vaiheessa henkilökohtaisesti toisiaan.

---

<sup>112</sup> KOM (2010)245, s.13.

<sup>113</sup> Terämaa, 2001, s.293.

Jos henkilöllisyydestä erehdytään, seuraukset voivat olla merkittäviä, varsinkin tapauksissa joissa rahasuoritus maksetaan ennakolta tai suorituksen määrä on suuri.<sup>114</sup> Myös viime aikoina lisääntyneet identiteettivarkaudet ovat korostaneet identiteetin oikeellisen tunnistamisen tärkeyttä maksutapahtumien yhteydessä. Näin ollen onkin syytä tarkastella sitä, mikä on juridisesta näkökulmasta katsottuna riittävä turvallisuuden taso henkilön sähköiselle tunnistamismenetelmälle ko. henkilön sitomiseksi sen perusteella maksutapahtumaan, identiteettierehdyksien seurauksia ja vastuunjakoa sekä toisaalta sitä, miten tällä hetkellä tunnistaminen on eri maksuvälineiden osalta käytännössä järjestetty.

### 5.1.1.1 Henkilön tunnistamisen juridiset velvoitteet

Vastuu osapuolten luotettavan tunnistamisen järjestämisestä maksutapahtumien yhteydessä on lähtökohtaisesti *maksun välittäjällä*. LuottolL145§ sääntelee luottolaitosten ja niiden konsolidointiryhmään kuuluvien rahoituslaitosten vastuuta asiakkaidensa tuntemisesta. Ko. pykälän mukaan näiden on tunnettava asiakkaansa ja tarvittaessa asiakkaan todellinen edunsaaja ja henkilö, joka toimii asiakkaan lukuun. Luottolaitoksiksi em. laissa määritellään yritykset, joilla on lupa luottolaitostoimintaan. Maksupalvelulain myötä myös sähköisen rahan liikkeeseenlasku on nimenomaisesti otettu osaksi luottolaitostoiminnan määritelmää, joten lain soveltamisala on kattava sähköisten maksujen välittäjälaitosten osalta.

Asiakkaan tuntemisesta on myös voimassa, mitä lain rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä 2. luvussa säädetään. Lisäksi ko. lain 18§ 3.momentissa säädetään erikseen *etätunnistamiseen liittyvästä tehostetusta tuntemisvelvollisuudesta* seuraavasti: ”Jos asiakas ei ole läsnä tunnistettaessa ja henkilöllisyyttä todennettaessa (etätunnistaminen), ilmoitusvelvollisen tulee todentaa asiakkaan henkilöllisyys vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa tarkoitetulla *tunnistusvälineellä tai laatuvarmenteella* taikka muun sähköisen tunnistamistekniikan avulla, joka on tietoturvallinen ja todisteellinen.”<sup>115</sup>

Sähköisessä ympäristössä henkilön tunnistamisen on näiden lakien perusteella tapahduttava siis luottolaitosten taholta ja erityisellä tunnistusvälineellä tai vaihtoehtoisesti vähintään laatuvarmenteen kriteerit täyttävällä tunnistamistekniikalla. *Tunnistusvälineen* määritelmä löytyy

---

<sup>114</sup> Terämaa, 2001, s.294.

<sup>115</sup> Muulla tietoturvallisella ja todisteellisella tunnistautumistekniikalla tarkoitetaan tässä sellaista varmennetta, joka täyttää laatuvarmenteelle asetetut vaatimukset.

Lain vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 2 pykälän 2. momentista: ”tunnistusvälineellä tarkoitetaan esineitä ja yksilöiviä tietoja tai ominaisuuksia, jotka yhdessä muodostavat *vahvaan sähköiseen tunnistamiseen* tarvittavat tunnisteet, tunnistamisen välineet ja todentamisen välineet”. *Varmenne* taas määrittellään saman lain 1. Luvun 2.7§:ssa ”sähköiseksi todistukseksi, joka todentaa henkilöllisyyden tai todentaa henkilöllisyyden ja liittää allekirjoituksen todentamistiedot allekirjoittajaan ja jota voidaan käyttää *vahvassa sähköisessä tunnistamisessa* sekä sähköisessä allekirjoituksessa”. *Laatuvarmenne* määrittellään vastaavasti varmenteeksi, joka täyttää 2 momentissa säädetyt vaatimukset<sup>116</sup> ja jonka on myöntänyt lain 33–38§:ssä säädetyt erilliset lisävaatimukset täyttävä varmentaja.

Sekä em. tunnistusvälineet että myös laatuvarmenteet perustuvat siis nimenomaisesti *vahvan sähköisen tunnistamismenetelmän käyttöön*. Vahva sähköinen tunnistaminen on määritelty lain vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 2 pykälän 1 momentissa. Sillä tarkoitetaan ”henkilön yksilöimistä ja tunnisteiden aitouden ja oikeudellisuuden todentamista sähköistä menetelmää käyttämällä perustuen *vähintään kahteen* seuraavista kolmesta vaihtoehdosta”:

- 1) salasanaan tai johonkin muuhun sellaiseen, mitä tunnistusvälineen haltija *tietää*
- 2) sirukorttiin tai johonkin muuhun sellaiseen, mitä tunnistusvälineen haltijalla *on hallussaan*
- 3) sormenjälkeen tai johonkin muuhun tunnistusvälineen haltijan *yksilöivään ominaisuuteen*

Voidaan katsoa, että tunnistamismenetelmän luotettavuus paranee sitä mukaa mitä useamman edellä mainituista oletuksista huomioi ja tarkistaa tunnistustilanteessa.<sup>117</sup> Toisaalta jos henkilö kyetään tunnistamaan täysin yksiselitteisesti ja luotettavasti pelkästään häneen liittyvän yksilöivän ominaisuuden perusteella, tällöin voidaan myös oletettavasti puhua vahvasta tunnistamisesta. Lisäksi vahvalle sähköiselle tunnistamisen menetelmille on asetettu lain 3. Luvun 8§:ssa muitakin vaatimuksia. Sen mukaan:

- 1) menetelmän perustana on oltava *ensitunnistaminen*
- 2) menetelmällä on voitava yksiselitteisesti tunnistaa tunnistusvälineen haltija

---

<sup>116</sup> Laatuvarmentajan osalta vaaditaan muun muassa käytettävien laitteiden ja ohjelmistojen luotettavuutta, erillisten varmennerekisterin ja sulkulistan ylläpitämistä sekä harjoitetun toiminnan laajuuteen nähden riittäviä teknisiä taitoja ja taloudellisia voimavaroja.

<sup>117</sup> Liikenne- ja viestintäministeriö, 2003<sup>b</sup>, s.20.

- 3) menetelmällä on voitava *riittävällä* luotettavuudella varmistua, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä
- 4) menetelmä on *riittävän* turvallinen ja luotettava ottaen huomioon kulloinkin käytävissä olevaan tekniikkaan liittyvät tietoturvallisuusuhat.

Ensitunnistamisen vaatimuksesta johtuu, että vahva henkilön tunnistamisprosessi ei koskaan voi olla täysin sähköinen, koska lain vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 17§:ssa nimenomaisesti säädetään, että tunnistusvälineen hakijan ensitunnistamisen on tapahduttava henkilökohtaisesti. Ainoastaan silloin, kun tunniste palvelun tarjoajat ovat tehneet sopimuksen siitä, että he luottavat toistensa tekemään ensitunnistamiseen, tunnistusvälinettä voidaan hakea kokonaan sähköisesti. Tällöinkin ensitunnistaminen on kuitenkin aiemmin tehty henkilökohtaisesti toisen tarjoajan taholta. Lain vaatimusten perusteella vahvan sähköisen tunnistamisen ei myöskään tarvitse olla täysin aukotonta: menetelmien on oltava ainoastaan *riittävän* luotettavia välineitten käytön osalta. Verrattuna fyysiseen tunnistamiseen, tämä voidaan mielestäni katsoa kohtuulliseksi, sillä henkilön tunnistamisessa voidaan erehtyä myös ko. tapahtumissa. Ko. lakien vaatimusten lisäksi Finanssivalvonta on antanut tarkempia määräyksiä asiakkaan tunnistamisessa noudatettavista menettelytavoista.<sup>118</sup>

### 5.1.1.2 Identiteetin oikeudellinen merkitys maksutapahtumassa

Henkilö tunnustetaan siis oikeudellisesta näkökulmasta tarpeeksi suurella varmuudella ainoastaan vahvan tunnistamisen menetelmillä. Henkilön identiteetin tunnistaminen antaa *tukevan perusteen oikeustoimen hyväksymiselle*, etenkin jos henkilö on tunnistettu em. vahvaa identifioimismenetelmää käyttämällä. Tästä huolimatta edes kehittyneillä menetelmillä ei ole ollut tarkoituksena luoda sellaista oikeudentilaa, jossa henkilö tulee *kaikissa tilanteissa* ja ilman myötävaikutustaan sidotuksi oikeustoimiin, jotka on tehty hänen nimissään jonkin teknisen tunnistamismenetelmän avulla. Tämä on varsin ymmärrettävää sen takia, että lähtökohtaisesti

---

<sup>118</sup> FiVan kannanoton mukaan asiakkaan tunnistaminen ja asiakkaan henkilöllisyyden todentaminen ovat keskeisiä asiakkaan tuntemiseen liittyviä velvollisuuksia. Tunnistusvälineiden hakijat pitää kannanoton mukaan tunnistaa henkilökohtaisesti siinä yhteydessä, kun he ensimmäisen kerran hakevat tunnituslain tarkoittamaa asiointitunnistetta. Asiakassuhde voidaan perustaa kuitenkin tapaamatta asiakasta henkilökohtaisesti sillä edellytyksenä että valvottavalla on käytössään menetelmät, joiden avulla se pystyy todentamaan asiakkaan henkilöllisyyden luotettavasti. Esimerkkinä tästä tunnituslaisia tarkoitettuja tunnistusvälineitä, jotka täyttävät vahvan sähköisen tunnitusvälineen tai laatuvarmenteen kriteerit tai muut sähköiset tunnistamistekniikat, jotka ovat tietoturvallisia ja todisteellisia. Asiakassuhteen aikana tunnistaminen voi kuitenkin perustua myös tietoturvalliseen ja todennettavissa olevaan asiointitunnukseen. Ks. Finanssivalvonta 2/101/2010: Standardi 2.4, s.20 - 21.

verkossa asioidessa ei ole täysin aukotonta keinoa välttää joko identiteettierohdykseen tai erityisesti identiteetin oikeudettomaan käyttöön liittyviltä riskeiltä. Näiden ko. riskien hallinnan kannalta tärkeä merkitys tunnistamismenetelmien ohella onkin myös sopimuksenmukaisten velvoitteiden oikea-aikaisella täyttämällä eli suoritusten ajoituksella.<sup>119</sup>

### 5.1.1.3 Identiteettierohdyksen seuraukset: oikeudettomat maksutapahtumat ja vastuunjako

Itse varsinaiset fyysiset maksuvälineet, joita tarvitaan sähköisessä maksutapahtumassa, kuten luottokortti, matkapuhelin tai pankkitunnukset voivat joutua virheellisesti kolmannen osapuolen haltuun. Tämän lisäksi huolimatta parantuneista turvallisuuskäytännöistä verkkomaksamisessa on myös mahdollista, että esim. luottokortin tai pankkipalvelun tunnistetiedot päätyvät sähköisessä ympäristössä kolmannen osapuolen haltuun. Kyseiset tilanteet voivat johtaa identiteettierohdyksiin ja sitä kautta oikeudettomiin maksutapahtumiin. Myös oikeudettomissa maksutapahtumissa sähköisessä maksuympäristössä on lähtökohtaisesti siis palveluntarjoajan näkökulmasta useimmiten kyse siitä, että maksajan henkilöllisyydestä erehdytään. Vaikka henkilöllisyyserehdyksistä johtuneet oikeustapaukset eivät sähköisessä maksamisessa ole olleet kovin yleisiä, asiaan liittyvää vastuunjako on syytä tarkastella koska ko. erehdystilanteiden vaikutukset voivat olla varsin huomattavia käyttäjien kannalta.

Sähköiseen maksusuoritukseen liittyvän identiteettierohdyksen seuraukset ja siihen liittyvä riskinjako voivat vaihdella käytetyn maksuvälineen ja siihen liittyvän sääntelyn sekä palvelusta tehtyjen sopimusten perusteella. Maksun suorittajan kannalta luvattomaan maksutoimeen liittyvän riskin kantajina voivat olla niin velkoja, maksunvälittäjä, varojen oikea omistaja kuin järjestelmän ylläpitäjäkin. Identiteettiä koskevien erehdystilanteiden moninaisuudesta johtuen vastuunjako on tarkasteltava tapauskohtaisesti. Merkityksellisiä seikkoja arvioinnissa ovat ensinnäkin osapuolten asema ja osapuolten toiminta mutta myös maksujärjestelmän rakenteelliset seikat ja maksutyypit.<sup>120</sup>

Vastuunjaon juridisena pääsääntönä tapauksissa on pidettävä oikeustoimiopin yleistä lähtökohtaa siitä että *oikeustoimi sitoo tekijäänsä vain silloin kun hän on sen itse tehnyt tai jos joku muu sellainen taho jolla on siihen kelpoisuus, on tehnyt sen hänen lukuunsa*. Toisin sanoen identiteettierohdystilanteissa tahdonilmaisun vastaanottaja kantaa oikeustoimiopin mukaan

---

<sup>119</sup> Terämaa, 2001, s.298.

<sup>120</sup> Terämaa, 2001, s.295.

taloudellisen riskin siitä, että oikeustoimi on tehty jonkun muun nimissä. Vastaanottajan asemaan ei tapauksessa vaikuta, onko hän tahdonilmaisun vastaanottaessaan vilpittömässä mielessä vai ei. Tähän pääsääntöön liittyy kuitenkin muutamia poikkeuksia. Oikeustoimi voi sitoa henkilöä, jonka nimissä se on tehty, jos

- oikeustoimen tekoon on annettu ennalta suostumus
- oikeustoimi hyväksytään jälkikäteen, vaikka sen on tehnyt joku muu
- henkilö, jonka lukuun oikeustoimi on tehty, on menetellyt lainvastaisesti tai huolimattomasti
- oikeustoimi sitoo toleranssivaltuutuksen tai vastaavan tilanteen takia
- oikeustoimen sitovuus perustuu lakiin.<sup>121</sup>

Identiteettierhdystä ja siihen liittyvää vastuunjakoa oikeudettomista maksutapahtumista, myös sähköisessä maksuympäristössä, käsitellään kotimaan lainsäädännössä usean eri lain kohdassa varsin vastaavan sisältöisinä. Taustana näille säännöksille on ylikansallinen lainsäädäntö. Jo aiemmin kuluttajansuojalaki sisälsi varsin nykyistä vastaavia säännöksiä luottokortin oikeudettoman käytön tapauksista. Nytemmin säännöksiin on tehty joitakin tarkennuksia, ja soveltamisalaa on laajennettu kattamaan muutkin maksuvälineet. Säännökset löytyvät pääosiltaan yhtenäisisältöisinä niin maksupalvelulaista, kuluttajansuojalaista<sup>122</sup> kuin laista vahvasta sähköisestä tunnistautumisesta ja sähköisistä allekirjoituksistakin<sup>123</sup> Koska käsitelen teoksessa ensisijaisesti maksamiseen liittyviä erehdys- ja väärinkäyttötilanteita, käytän näistä vaihtoehdoista laajemman tarkastelun kohteena maksupalvelulain säännöksiä. MPL 62§ sisältää säännökset maksupalvelun käyttäjän vastuusta ja sen rajoituksista maksuvälineen oikeudettoman käytön tilanteissa ja 63§ palveluntarjoajan vastuusta oikeudettomien maksutapahtumien osalta. Maksupalvelun käyttäjän vastuu rajoitetaan pykälän 62 kohtien tilanteissa 2 ja 3 enintään 150 euroon. Tätä rajoitusta ei kuitenkaan sovelleta, jos käyttäjä on toiminut *tahallisesti* tai *törkeän huolimattomasti*.<sup>124</sup>

---

<sup>121</sup> Terämaa, 2001, s.298.

<sup>122</sup> Ks. KSL 40§: Kuluttajan vastuu luottokortin tai muun jatkuvan luoton käyttöön oikeuttavan tunnisteen oikeudettomasta käytöstä.

<sup>123</sup> Ks. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 27§: Tunnistusvälineen haltijan tunnistusvälineen oikeudetonta käyttöä koskevat vastuunrajoitukset.

<sup>124</sup> Se mitä voidaan pitää lain mukaan törkeänä huolimattomuutena, on jätetty maksupalveludirektiivissä kansallisen tulkinnan varaan. Hallituksen esityksessä mainitaan, että törkeällä huolimattomuudella tarkoitetaan MPL: ssa sellaista erittäin vakavaa varomattomuutta, joka osoittaa selvästi piittaamatonta suhtautumista maksuvälineen hallintaan ja käyttöön liittyviin turvallisuusriskeihin. Esimerkkinä törkeästä huolimattomuudesta mainitaan esimerkiksi maksukortin ja tunnusluvun säilyttäminen samassa lompakossa. Matkapuhelinten osalta esitys on kuitenkin lievempi. Sen mukaan on tavanomaista, että matkapuhelinta pidetään jatkuvasti auki, jonka takia esimerkiksi sitä, että matkapuhelimen

Ko. pykälän mukaan maksupalvelun käyttäjä, joka on tehnyt maksuvälinettä koskevan sopimuksen palveluntarjoajan kanssa vastaa maksuvälineen oikeudettomasta käytöstä vain, jos

- 1) hän (tai muu maksuvälineen haltija) on luovuttanut maksuvälineen sen käyttöön oikeudettomalle,
- 2) maksuvälineen katoaminen, joutuminen oikeudettomasti toisen haltuun tai oikeudeton käyttö johtuu hänen (tai muun maksuvälineen haltijan) *huolimattomuudestaan* itse maksuvälineestä tai siihen liittyvistä tunnistetiedoista huolehtimisessa
- 3) hän (tai muu maksuvälineen haltija) on laiminlyönyt velvollisuuttaan ilmoittaa palveluntarjoajalle tai sen nimeämälle muulle taholle maksuvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheetonta viivytystä sen havaittuaan.

Lisäksi säädetään, että maksupalvelun käyttäjä **EI** kuitenkaan vastaa tunnisteen oikeudettomasta käytöstä:

- 1) siltä osin kuin maksuvälinettä on käytetty sen jälkeen, kun palveluntarjoajalle on ilmoitettu maksuvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä
- 2) jos palveluntarjoaja on laiminlyönyt huolehtia siitä, että maksuvälineen haltijalla on mahdollisuus täyttää 1 momentin 3 kohdan mukainen ilmoitusvelvollisuutensa; tai
- 3) jos maksunsaaja ei ole maksuvälinettä käytettäessä asianmukaisesti varmistunut maksajan oikeudesta käyttää maksuvälinettä.

Lainkohdassa on myös lisäys, että ”maksupalvelun käyttäjä on kuitenkin vastuussa maksuvälineen oikeudettomasta käytöstä, jos hän tai muu maksuvälineen haltija on tahallaan tehnyt väärän ilmoituksen tai toiminut muuten petollisesti”. Lisäksi laissa on mainittu, että osapuolet voivat sopia, että vastuu jakaantuu toisin kuin 62§ ja 63§:n mukaan sikäli kun maksupalvelun käyttäjä ei ole kuluttaja. Lisäksi 77§:ssa säädetään vastuusta käytettäessä pienmaksuvälinettä: lainkohtien mukaan maksupalvelun käyttäjä ja palveluntarjoaja voivat sopia, ettei ilmoitusvelvollisuuspykälää sovelleta

---

käyttäjältä jää matkapuhelin joukkoliikennevälineeseen jonka seurauksena sitä käytetään oikeudettomasti maksutapahtumiin, ei voida vielä sinänsä pitää törkeänä huolimattomuutena. (HE 169/2009vp, s.75)



jos pienmaksuvälineen käyttöä ei sen ominaisuuksien vuoksi voida estää. Lain 78§:ssa todetaan, että ko. säännöksiä ei sovelleta sähköiseen rahaan, mikäli palveluntarjoajalla ei ole mahdollisuutta estää tilin tai maksuvälineen käyttöä.

Kyseiset säännökset rajaavat ja tarkentavat kuluttajan vastuuta identiteettirehdyksistä johtuvista oikeudettomista maksutapahtumista varsin merkittävästi. Usein lainsäädäntöä täydennetään maksajan ja palveluntarjoajan välisellä sopimuksella, johon voi sisältyä tarkempia sääntöjä siitä, mitä tietoja käyttäjän on sallittua luovuttaa. Maksuvälineen luovuttamisella *ei* kuitenkaan yleensä tarkoiteta maksuvälineessä olevan kiinteän numerotiedon luovuttamista, joka on usein palveluntarjoajien hyväksymä tapa käyttää maksuvälinettä (esimerkiksi luottokortin numero), vaan varmennetietojen luovuttamista, joiden avulla vastapuoli voi valheellisesti varmistua maksuvälineen haltijan identiteetistä. Maksupalvelun käyttäjien vastuu oikeudettomista maksutapahtumista on näin ollen varsin rajattu sikäli, kun he toimivat lain edellyttämällä huolellisuudella. Tämän voidaan katsoa olevan maksujärjestelmien käytettävyyden edistämisen kannalta varsin oleellista.

Laki jättää kuitenkin epäselväksi sen, mikä on maksupalvelun käyttäjiltä vaadittava riittävä huolellisuuden taso. Kotimaan oikeuskäytännössä on käsitelty maksulaitoksen ja maksupalvelun käyttäjän välistä vastuunjakoa maksuvälineen oikeudettoman käytön tilanteessa lähinnä luottokorttimaksamiseen liittyvien erehdystilanteiden osalta. Näissä tilanteissa itse identiteetistä ei ole varsinaisesti erehdytty, vaan henkilön oikeudesta käyttää maksuvälinettä, mutta koska seuraamukset ovat samat, voidaan tapauksia käsitellä vastaavasti.

Esimerkiksi tapauksessa KKO 2006:81 henkilön luottokorttia oli käytetty oikeudettomasti kahtena päivänä yhteensä 21 maksutapahtumassa 2 870,18 euron arvosta. Myyjäliikkeiden toimesta oli tarkastettu, ettei korttia ollut ilmoitettu kadonneeksi tai anastetuksi ja että luottoraja oli riittävä. Henkilö oli pitänyt luottokorttiaan, jonka luottoraja oli 4 000 euroa, lompakossa pikkutakkinsa povitaskussa. Ko. henkilö ei ollut tarkistanut luottokortin tallella oloa eikä ollut itse ennen pankin yhteydenottoa havainnut kortin katoamista, vaikka oli mm. matkustanut täysissä metrojunissa ja riisunut takkinsa ravintolassa tuolin selkänojalle. Henkilö oli ollut tietoinen siitä, että kaupungissa, jossa hän oleskeli, oli erityinen vaara joutua taskuvarkauden kohteeksi. Vaikka henkilön seurue ei ollut havainnut mitään epäilyttävää tapahtuneen, korkein oikeus määräsi, että ko. henkilö on KSL 7.19§ huolimattomuussäännöksen nojalla itse vastuussa luottokorttinsa oikeudettomasta käytöstä. Perusteluina päätökselle esitettiin, että maksuvälineen haltijalta on edellytettävä sen tallella olon seuraamista *olosuhteiden vaatimaa huolellisuutta noudattaen*, vaikka laissa ei olisikaan nimenomaisesti mainittu ko. velvollisuudesta. Tämän olemassaoloon viittaa kuitenkin velvollisuus ilmoittaa viipymättä kortin katoamisesta. Se, kuinka

usein tapahtuvaa tarkistamista huolellisuus edellyttää, riippuu olosuhteista ja erityisesti niihin liittyvistä katoamis- ja anastusriskeistä. Esimerkiksi kortinhaltijan liikkua suurissa ihmisjoukoissa tai muissa paikoissa, joissa taskuvarkauksen riski on erityisen suuri, tarkistamisvelvollisuus on korostunut, koska ammattimaisesti suoritettua taskuvarkautta ei yleensä huomata sen tapahtuessa.<sup>125 126</sup>

Vaikka em. tapaus ei olekaan tapahtunut nimenomaisesti sähköisessä ympäristössä, sitä voidaan mielestäni soveltaa lain tulkintaan myös mahdollisissa vastaavissa sähköisen maksamisen tilanteissa. Tapauksesta voidaan vetää johtopäätöksiä vaadittavasta huolellisuuden tasosta, ja periaatteet ovat yleistettävissä koskemaan yhtä lailla kaikkia muitakin oikeustoimen teossa käytettäviä tunnisteita,<sup>127</sup> kuten esimerkiksi verkkopankkien tunnuslukulistoja tai sähköisen rahan sovellusten asiointitunnuksia. Voidaan katsoa, että identiteettierhdyksen ja oikeudettomien maksutapahtumien kohdalla keskeisin yksittäinen tekijä vastuunjaon kannalta onkin tarkennettuna maksupalvelun käyttäjien *tilannesidonnainen huolellisuus* maksuvälineen ja siihen liittyvien tunnistetietojen huolehtimisesta. Näkemystä tukee maksupalvelulain 53§ jonka mukaan maksuvälineen haltijan on huolehdittava maksuvälineestä ja siihen liittyvistä tunnistetiedoista kohtuullisin toimenpitein, sekä HE169/2009:n perustelut kohtuullisista varotoimista sekä huolellisuuden tasosta, jonka vaatimukset ovat yhtäläisiä tapauksen KKO 2006:81 perustelujen kanssa.

Tämä tarkoittaa käytännössä sitä, että kun maksaja on toiminut em. riittävällä tilannesidonnaisella huolellisuudella, vastuu identiteettierhdyksistä jakautuu palveluntarjoajien sekä myös mahdollisesti kauppiaiden kesken. Vahvan henkilön tunnistamismenetelmän sisältävissä maksutapahtumissa vastuu on kuitenkin tunnistamisesta vastuussa olevalla osapuolella eli sähköisessä toimintaympäristössä asioidessa yleensä palveluntarjoajalla. Maksutapahtumissa, joissa ko. vahvaa tunnistamista ei suoriteta, vastuuta voidaan vierittää myös myyjille. Esimerkiksi pelkkien luottokortin tunnistetietojen avulla maksettaessa sähköisessä ympäristössä, luottokorttiyhtiöt solmivat kauppiaiden kanssa usein ns. acquirer- sopimuksia, joissa vastuu identiteettierhdyksistä asetetaan maksun vastaanottavalle taholle kohtuuttoman riskin välttämiseksi.

---

<sup>125</sup> KKO 2006:81

<sup>126</sup> Luottokortin katoaminen ei KSL 7 luvun 19 §:n 1 momentin mukaan sinänsä aiheuta tilinhaltijalle vastuuta kortin käytöstä katoamisen jälkeen eikä esimerkiksi taskuvarkauden kohteeksi joutumisen sellaisenaan voida katsoa osoittavan huolimattomuutta.

<sup>127</sup> Saarenpää et al., 1997, s.458.

#### **5.1.1.4 Yleisesti sähköisessä maksuympäristössä käytössä olevien henkilön tunnistamismenetelmien arviointia**

Henkilön tunnistamiseen sähköisessä ympäristössä on olemassa monia erilaisia menetelmiä.<sup>128</sup> Nämä menetelmät tuottavat usein eriasteista varmuutta siitä tosiasiaista onko henkilö se, joksi hän esittäytyy varmentamistilanteessa. Sähköisessä maksamisessa kussakin tapauksessa käytettävän tunnistamismenetelmän varmuuden olisi vähintäänkin oltava tarkoituksenmukaisessa suhteessa ko. transaktion merkittävyyteen.

Jotta henkilö voitaisiin tunnistaa sähköisesti, on henkilön yksilöivä ja henkilön hallussa oleva ominaisuus, tieto tai fyysinen tunniste oltava sähköisesti luettavissa ja todennettavissa. Käytettyjä menetelmiä henkilön sähköiseen tunnistamiseen ovat muun muassa käyttäjätunnukset ja salasanat sekä niiden yhdistelmät, varmenteet mukaan luettuna laatuvarmenteet, biometriset tunnisteet sekä radiotaajuustunnisteet.<sup>129</sup> Toistaiseksi ei ole käytössä yhtäkään laajasti levinnyttä ja yhteensopivaa teknistä tunnistamismenetelmää sähköisen kaupan tarpeita tai edes pelkästään maksuliikennettä varten,<sup>130</sup> vaan sähköisen tunnistamisen menetelmät ovat vielä pääosin kansallisia. Nykyisin yleisimmin käytetty todentamistapa on salasanan käyttö. Tämä voi riittää monissa sovelluksissa, mutta turvallisempia ratkaisuja tarvitaan entistä useammin.

##### **5.1.1.4.1 Korttimaksujen yhteydessä käytettävät tunnistusmenetelmät**

Luottokortin tunnistetietojen avulla verkossa maksettaessa luottokorttiyhtiöt ovat tunnistaneet asiakkaansa perinteisesti pelkästään korttiin liittyvän informaation perusteella. Tämä tunnistustapa on kuitenkin puutteellinen, eikä täytä vahvan tunnistamisen kriteereitä: kortin numero ja muut tiedot ovat maksun yhteydessä yleensä kaikkien korttimediaa käsittelevien tahojen saatavilla,<sup>131</sup> jonka lisäksi huolena tämäntyppisessä maksamisessa on myös ollut luotettavuus käytettävää tiedonsiirtojärjestelmää kohtaan. Myöskään sekä maksajan että maksun vastaanottajan identiteetistä

---

<sup>128</sup> Terämaa, 2001, s.297.

<sup>129</sup> Biometriset tunnisteet sekä radiotaajuustunnisteet (RFID) eivät ole olleet kovinkaan yleisessä käytössä sähköisissä maksujärjestelmissä. Radiotaajuusteknologiasta on kuitenkin saatu viime aikoina hyviä kokemuksia etenkin sähköisen rahan sovelluksissa. RFID perustuu elektronisen sirun käyttöön. Siru voidaan liittää eri välineisiin, kuten tuotetunnisteisiin tai henkilökortteihin. Sirun sisältämät tiedot luetaan langattomalla lukulaitteella: kortin täytyy vain koskettaa lukijaa. Kyseistä sovellusta kutsutaan kuitenkin ”kontaktittomaksi”. (Euroopan talous- ja sosiaalikomitea, 2009, liite 1)

<sup>130</sup> Terämaa, 2001, s.296.

<sup>131</sup> Terämaa, 2001, s.302.

ei tällä menettelyllä pystytä luotettavasti varmistumaan, vaan ainoastaan seikoista, kenen luottokorttia maksussa käytetään ja keneksi maksun vastaanottaja esittäytyy sähköisessä toimintaympäristössä.

Koska vilpilliset Internet-transaktiot ovat lisääntyneet, on syntynyt tarve parantaa maksamiskäytäntöä. Luottokorttiyhtiöt ovat kehittäneet pankkien kanssa yhteistyössä luotettavampia tekniikoita asiakkaiden tunnistamiseksi ja maksutapahtuman suorittamiseksi. Yleiseksi käytännöksi luottokortilla maksamisessa onkin muodostunut ns. vahvan identifioimismenetelmän liittäminen osaksi maksutapahtumaa. Käyttäjä varmentaa henkilöllisyytensä maksutapahtumassa kortti-informaation lisäksi omien verkkopankkitunnustensa tai erillisen salasanan avulla. Tunnistautuminen tapahtuu siis ns. pseudonyymisti<sup>132</sup>: luottokorttiyhtiö toimii välikätenä ja luotettuna kolmantena osapuolena kauppiaan ja asiakkaan välissä, jolloin kauppiaille ei välity lainkaan ostajan luottokorttinumeroa. Turvallisemman maksutapahtuman lisäksi tällä menettelyllä vältetään myös tarpeettomalta henkilötietojen keruulta: käyttäjien tiedot eivät pääse leviämään eri palveluntarjoajille sitä mukaa kun he asioivat verkossa luottokortin tunnistetietojen avulla.<sup>133</sup> Esimerkkinä ko. menettelystä ovat muun muassa luottokorttiyhtiöiden Visan ja MasterCardin lanseeraamat kansainväliset Verified by VISA- ja MasterCard SecureCode- todentamispalvelut, joiden avulla yritysten kortinhaltijat voivat maksaa verkkoympäristöissä joko luottokortin ja verkkopankkitunnusten tai vaihtoehtoisesti luottokortin ja erillisen henkilökohtaisen salasanan avulla. Myyjien palveluissa ko. järjestelmän olemassaolosta on ilmoitettu selkeästi. Näin *sekä ostajan että kauppiaan tunnistamisen varmuus on parantunut.*<sup>134</sup> Verified by Visa – palvelu on pelkästään Euroopassa jo yli 50 000 verkkokauppiaan käytössä, ja palvelua käyttävien kauppiaiden määrä kasvaa päivittäin.<sup>135</sup>

Voidaan kuitenkin kyseenalaistaa, onko kehitys riittävää. Mm. Korhonen väittää, että vaikka teknisellä puolella kehitystä onkin tapahtunut, toteutuksessa on yhä toivomisen varaa: kansainväliset luottokorttiyhtiöt mahdollistavat edelleen että verkkokaupassa maksukortteja voidaan

---

<sup>132</sup> Kolmikanta: yksilö toimittaa todistuksen identiteetistään kolmannelle, luotetulle osapuolelle, joka vuorostaan laskee liikkeelle yksilölle määritellyn pseudotunnisteen. Ns. oikeudet varmistetaan suoran identiteettivarmistuksen sijaan. Usein tärkeintä osoittaa että pseudonyymien takana oleva henkilö pysyy samana koko tapahtuman ajan. (Viemerö, 2009, s.224-225.)

<sup>133</sup> Viemerö, 2009, s.225.

<sup>134</sup> Visa:n internetsivut, <http://www.visa.fi>. Haettu 25.11.2010.

<sup>135</sup> Luottokunnan internetsivut, [http://www.luottokunta.fi/fi/kortit\\_ja\\_setelit/visa/verified\\_by\\_visa](http://www.luottokunta.fi/fi/kortit_ja_setelit/visa/verified_by_visa). Haettu 25.11.2010.

käyttää pelkän korttinumeron perusteella, eikä Verified by Visa – palvelu ei ole yleistynyt riittävästi verkkokaupoissa Euroopan ulkopuolella. Näin ollen korttidatan joutuessa väärin käsiin, ostoksia voidaan tehdä esimerkiksi monissa amerikkalaisissa tai aasialaisissa verkkokaupoissa ilman varmuutta maksajan identiteetistä.<sup>136</sup> Korttidatan tai korttinumeroiden perusteella voidaan myös valmistaa väärennettyjä luottokortteja, joilla voidaan tehdä ostoksia tai käteisnostoja.<sup>137</sup> Korttimaksamiseen liittyvässä tunnistamisessa onkin sen käyttöasteeseen suhteutettuna havaittavissa kokonaisuudessaan kaikkein eniten puutteita: sähköiseen korttimaksamiseen liittyvät ongelmat ovat globaalilla tasolla varsin merkittävä kaikkien sähköisten maksupalveluiden luottamusta heikentävä tekijä.

#### 5.1.1.4.2 Verkkopankkitunnistautuminen

Pankkiyhteismaksuissa suomessa verkkopankit tunnistavat asiakkaansa yleensä henkilökohtaisten asiakastunnusten ja vaihtuvien salasanojen yhdistelmillä. Yksityisellä sektorilla on jo pitkään katsottu voitavan luottaa näihin pankkien myöntämiin Tupas2–tunnisteisiin<sup>138</sup> vahvana tunnistamisena. Myös julkisella sektorilla on sittemmin annettu suositus ja ohje, jonka mukaan pankkitunnisteita voidaan käyttää vahvana tunnistamismenetelmänä varmenteiden rinnalla.<sup>139</sup> Tätä tunnistamistapaa pidetään teknisesti PKI- menetelmään<sup>140</sup> perustuvaa tunnistamista heikompana, mutta käytännössä riittävän luotettavana ja turvallisena.<sup>141</sup> Pankkitunnisteiden suurimpina etuina verrattuna muihin menetelmiin on niiden vakiintunut ja säännöllinen käyttö verkkopankeissa ja laaja käyttäjäkunta.<sup>142</sup> Suomessa verkkopankkitunnistaminen onkin ylivoimaisesti suosituin tunnistamismuoto: Finanssialan Keskusliiton mukaan verkkopankkisopimuksia oli vuonna 2009 tehty yhteensä 4 928 000 kappaletta. Tupas2- tunnistautumista käytetään verkkopankin ohella myös

---

<sup>136</sup> Korhonen, Talouselämä 40/2009, s.8.

<sup>137</sup> Keskusrikospoliisi, 2009, s.7.

<sup>138</sup> Tupas2 on pankkien yhteistyössä kehittämä tunnistuspalvelu asiointipalveluntuottajille. Tarkempi palvelun kuvaus löytyy esim. Finanssialan keskusliiton sivuilta [http://www.fkl.fi/teemasivut/sahkoinen\\_asiointi/tupas/Sivut/default.aspx](http://www.fkl.fi/teemasivut/sahkoinen_asiointi/tupas/Sivut/default.aspx)

<sup>139</sup> Liikenne- ja viestintäministeriö, 2008<sup>a</sup>, s.3.

<sup>140</sup> PKI, Public Key Infrastructure, ts. Julkisen avaimen menetelmä.

<sup>141</sup> Menettelyn suurimmat tekniset heikkoudet ovat salasanojen lyhyys ja se, että kertakäyttösalsat luodaan pankin ympäristössä ennen niiden toimittamista asiakkaalle. Ks. TIEKE, Tietoyhteiskunnan kehittämiskeskuksen julkaisusarja: Luottamus tietoverkkojen käytössä – Varmenteet ja pankkitunnisteet, 2007, s.16.

<sup>142</sup> Liikenne- ja viestintäministeriö, 2008<sup>a</sup>, s.6.

muissa maksutapahtumissa, joissa pankki tunnistaa asiakkaansa pankkipalvelutunnusten avulla myös palveluntuottajan puolesta.

Arvostelijoidensa mukaan kyseinen tunnistautumismuoto ei suuresta suosiostaan sekä tunnistamisohjeistuksesta huolimatta ole kuitenkaan tietoturvasoltaan paljoakaan käyttäjätunnukseen ja salasanaan perustuvaa tunnistamista turvallisempi, saati sitten täytä vahvan tunnistamisen määritelmiä.<sup>143</sup> Salasanalistat ovat tulostettuna paperille tai luottokortin tyyppiselle ”turvakortille”, joten ne ovat helposti kopioitavissa. Tämän lisäksi käyttäjät kirjoittavat valitettavan usein käyttäjätunnuksensa paperille ja jopa ko. salasanalistoihin, jotta muistaisivat ne itse. Salasanalistoista voidaan myös yleensä päätellä varsin vaivattomasti, mihin palveluun ne antavat käyttöoikeuden.<sup>144</sup> Näin onkin siis mahdollista, että sekä henkilökohtaiset asiakastunnukset että vaihtuvat salasanat päätyvät samanaikaisesti jonkun muun kuin kyseisen asiakkaan käyttöön, joka tietää lisäksi palvelun, jossa niitä käytetään. Tätä ei toisaalta voida pitää kuitenkaan kovinkaan todennäköisenä ilman asiakkaan erityisen huolimattontaa menettelyä, joka on muutenkin rajaava peruste palveluntarjoajien vastuun kannalta.

Kuitenkin, ainakin yhdessä tapauksessa Tupas2 – palvelu on toisaalta pettänyt myös teknisellä tasolla: käyttäjä pääsi kirjautumaan palveluun toisen käyttäjän nimissä omilla pankkitunnuksillaan. Poliisin tietotekniikkarikosyksikön suoritetun esitutkinnan perusteella annetun tiedotteen<sup>145</sup> mukaan kyse oli ”useista sattumista joiden toistumisen todennäköisyys on erittäin pieni.” Kuitenkin todennäköisyys tähän on siis olemassa, joten tapaus paljastaa että ko. tunnistautumismenetelmä ei ole täysin aukoton. Tupas2 – tunnisteiden soveltuvuuden arvioinnissa vahvaan henkilön tunnistamiseen kysymys kuuluukin, voidaanko tällaisista epätodennäköisistä tapauksista huolimatta katsoa, että kyseinen tunnistautumisen muoto antaa *riittävän* varmuuden henkilön identiteetistä sähköisessä tunnistautumisessa.

#### 5.1.1.4.3 Varmenteet

Luotettavimpina tunnistamismenetelminä Suomessa on yleisesti pidetty julkisen avaimen menetelmään (PKI) perustuvia varmenteita. Väestörekisterikeskus on Suomessa ainoa

---

<sup>143</sup> Aikavuori, Tilisanomat 2/2009, s.68.

<sup>144</sup> Liikenne- ja viestintäministeriö, 2003<sup>b</sup>, s.40.

<sup>145</sup> Poliisi, 2008. <http://www.poliisi.fi/poliisi/bulletin.nsf/vwSearchView/161EC35E75C233BCC2257455003ECB03>  
Haettu 13.2.2011.

laatuvarmentaja, joka pystyy tarjoamaan lain vaatimukset täyttäviä ja EU-direktiiviin pohjautuvia yleiseurooppalaisia, korkean tietoturvan ja oikean henkilöllisyyden sisältäviä varmenteita - sen myöntämät varmenteet ovat julkisen avaimen menetelmään perustuvia laatuvarmenteita.<sup>146</sup> Väestörekisterikeskuksen kansalaisvarmenne oli myönnetty marraskuun 2010 loppuun mennessä 341 800 henkilölle, ja voimassaolevia varmenteita oli tällöin 272 200 kappaletta.<sup>147</sup>

Väestörekisterikeskuksen tarjoamien varmenteiden osalta ongelma on ollut enemmän puutteissa niiden käytettävyydessä kuin turvallisuudessa. Tällä hetkellä suurin osa myönnettyistä varmenteista on hst- henkilökorteilla: kortin sirulla oleva tunnistusväline ei ole kuitenkaan nykypäivää, eikä läheskään kaikissa tietokoneissa ole edes sopivaa kortinlukijaa. Tästä huolimatta niiden käyttöä on ylläpidetty, koska on katsottu että pankkitunnisteiden rinnalla tulee olla tarjolla muitakin sähköisestä tunnistamisesta ja allekirjoituksista annetun lain mukaisia vahvan tunnistautumisen ratkaisuja.<sup>148</sup>

#### **5.1.1.4.4 Muut tunnistusratkaisut**

Ongelmat luottokorttien, verkkopankin ja varmenteiden osalta sekä verkkorikollisuuden lisääntyminen sähköisessä ympäristössä ovat viitanneet siihen, että sähköisen maksamisen alueella saattaisi olla kysyntää uusille tunnistusratkaisuille. Yhtenä varteenotettavana vaihtoehtona on nähty esimerkiksi ns. kahden kanavan tunnistusratkaisut, joissa asiakkaan oikeus käyttää maksuvälinettä varmennetaan kahta erillistä välinettä hyödyntäen. Tämän tyyppisen menetelmän käyttö vähentää riskiä identiteettirehdyksistä ja oikeudettomista maksutapahtumista huomattavasti.

Nämä uudet tunnistusratkaisut on usein yhdistetty matkapuhelimiin ja matkapuhelinteknologian hyödyntämiseen. Mm. Ranskassa pankit ovat ilmoittaneet siirtyvänsä uudenlaiseen varmennusmenetelmään luottokorttimaksamisen yhteydessä lisätäkseen varmuutta kortinkäyttäjistä: asiakkaan syötettyä korttitietonsa ja turvallisuuskoodinsa verkkokauppaan, pankki lähettää vielä hänen kännykkäänsä joka kerta vaihtuvan varmennustunnuksen tekstiviestillä, ja asiakas varmentaa sillä ostotapahtuman. Kauppa ja pankki varmistavat näin kahdella erillisellä

---

<sup>146</sup> Väestörekisterikeskuksen internetsivut, <http://www.vaestorekisterikeskus.fi/default.aspx?id=145> Haettu 9.4.2011.

<sup>147</sup> Väestörekisterikeskuksen FINEID.FI -internetsivut, <http://fineid.fi/default.aspx?site=9&docid=4035>. Haettu 9.4.2011.

<sup>148</sup> KK 620/2010vp, s.2.

välineellä asiakkaan oikeuden käyttää tilin varoja.<sup>149</sup> Kyseinen menettely minimoi identiteettirehdyksen riskiä, koska tällöin rikollisten olisi saatava haltuunsa sekä asiakkaiden matkapuhelin että asiointitiedot. Verkkopankkeihin kohdistuneiden phishing ja man-in-the middle – tyylisten hyökkäysten jäljiltä myös Suomessa joidenkin verkkopankkien tunnistautumiseen on lisätty vastaavanlaisia turvaominaisuuksia: epätavallisen suuria tai muuten poikkeuksellisia maksutapahtumia ei enää välttämättä hyväksytä suoraan, vaan niihin voidaan pyytää vahvistus käyttäjiltä esimerkiksi puhelimitse tai tekstiviestillä. Näin ollen käyttäjän tunnistus perustuu tässäkin kahteen eri välineeseen.

Toisaalta, matkapuhelinta voidaan käyttää identiteetin varmistamisessa em. viestintäominaisuuksia hyödyntävien tapojen ohella myös varsinaisena tunnistusvälineenä, ns. mobiilivarmenteena. Se on matkapuhelimen sim- korttiin liitettävä sähköisen tunnistautumisen ja allekirjoituksen väline, jota voi käyttää sähköiseen henkilöllisyyden todistamiseen niin erilaisiin sähköisiin palveluihin kirjautumisessa kuin myös henkilöiden keskinäisessä asiointissa. Mobiilivarmenne täyttää viimeaikaisten lakimuutosten jälkeen myös laissa vahvalle sähköiselle tunnistamiselle asetetut vaatimukset: asiakas tunnistetaan varmenteellisen sim- kortin sekä itse luotavan 4-8 numeroisen tunnusluvun yhdistelmällä. Avainlukulistoja mobiilivarmenteessa ei käytetä, jonka voidaan katsoa lisäävän menetelmän turvallisuutta.<sup>150</sup> Lisäksi, koska tunnistautuminen tapahtuu erillään asiointikanavasta, esimerkiksi netissä yleistynyt tunnusten kalastelu ei myöskään onnistu.

Suomessa mobiilivarmenne otettiin yleisökäyttöön marraskuun 2010 lopulla, joten sen käyttömahdollisuudet ovat vielä erittäin rajalliset. Ulkomailla vastaavaan teknologiaan perustuvia palveluita on jo käytössä lukuisissa eri maissa, kuten Turkissa (pankkitunnistautuminen, rahan nosto pankkiautomaatista), Virossa (kansalaisvarmenne laajasti käytössä) ja Norjassa (BankID). Kokemukset mm. näistä maista osoittavat, että sähköisen tunnistamisen alueellinen kehitys on edennyt muita vertailumaita paremmin, kun alueella on kyetty kahden tai useamman osapuolen välisiin toimiviin yhteistyöjärjestelyihin. Suomessa on myös perinteisesti ollut vahvuutena yksityisen ja julkisen sektorin yhteistyö. Nämä perinteet on syytä ottaa käyttöön myös vahvan sähköisen tunnistamisen osalta, sillä toimivien vahvan sähköisen tunnistamisen markkinoiden vaikutus tietoyhteiskuntakehityksemme hyödyttää voimakkaasti kaikkia osapuolia.<sup>151</sup> Käyttäjien

---

<sup>149</sup> Korhonen, Talouselämä 40/2009, s.8.

<sup>150</sup> Mobiilivarmenne.fi, 2010. [http://www.mobiilivarmenne.fi/fi/fi\\_7.html](http://www.mobiilivarmenne.fi/fi/fi_7.html) Haettu 1.12.2010.

<sup>151</sup> Liikenne- ja viestintäministeriö, 2008<sup>b</sup>, s.3.



luottamus vahvan sähköisen tunnistamisen palveluihin edellyttää lisäksi, että vahvaa tunnistamista tarjoavat ja käyttävät palveluntarjoajat huolehtivat kuluttajansuojaa ja yksityisyyden suojaa koskevien säännösten huolellisesta noudattamisesta.<sup>152</sup>

Joka tapauksessa, mobiilivarmenne näyttäisi tällä hetkellä olevan varsin varteenotettava vaihtoehto tuotaessa markkinoille uusia sähköisen henkilön tunnistamisen ratkaisuja. Turvallisuuskulmien lisäksi sillä on muihin tunnistamiskäyttöihin verrattuna muitakin etuja: kehittämissä on ajateltu myös operaattoririippumattomuutta sekä käyttömukavuuteen liittyviä näkökulmia.<sup>153</sup> Lisäksi järjestelmä on palveluntarjoajille esimerkiksi kertakäyttösalasanoihin perustuvaa tunnistautumista huomattavasti kustannustehokkaampi.<sup>154</sup> Pitemmällä tähtäimellä on jopa suunniteltu, että sekä verkkopankkitunnistautuminen että luottokorttimaksut verkossa voitaisiin suorittaa ainakin vaihtoehtoisesti mobiilivarmen avulla. Yleistyäkseen palvelun täytyy kuitenkin olla myös hintatasoltaan kilpailukykyinen muihin tunnistuskäyttöihin verrattuna.

#### 5.1.1.5 Anonyymi maksaminen vaihtoehtona

On hyvä muistaa, että sähköinen tunnistaminen ei ole kuitenkaan itse tarkoitus vaan luotettavan sähköisen asioinnin mahdollistaja.<sup>155</sup> Vaikka sähköiset varmentamismenetelmät kehittyvätkin jatkuvasti, on myös syytä huomata että joissain sähköisissä maksutapahtumissa muiden, usein käytön sujuvuuteen ja käyttömukavuuteen liittyvien, seikkojen merkitys voi olla niin merkittävä, että käyttäjien näkökulmasta maksajaa ei välttämättä tarvitsisi tunnistaa. Tämä voi olla palvelun käyttäjille tarkoituksenmukaista esimerkiksi mikromaksujen yhteydessä, kun maksettava summa ja/tai maksutilin taloudellinen arvo ovat riittävän pieniä. Tällöin voidaan katsoa että jokaisen maksutapahtuman yhteydessä erikseen mm. tunnistautumisen vaivalloisuudesta aiheutuvat vaihtoehtoiskustannukset ovat suurempia käyttäjille kuin se riski, että maksutiliä käytettäisiin oikeudettomasti.

Näiden ns. anonyymien maksupalveluiden osalta on kuitenkin huomattava, että tällöin myös vastuu maksuvälineen tai maksutilin oikeudettomasta käytöstä voidaan jakaa eri tavalla. Maksupalvelulain 77§ sekä eräiden muiden lain säännösten mukaan jos *pienmaksuväline* on ominaisuuksiltaan

---

<sup>152</sup> Liikenne- ja viestintäministeriö, 2008<sup>b</sup>, s.5.

<sup>153</sup> Hämäläinen, Tietokone 8/2010, s.50 - 51.

<sup>154</sup> Liikenne- ja viestintäministeriö, 2008<sup>b</sup>, s.43.

<sup>155</sup> Liikenne- ja viestintäministeriö, 2008<sup>b</sup>, s.7.

sellainen, että sitä käytettäessä käyttäjän henkilöllisyys ei tule ilmi, osapuolet voivat sopia, ettei 62§ ja 63§:n vastuusäännöksiä sovelleta. Näin ollen anonyymiä maksutekniikkaa hyödyntävän pienmaksuvälineen haltija voidaan laittaa itse kokonaan vastuuseen maksuvälineestään ja sen asianmukaisesta käytöstä. Koska pienmaksuvälineitä on suunniteltu juuri käteisen korvaajiksi, voidaan myös ko. vastuusäännösten rajoitukset nähdä tarkoituksenmukaisina, sillä näin vastuu pienmaksuvälineen kadottamistapauksissa rinnastuu varsin kitkattomasti lompakon kadottamiseen. Kuitenkin on syytä huomioda, että vaikka *yksittäiset maksutapahtumat* on tapauskohtaisesti mahdollista toteuttaa anonyymisti, sähköinen maksaminen ei voi milloinkaan olla täysin anonyymiä asiakkaan ja liikkeeseenlaskijan välisessä asiakkuussuhteessa. Tämä johtuu ensisijaisesti kansainvälisestä rahanpesun estämislainsäädännöstä, joka luokin huomattavia reunaehtoja mm. sähköisen rahan liikkeeseenlaskijoiden toiminnalle. Siitä huolimatta, että usein anonyymeissa maksujärjestelmissä liikkuvat rahamäärät ovat niin pieniä etteivät ne houkuttele käytännössä rahanpesuun, on syytä kuitenkin muistaa, että anonymiteettiin liittyy aina rikollisen toiminnan, kuten rahanpesun ja veronkierron mahdollisuus, joka täytyy huomioda myös lainsäädännön tasolla. Palveluntarjoajilla onkin aina myös anonyymien maksutapahtuman sisältävissä asiakkuussuhteissa asiakkaidensa tuntemisvelvollisuus.

### 5.1.2 Tietoturvallisuus maksamisessa

Sähköisen maksamisen volyymin kasvaessa viestintäverkkojen ja tietotekniikan turvallisuuden merkitys on noussut maksuvälineiden ja -järjestelmien kannalta keskeiseen asemaan. Internetin leviäminen sekä sähköisten maksujen ja verkkopankkitoiminnan yleistyminen edellyttävät hyvää turvallisuuden tasoa, jotta järjestelmät ja transaktiot sekä käyttäjien henkilötiedot voidaan suojata ulkopuolisilta.<sup>156</sup> Maksaminen verkossa edellyttää hyvin pitäviä tietoturvatkaisuja: mitä enemmän rahaa avoimissa verkoissa liikkuu, sitä enemmän se houkuttelee väärinkäyttäjiä ja rikollisia.<sup>157</sup>

Tietoturvallisuus perusoikeutena voidaan johtaa perustuslain 7.1 pykälästä, jonka mukaan ”jokaisella on oikeus elämään sekä henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen.”<sup>158</sup> Tietoturvallisuus voidaan nähdä sekä kokonaisten järjestelmien toimivuuden takeena että yksilön suojana. Näin on myös maksamisen alueella. Myös yhtenäisen Eurooppalaisen

---

<sup>156</sup> KOM (2003)718, liite 20.

<sup>157</sup> Leinonen, 2008, s.32.

<sup>158</sup> Viemerö, 2009, s.35.

maksualueen syntymiselle järjestelmien turvallisuus on keskeinen haaste. Muun muassa eurooppalaisen digitaalistrategian 2010 yhtenä seitsemästä päämäärästä on luottamuksen ja tietoturvan edistäminen: eurooppalaiset eivät omaksu teknologiaa, johon he eivät luota – käyttäjien on tunnettava olonsa turvalliseksi kytkeytyessään verkkoon.<sup>159</sup> Yksi suurimmista yksittäisistä tekijöistä sille, miksi sähköinen maksaminen ei ole yleistynyt niin nopeasti kuin olisi voinut odottaa, on että monet ovat epäileväisiä sähköisten maksujärjestelmien turvallisuutta kohtaan. Tallennusyhtiö EMC:n tietoturveysyksikkö RSA:n teettämään tietoturvatutkimukseen vastanneista kokonaiset 86 % ilmoitti olevansa huolissaan verkon tietoturvallisuudesta. Ko. tutkimuksen mukaan kuluttajat olisivat valmiita tinkimään jopa maksupalveluiden käyttömukavuudesta, jos asiointi internetissä olisi sen ansiosta turvallisempaa.<sup>160</sup>

Huolet ovat varsin aiheellisia: keskusrikospoliisin mukaan vaikka sekä yritysten tietopääoman käsittely että maksuliikenne ovat siirtyneet sähköiseen muotoon, niiden käsittelyyn käytettävät järjestelmät eivät kaikilta osin tarjoa tiedolle riittävää suojaa.<sup>161</sup> Mm. Euroopan unionin poliisivirasto Europol on todennut kansainvälisen järjestäytyneen maksukorttirikollisuuden, erityisesti tietoverkossa toimivan maksukorttirikollisuuden yhdeksi merkittävimmäksi ja vahvistuvaksi petosrikollisuuden uhaksi. Lisäksi krp painottaa, että ko. rikollisuuden torjumiseen on kuitenkin usein käytettävissä vain kansallisia tai alan rikollisuuteen nähden liian hitaita kansainvälisiä keinoja.<sup>162</sup> Phishing -tyylisten hyökkäysten ohella rikosten toteuttamisessa käytetään nykyään myös muita, kehittyneempiä tekniikoita. Internetissä levitettävien haittaohjelmien avulla maksukorttirikolliset voivat anastaa suuria määriä rahaksi muutettavia luottokorttitietoja ja verkkopankkitunnuksia vähäisellä kiinnijäämisriskillä.<sup>163</sup> Tämän lisäksi maksuympäristönä kehittyvä mobiiliympäristö muodostaa uudenlaisen riskin: koska monien mobiililaitteiden päivitettävyyden ei ole muiden tietokoneiden tasolla, niissä ilmenevä haavoittuvuus saattaa mahdollistaa myös mobiilimaksamisen väärinkäytön.<sup>164</sup>

---

<sup>159</sup> KOM (2010)245, s.18.

<sup>160</sup> Lehto (2010<sup>c</sup>), Tietokone, 27.1.2010.

[http://www.tietokone.fi/uutiset/rsa\\_verkkopankkien\\_tietoturvaa\\_voisi\\_parantaa](http://www.tietokone.fi/uutiset/rsa_verkkopankkien_tietoturvaa_voisi_parantaa) Haettu 18.2.2011.

<sup>161</sup> Keskusrikospoliisi, 2009, s.3.

<sup>162</sup> Keskusrikospoliisi, 2009, s.1.

<sup>163</sup> Keskusrikospoliisi, 2009, s.3.

<sup>164</sup> Keskusrikospoliisi, 2009, s.2.

Vaikka verkon maksuvälinerikoksissa suositaankin usein yritysten maksuvälineitä<sup>165</sup> niiden suuremman taloudellisen arvon vuoksi, ei tämä kuitenkaan tarkoita että yksityishenkilötkään olisivat turvassa verkkorikollisilta. Ilmenevät tietoturvallisuusongelmat heikentävät edelleen kuluttajien luottamusta sähköiseen maksamiseen. Sekä yksittäisten maksutapahtumien- että säilytettävien asiakastietojen riittävä ja huolellinen suojaaminen ovat luonnollisesti tärkeä osa maksupalveluyritysten toimintaa. Tähän on syytä kiinnittää huomiota myös sääntelyn tasolla. Muun muassa Euroopan komissio on huomauttanut tiedonannossaan, että maksuliikennealan olisi varmistettava sähköisille maksuille korkein mahdollinen liiketaloudellisesti kannattava turvallisuustaso.<sup>166</sup> Turvallisen maksuympäristön toteutuminen edellyttää myös viranomaisten ja markkinatoimijoiden yhteistyötä,<sup>167</sup> jonka lisäksi myös kauppiaille ja maksupalvelujen käyttäjillä on omalta osaltaan olennainen rooli turvallisen maksuympäristön luomisessa. Paremmiin koordinoitu vastaus verkkohyökkäyksiin ja henkilötietojen suojaa koskevat tiukemmat säännöt ovat eurooppalaisen digitaalistrategian mukaan osa ratkaisua.<sup>168</sup>

Tietoturvallisuuskysymysten suhteen maksutapahtumissa on syytä erottaa kaksi kokonaisuutta. Ensinnäkin, *yksittäisen maksutapahtuman* turvallisuudesta huolehtiminen on ensisijaisesti maksujärjestelmän ylläpitäjän, mutta myös osittain maksupalvelun käyttäjien vastuulla. Toinen kokonaisuus liittyy *tietomurtoihin tietoverkkoihin* ja niiden kautta erilaisiin tietokantoihin, joissa säilytetään olennaisia tietoja asiakkaista. Näissä esim. luottotietolaitosten tietokantojen turvallisesta säilyttämisestä huolehtimisessa itse luottokortinhaltijoilla ei ole luonnollisestikaan ole mahdollisuutta vaikuttaa omaan turvallisuuteensa.

### 5.1.2.1 Yksittäisten maksutapahtumien turvallisuus ja vastuunjako

Yksittäisten maksutapahtumien osalta lähtökohtana voidaan katsoa olevan, että jokainen maksutapahtumaan liittyvä osapuoli vastaa omalta osaltaan siitä että maksutapahtumasta muodostuu turvallinen. Vaikka yksittäisten maksutapahtumien turvallisuudesta huolehtimisessa suurin rooli onkin maksujärjestelmän ylläpitäjällä, on myös maksupalvelun käyttäjillä, erityisesti kauppiaille mutta myös kuluttajilla omat erityiset velvollisuutensa täytettävinaan. Lainsäädännössä aihetta

<sup>165</sup> Kajantie, Tiedosta 4/2010, s.16.

<sup>166</sup> KOM (2004)679, kappale 5.

<sup>167</sup> Ripatti – Iivarinen, 2010, s.10.

<sup>168</sup> Euroopan komissio, 2010, s.2.

<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/581&format=PDF&aged=1&language=FI> Haettu 21.2.2011. Ks. aiheeseen liittyen myös KOM (2010)245, s.20.

käsitellään kuitenkin varsin yleisellä tasolla, ja yksityiskohtaisempia ohjeita löytyykin maksuyhteisöjen omien valvontaelinten antamista raporteista, joiden lisäksi tärkeä rooli tietoturvallisuusasioihin liittyvän vastuunjaon kannalta on myös maksupalvelusta tehtävillä sopimuksilla.

Esimerkiksi pankkiyhteysmaksujen osalta Euroopan maksuneuvosto EPC on antanut kuvauksen hyvistä tietoturvakäytännöistä elektronisten maksujen osalta, jota kaikkien eurooppalaisten pankkien tulisi noudattaa. Ko. kuvauksessa annetaan varsin kattava selvitys siitä, miten pankkien tulisi järjestää tietoturva-asiansa. Yksittäisten transaktioiden turvallisuutta käsitellään kappaleessa 5.5. Sen pääperiaatteiden mukaan mm. asiakasdataa on suojeltava riittävällä tavalla peilattuna sen tärkeyteen ja riskisyyteen, maksujärjestelmien toimivuutta ja turvatasoa tulee testata ja arvioida säännöllisesti sekä turvalliseen tietojen vaihtoon pitää käyttää ainakin SSL/TLS/https – tason protokollaa, jonka lisäksi korkean luottamuksen data suositellaan kryptattavaksi.<sup>169</sup>

Omien järjestelmiensä turvallisuudesta huolehtimisen lisäksi rahalaitosten tulisi ohjeistaa myös palvelun käyttäjiä asianmukaiseen turvallisuuskäyttäytymiseen. Asiakkaita tulisi ohjeistaa riittävällä tavalla, etteivät he itse paljasta omia arkaluonteisia asiakastietojaan (sensitive data), esimerkiksi sähköpostikalastelun (phishing) tai troijalaisten virusten välityksellä. Instituutioiden ei ole myöskään soveliaista lähettää asiakkailleen sähköpostia jotka sisältävät linkkejä, koska nämä voidaan sekoittaa kalasteluyrityksiin. Lisäksi laitosten tulisi rohkaista asiakkaitaan pitämään päätelaitteensa torjuntaohjelmat ajan tasalla ja päivitettyinä. Niiden pitäisi myös harkita varoitusten antamista tietokoneista, jotka ovat sijoitettu vihamielisiin ympäristöihin. Yhteistyö tietoturvallisuusyritysten kanssa on lisäksi suotavaa. Asiakkailta, jotka yrittävät kirjautua palveluun laitteistolla joka ei täytä teknisiä tai algoritmisiä vaatimuksia, pitäisi evätä sisäänkäyntiä ja ohjeistaa heitä päivittämään laitteistonsa ennen kirjautumista.<sup>170</sup>

Lisäksi rahalaitosten pitäisi kuvauksen mukaan mm. tunnistaa käyttäjiensä korkean riskin transaktiot ja valvoa niiden toteuttamista erityisellä tarkkuudella. Tällaisiin lukeutuvat mm. tilanteet, joissa tili tyhjenetään tai koko luottoraja käytetään kerralla, suuret transaktiot epätavallisiin paikkoihin, transaktiot ns. money mule<sup>171</sup> -tileille sekä tilanteet, joissa esiintyy

---

<sup>169</sup> European Payments Council, 2009, s.16 - 17.

<sup>170</sup> European Payments Council, 2009, s.16 - 17.

<sup>171</sup> Muuli, ts. henkilö, jonka tehtävänä on vastaanottaa rikoksella hankittua omaisuutta ja toimittaa se ketjussa eteenpäin, esim. toiseen valtioon.

viitteitä maksutapahtuman kaappauksesta.<sup>172</sup> Tietoturvallisuudesta huolehtiminen on näin ollen kuvauksen mukaan pankkien osalta kokonaisvaltaista, ja kattaa pankin omista turvallisuuskäytännöistä huolehtimisen lisäksi myös asiakkaiden ohjeistamis- ja valvomisvelvoitteita.

Palveluntarjoajien ohella myös muilla maksutapahtumaan osallistuvilla tahoilla on omat erityiset tietoturvaan liittyvät velvollisuutensa täytettävinaan: kauppiaiden osalta tietoturvallisuutta säännellään esim. maksukorttien käytön osalta PCI-standardeilla. Niiden noudattaminen on pakollista kaikille korttitapahtumia vastaanottaville, välittäville tai tallentaville tahoille.<sup>173</sup> Standardien mukaan mm. tietojen siirron julkisissa verkoissa on tapahduttava aina salatussa ja suojatussa muodossa, jonka lisäksi kauppiaille on myös erilaisia testaus-, kehittämis- ym. velvoitteita. Keskusrikospoliisin tekemän tietoturvallisuusraportin mukaan PCI-standardi on parantanut merkittävästi maksukorttiasioinnin turvallisuutta luomalla kauppiaille aidon kannustimen parantaa järjestelmiensä turvallisuutta. Luottokorttiyhtiöiden käyttöehtojen mukaan tietorikoksesta aiheutuvat kustannukset ovat kauppiaan vastuulla, ellei kauppiaan järjestelmä täytä PCI:n vaatimuksia.<sup>174</sup>

Maksujärjestelmän käyttäjän vastuu huolehtia omalta osaltaan tietoverkon turvallisuudesta yksittäisissä maksutapahtumissa on taas yleensä määritelty maksupalvelun tarjoajan sekä kuluttajan välisissä sopimuksissa. Kuluttaja-asiamiehen kannanoton mukaan siirrettäessä maksukorttitietoja ja muita maksujärjestelmiin liittyviä koodeja Internetissä tai säilytettäessä maksutietoja Internetiin liitettyllä palvelimella, tiedot olisi aina suojattava tehokkaalla salauksella.<sup>175</sup> Yksittäisten maksutapahtumien turvallisuudesta internet- ympäristössä on yleensä huolehdittu salaamalla tietoliikenneyhteys SSL- tekniikalla. Tämä on myös esimerkiksi luottokunnan vähimmäisohjeistus korttimaksujen suorittamiseen internetissä.<sup>176</sup> Käyttäjän vastuulla on turvallisen tietoliikenneyhteyden olemassaolon varmistamisen lisäksi huolehtia myös muista maksutapahtuman turvallisuuteen liittyvistä seikoista, kuten esim. siitä että *oma päätelaite on riittävän turvattu*

---

<sup>172</sup> European Payments Council, 2009, s. 16.

<sup>173</sup> Luottokunta, 2010, s.2.

<sup>174</sup> Keskusrikospoliisi, 2009, s.10.

<sup>175</sup> Kuluttajavirasto, 2004, s.11.

<sup>176</sup> Ks. Luottokunta: Maksaminen internetissä. Luottokunnan internetsivut, [http://www.luottokunta.fi/fi/kortit\\_ ja\\_setelit/ohjeita\\_kortinhaltijalle/maksaminen\\_internetissa#portal-rewrite?a=1;e=0;p=0/portal-rewrite#](http://www.luottokunta.fi/fi/kortit_ ja_setelit/ohjeita_kortinhaltijalle/maksaminen_internetissa#portal-rewrite?a=1;e=0;p=0/portal-rewrite#) Haettu 25.11.2010.

*maksutapahtumaa varten*. Esimerkiksi Nordean pankkitunnuksilla käytettävien palveluiden yleisissä sopimusehdoissa määritellään, että pankki ja asiakas huolehtivat kumpikin omien tietojärjestelmiensä tietoturvasta ja vastaavat siitä, että järjestelmä on riittävällä tavalla suojattu luvaton käyttöä vastaan. Lisäksi mainitaan, että pankin tietoturvaohjeissa on määritelty ne etäviestinväliseen teknisten ominaisuuksien vähimmäisvaatimukset, joita verkkopankkipalvelun käyttö edellyttää.<sup>177</sup> Mahdollisuudet päätelaitteiden suojaamiseen vaihtelevat käytetystä päätelaitteesta riippuen: kannettavia tietokoneita varten on markkinoilla lukuisia suojausohjelmia, kämmentietokoneiden ja vastaavien laitteiden suojausmahdollisuudet ovat toistaiseksi rajoitetummat.<sup>178</sup>

On kuitenkin huomioitava, että edes ohjeiden mukainen toiminta ei kuitenkaan aina ole riittävää. Verkkorikolliset ovat viime aikoina ryhtyneet hyödyntämään uusia tekniikoita verkkopankki-iskuihinsa. Esimerkki tällaisista on Suomeenkin vuonna 2010 rantautunut mies välissä -tyyppinen hyökkäys.<sup>179</sup> Se perustuu vaikeasti havaittavan, kehittyneen haittaohjelman ujuttamiseen maksupalvelun käyttäjän maksupäätteeseen, kuten tietokoneeseen. Haittaohjelma saattaa olla piilossa huomaamattomana käyttäjän laitteessa jopa useita kuukausia ennen aktivoitumistaan. Aktivoituessaan se menee verkkoasetuksia muuttamalla maksupalvelun käyttäjän ja palveluntarjoajan verkkoyhteyden väliin, ja vaikuttaa siihen, minkälaisena käyttäjä näkee web-sivunsa: haittaohjelma ohjaa käyttäjät verkkorikollisten omille, palveluntarjoajan sivustoa matkiville ja usein myös varsin läheisesti muistuttaville sivuilleen, kun he syöttävät palveluntarjoajan osoitteen selaimensa. Kun käyttäjä luulee olevansa palveluntarjoajan sivustolla, hän tosiasiaa onkin verkkorikollisten sivustolla, jossa hän maksutapahtumia suorittaessaan sitten antaa asiakastunnuksiaan, salasanojaan sekä vahvistustunnuksiaan rikollisille, jotka pääsevät niiden avulla käyttäjien tileille sekä suorittamaan haluamiaan transaktioita. Tilin varat siirretään usein ensin samassa maassa olevalle ”muulille”, joiden kautta ne välitetään eteenpäin, tyyppillisesti ulkomaille esimerkiksi Western Union – palvelun tai muun maksunvälittäjän kautta.

---

<sup>177</sup> Ks. Nordea, 2010<sup>b</sup>. [http://www.nordea.fi/sitemod/upload/Root/fi\\_org/appx/fin/ehdot/MMST960DL.pdf](http://www.nordea.fi/sitemod/upload/Root/fi_org/appx/fin/ehdot/MMST960DL.pdf) Haettu 10.4.2011.

<sup>178</sup> FiCom, 2008. [http://www.ficom.fi/tietoa/tietoa\\_4\\_1.html?id=1156845988.html](http://www.ficom.fi/tietoa/tietoa_4_1.html?id=1156845988.html) Haettu 7.1.2011.

<sup>179</sup> Suomessa Nordean verkkopankki joutui tällaisen hyökkäyksen kohteeksi tammikuussa 2010. Pankin mukaan 15 asiakkaan tileiltä onnistuttiin viemään yhteensä 50 000 euroa. Pankki korvasi menetykset asiakkailleen. Ainakin yhdellä huijatuista asiakkaista oli teleoperaattorilta palveluna ostettu F-Securen Windows-tietoturvaohjelma, joka ei kuitenkaan torjunut haittaohjelmaa ajoissa. Ks. aiheesta esimerkiksi Poliisin tiedote <http://www.poliisi.fi/poliisi/bulletin.nsf/vwSearchView/0F6F31226E1365CEC225778600211F11> sekä Nordean tiedotteet <http://www.nordea.fi/Tietoa+Nordeasta/Nordea+varoittaa+asiakkaitaan+haittaohjelmasta/1285712.html> ja <http://www.nordea.fi/Tietoa+Nordeasta/Haittaohjelman+aiheuttamat+vahingot+korvataan/1285782.html> (Haettu 14.3.2011).

Tilannetta hankaloittaa erityisesti se, että jopa päätelaitteiden suojausohjelmat voivat olla toisinaan voimattomia tällaisten haittaohjelmien kanssa: edes asianmukaisesti päivitetty tietoturvaohjelmat eivät välttämättä aina ole ajan tasalla uusimpien uhkien kanssa, eivätkä näin ollen tunnista ko. haittaohjelmia. EMC:n tietoturveysyksikkö RSA arvioi tammikuussa 2010, että sen hetken tehokkaimman pankkitroijalaisen *Zeus 2*:n tunnisti ko. hetkellä vain 23 prosenttia ajan tasalla olevistakin torjuntaohjelmista. Sama yksikkö arvioi myös, että netissä olisi yli 10 miljoonaa Windows-konetta, jotka olisi saastutettu pankkitroijalaisella.<sup>180</sup> Myös viestintäviraston Cert.fi –yksikössä myönnettiin tämän jälkeen, että pankkihaittaohjelmat jäävät usein torjuntaohjelmilta huomaamatta. Vaikka asiakkaat siis olisivat noudattaneet palveluntarjoajien tietoturvaohjeita, kuten mm. suojanneet päätelaitteensa asianmukaisesti sekä pitäneet tietoturvaohjelmistonsa ajan tasalla, voi vastaavanlainen hyökkäys silti tapahtua. Asiantuntijoiden mukaan suurin riski on yleisimpien ohjelmistojen<sup>181</sup> käyttäjillä.

Kysymys kuuluukin, kenen vastuulla on, jos maksupalvelun tietoturva pettää siitä huolimatta, että kaikki maksupalveluun liittyvät osapuolet ovat lähtökohtaisesti toimineet lain sekä maksu yhteisön ohjeiden edellyttämällä tavalla? Mikä on tällöin esim. tietoturvapalvelun myyjän, sen valmistaneen ohjelmistoyhtiön tai hyökkäyksen kohteena olevan käyttöjärjestelmäyhtiön vastuu vahingoista? Voidaan myös kysyä minkälaisista huolellisuuden tasoa asiakkailta voidaan sopimuksen mukaisesti vaatia: riittääkö, että tietoturvaohjelmistot ovat ajan tasalla, vai vaaditaanko kenties suurempaa, tilannesidonnaista huolellisuutta? Esimerkiksi eräässä kotimaista palveluntarjoajaa kohtaan tapahtuneessa hyökkäyksessä sivusto, johon käyttäjät ohjattiin, muistutti palveluntarjoajan sivustoa, mutta oli ainakin osittain englanninkielinen. Voidaanko tätä pitää jo riittävänä epäilyttävänä merkinä, joka käyttäjän olisi ollut syytä huomata ja osata yhdistää se mahdolliseen tietoturva-uhkaan? Kuinka suuren osan tietoturvallisuusasioista palveluntarjoajat voivat sopimusehtojaan ja tietoturvaohjeistustaan tiukentamalla vierittää maksujärjestelmän käyttäjien vastuulle? Kuitenkin velvoiteoikeudellisten periaatteiden mukaan palveluntarjoajien sopimusperusteista vastuuta voidaan periaatteessa rajoittaa merkittävästikin vahingonkärsijän eli käyttäjän myötävaikutuksen perusteella. Toisaalta huomioon on otettava myös käyttäjien asema

---

<sup>180</sup> Lehto (2010<sup>c</sup>), Tietokone 27.1.2010.

[http://www.tietokone.fi/uutiset/rsa\\_verkkopankkien\\_tietoturvaa\\_voisi\\_parantaa](http://www.tietokone.fi/uutiset/rsa_verkkopankkien_tietoturvaa_voisi_parantaa) Haettu 18.2.2011.

<sup>181</sup> Monissa hyökkäyksissä on suunnattu käyttäjiin, joilla on Internet Explorer-selain, Windows-käyttöjärjestelmä ja Adobe Reader pdf-lukijana. Yhden tai useamman näistä vaihtaminen voi parantaa tietoturvaa, sillä suosituimpiin ohjelmiin hyökätään eniten. (Lehto, 2010<sup>c</sup>) Kuitenkaan, myöskään vaihtoehtoiset järjestelmät yleistyessään riittävästi eivät takaa täyttä turvallisuutta. Siitä ei myöskään voida lähteä liikkeelle, että ihmisten pitäisi vaihtaa käyttöjärjestelmää tai selainta asioidakseen turvallisesti verkkopankissa.



suhteessa palveluntarjoajaan: näin ollen ainakaan kuluttaja-asiakkailta ei voitaisi yleensä vaatia maallikolle asetettavia vaatimuksia korkeampaa havaitsemisvelvollisuutta tietoturvauhkiin liittyen.<sup>182</sup>

Rajanveto asiassa vaikuttaa varsin hankalalta, ja ainakaan vielä näihin kysymyksiin ei ole saatu kannanottoja. Aiemmin mainittujen EPC:n tietoturvakäytäntöjen perusteella palveluntarjoajille lankeaa suuri osa vastuusta ainakin suhteessa käyttäjiin. Ne ovatkin reagoineet kasvaneisiin tietoturvauhkiin: esimerkiksi Nordea aloitti helmikuussa 2010 ylimääräiset tekstiviesti- tai puhelintarkastukset, jos maksutapahtuma on erityisen iso tai muuten poikkeuksellinen.<sup>183</sup> Toistaiseksi kotimaiset pankit ovat korvanneet rikollisten aiheuttamat menetykset asiakkailleen. Toisaalta, korvaussummat ovat jääneet vielä pieniksi - maailmalla pankkien halukkuus korvata vahinkoja on jo vähentynyt tappioiden kasvaessa miljoonaluokkaan. Viranomaisten on Lehdon mukaan linjattava asiaa viimeistään siinä vaiheessa, jos ja kun joku pankki kieltäytyy korvaamasta asiakkailleen menetettyjä varoja.<sup>184</sup>

### 5.1.2.2 Tietojen säilyttämisen turvallisuus ja vastuunjako

Komission tiedonannon mukaan viime vuosina on tehty useita tietomurtoja sähköistä kaupankäyntiä harjoittavien yritysten, luottotietolaitosten ja hallitusten tietokantoihin, joista on viety asiakkaiden luottokorttinumeroita ja muita henkilötietoja. Myös ko. tietomurrot ovat lisänneet mahdollisuuksia maksuvälinepetoksiin, jonka lisäksi tällaisten tapahtumien yhteydessä yksittäisten kauppiaiden maine sekä kuluttajien luottamus internetin turvallisuuteen sekä maksuvälineiden käyttöön sähköisessä ympäristössä heikkenee.<sup>185</sup> Tämä vastaavasti rapauttaa kuluttajien luottamusta myös sähköiseen kaupankäyntiin. Näin ollen sähköisen maksamisen ja koko sähköisen kaupankäynnin kehittymisen kannalta onkin ensiarvoisen tärkeää, että vastuunjako sekä rangaistussäännökset ko. tietomurtojen osalta ovat selkeitä ja edistävät omalta osaltaan tietojen suojaamistavoitteita.

---

<sup>182</sup> Ks. vahingonkärsijän myötävaikutuksesta Saarnilehto – Hemmo – Kartio, 2001, s. 602 - 603.

<sup>183</sup> Lehto (2010<sup>b</sup>), Tietokone 3/2010, s.19.

<sup>184</sup> Lehto, 2010<sup>d</sup>. <http://blogit.tietokone.fi/tietojakoneesta/2010/02/verkkopankkirosvo-vei-rahat-kuka-maksaa/> Haettu 18.2.2011.

<sup>185</sup> KOM (2003)718, Liite 20.

Käyttäjien maksupalveluun liittyvien tietojen säilytyksestä säännellään lähtökohtaisesti tietosuojadirektiivin 17. Artiklassa, joka on implementoitu henkilötietolain 7. Lukuun. Artiklaan sisältyy yleisluonteisia velvollisuuksia, joihin kuuluu mm. sen varmistaminen, että

A) maksupalvelun tarjoajat ja kauppiat, jotka varastoivat tai käsittelevät maksutapahtumiin liittyviä henkilötietoja, noudattavat asianmukaisia teknisiä ja organisatorisia menettelyjä, jotka liittyvät verkon turvallisuuteen ja estävät luvattoman pääsyn kyseisiin tietoihin,

B) maksupalvelun tarjoajat ja kauppiat, jotka ulkoistavat toimintonsa kokonaan tai osittain ulkopuoliselle osapuolelle, tarkastavat tämän turvajärjestelmät ja organisatoriset menettelyt verkon turvallisuuden takaamiseksi.

C) asiakkaille tiedotetaan, jos tietoturvaan kohdistuvat rikkomukset mahdollistavat ulkopuolisten luvattoman pääsyn kyseisiin tietoihin tietoverkkojen kautta,

D) asiakkaille tiedotetaan, etteivät turvallisuusrikkomukset ja niiden mahdolliset seuraukset koidu asiakkaan maksettavaksi.<sup>186</sup>

Kuten direktiivin sanamuodosta käy siis ilmi, maksupalvelun tarjoajat ja kauppiat ovat molemmat lain mukaan vastuussa sekä omien että myös ulkoistamiensa järjestelmien turvallisuudesta ja siitä, että asiakkaille tiedotetaan turvallisuusrikkomuksista ja niiden seuraamusten korvaamisesta.

Näiden henkilötietolain yleisten säännösten lisäksi tietojen säilyttämisestä on myös maksulaitoskohtaisia säännöksiä. Esimerkiksi EPC:n turvallisuusstandardeissa on ohjeita pankeille myös transaktio- ja asiakastietojen pitkäaikaisen säilyttämisen osalta. Tiedon eheyttä tulisi suojella, hyviä keinoja tähän ovat esimerkiksi 1) sen kirjoittaminen pysyväälle alustalle jota voidaan suojata fyysisesti sekä 2) datan suojaaminen laitteisto- ja ohjelmistokeinoilla jotka estävät tiedon muuttamisen. Elektroniset pankkijärjestelmät tulisi standardien mukaan suunnitella siten, että arkaluontoisen datan varastoiminen ja lähettäminen haavoittuviin ympäristöihin pyritään minimoimaan. Lisäksi myös em. PCI-standardit sisältävät ohjeita maksukorttitietojen säilyttämisen osalta. Keskusrikospoliisin raportin mukaan rahanarvoista tietoa sisältävien tietokantojen suojaukset ovatkin PCI-standardin myötä parantuneet olennaisesti.<sup>187</sup>

---

<sup>186</sup> EY/95/46

<sup>187</sup> Keskusrikospoliisi, 2009, s.6.

Euroopan komission teettämän Eurobarometri – tutkimuksen mukaan noin joka toinen kuluttaja on huolissaan henkilötietojensa käsittelyn asianmukaisuudesta sähköisen kaupankäynnin ja palveluiden kohdalla. Tästä huolimatta suomalaisten rekisterinpitäjien asenne tietosuoja ja tietoturva kohtaan on mm. Salmisen mukaan ollut kuitenkin jopa välinpitämätön.<sup>188</sup> Myös Euroopan Komissio on huomionnut tämän kannanotoissaan.<sup>189</sup> Näissä komissio katsoo että kuluttajille ei anneta maksujärjestelmien turvallisuudesta riittävää tietoa, ja säännöksistä huolimatta monista tietomurroista ei edes ilmoiteta poliisille. Yhdistettynä tämänlaisen käyttäytymisen siihen, että tekniikan ja tietojärjestelmien monimutkaisuudesta johtuen maksujärjestelmän käyttäjien on kuitenkin usein vaikeaa todentaa, kuinka turvallinen käytössä oleva maksujärjestelmä oikeastaan on, voidaan katsoa että kuluttajien näkökulmasta tilanne on varsin ongelmallinen.

Vaikka lainsäädännössä rekisterinpitäjiltä ei edellytetäkään täydellistä tietoturvan varmistamista hinnalla millä hyvänsä, vaan ainoastaan riittävää tietoturvan varmistamista kohtuullisin uhrauksin,<sup>190</sup> olisi sähköisen kaupan ja maksamisen kehittymisen kannalta kuitenkin tarpeellista luoda yhtenäiset kriteerit järjestelmien turvallisuudelle. Maksutapojen turvallisuuden kehittymisen pitäisi olla nykyistä vahvemmin myös kaikkien elinkeinonharjoittajien intressissä, sillä järjestelmien tietoturvaongelmat vaikuttavat olennaisesti kuluttajien valintoihin. Tekniset turvallisuusvaatimukset voivat muuttua nopeastikin uusien menetelmien syntyessä, joten lainsäädäntö ei välttämättä kuitenkaan ole paras keino teknisen turvallisuuden lisäämiseksi, vaan turvallisuuden kehittäminen luonnistuu todennäköisesti parhaiten elinkeinonharjoittajien omaehtoisen vastuunoton kautta.<sup>191</sup> Sääntelyviranomaisten tähän saakka noudattama lähestymistapa onkin käsittänyt pääasiassa rikoslainsäädännön muutoksista koskemaan uudentyyppisiä rikoksia ja niihin sovellettavien asianmukaisten rangaistusten määrittelyyn. Komissio tähdentääkin, että itse maksualan infrastruktuurin turvallisuutta koskevien uusien säädösten laatiminen ei ole tarpeen ja muut aloitteet voidaan jättää itsesääntelyn piiriin.<sup>192</sup>

---

<sup>188</sup> Salminen, 2009, s.7.

<sup>189</sup> KOM (2003)718, liite 20 ja KOM (2004)679, kappale 8.

<sup>190</sup> Salminen, 2009, s.82.

<sup>191</sup> Kuluttajavirasto, 2004, s.3.

<sup>192</sup> KOM (2003)718, liite 20h.

## 5.2 MAKSUJEN SUORITTAMISEEN LIITTYVÄT KYSYMYKSET

Toinen tärkeä kokonaisuus sähköisen maksamisen alueella on maksujen suorittaminen ja siihen liittyvät kysymykset. Sähköisessä maksujen suorittamisessa voi tapahtua virheitä, esimerkiksi maksu suoritetaan erehdyksessä väärälle henkilölle tai maksutapahtumassa veloitettu summa on suurempi kuin mitä toinen osapuoli on voinut kohtuudella olettaa sen olevan. Myös käytettävä järjestelmä voi pettää, joko hetkellisesti maksutapahtuman aikana tai pitemmällä aikavälillä, jolloin käyttäjät eivät pääse suorittamaan maksujaan ollenkaan. Joissain tapauksissa myös maksuun liittyvän veloitteen laiminlyönti voi vaikuttaa maksutapahtuman oikeellisuuteen.

### 5.2.1 Virheet maksutapahtumassa tai maksuun liittyvän veloitteen täyttämässä

#### 5.2.1.1 Yksilöivän tunnisteen korostunut merkitys maksutapahtumassa

Yksilöivä tunniste määritellään maksupalvelulaissa ”*palveluntarjoajan maksupalvelun käyttäjälle määrittämäksi kirjain-, numero- tai merkkiyhdistelmäksi, joka maksupalvelun käyttäjän on esitettävä, jotta toinen maksutapahtumaan liittyvä maksupalvelun käyttäjä tai tämän maksutili voidaan yksilöidä.*” Yksilöivää tunnistetta koskevan sääntelyn voidaan katsoa liittyvän erityisesti juuri sähköiseen maksamiseen. Pankkiyhteysmaksuissa tällaisena yksilöivänä tunnisteenä voidaan pitää maksunsaajan tilinumeroa ja esim. PayPalin kautta suoritettavissa maksuissa maksun vastaanottajan sähköpostiosoitetta.

MPL 44§:n mukaan palveluntarjoaja *saa toteuttaa maksutapahtuman tällaisen yksilöivän tunnisteen perusteella, vaikka maksupalvelun käyttäjä olisi antanut sen lisäksi muitakin tietoja maksutapahtuman toteuttamiseksi.* Kyseisen pykälän tarkoituksena on edistää maksujen automatisointia ja sitä kautta myös nopeuttaa maksujenvälitystä.<sup>193</sup> Lain 44§:n säädös yksilöivän tunnisteen priorisoinnista muiden tietojen suhteen merkitsee kuitenkin myös sitä, ettei palveluntarjoajalla ole erityistä velvollisuutta tarkistaa, että yksilöivä tunniste vastaa maksajan antamia muita tietoja. Esimerkiksi jos palveluntarjoaja on määrittänyt yksilöiväksi tunnisteen maksunsaajan tilinumeron, palveluntarjoajalla ei ole maksupalvelulain perusteella velvollisuutta tarkistaa, että kyseinen tilinumero kuuluu juuri maksajan tarkoittamalle maksunsaajalle. Näin on

---

<sup>193</sup> HE 169/2009vp, s.63.

siinäkin tapauksessa, että palveluntarjoaja on itse pyytänyt tietoa maksunsaajan nimestä maksunsaajan tilinumeron lisäksi.<sup>194</sup>

MPL 7. luvussa on säännökset maksajan käynnistämistä, mutta toteuttamatta jääneistä tai virheellisesti toteutetuista maksutapahtumista. Kuten voidaan odottaa, lähtökohtana laissa on että palveluntarjoajat ovat vastuussa virheellisistä sekä toteuttamatta jääneistä maksutapahtumista. Se, onko vastuu maksajan vai maksunsaajan palveluntarjoajalla, määrittyy palveluntarjoajien välisiä maksutapahtuman toteuttamisaikoja koskevien säännösten mukaisesti. Maksupalvelun käyttäjillä on ko. maksutapahtumien osalta pääsäännön mukaisesti ainoastaan ilmoitusvelvollisuus maksutapahtumissa tapahtuneista virheistä sellaisen huomattessaan palveluntarjoajan vastuun realisoimiseksi.

Kuitenkin, tähän pääsääntöön vastuunjaosta on nimenomaisesti yksilöivien tunnisteiden osalta sisällytetty eräs tärkeä poikkeus. Lain 68§:ssa sanotaan, että palveluntarjoajat eivät ole vastuussa toteuttamatta jääneistä tai virheellisistä maksutapahtumista, jos syynä on se, että *maksupalvelun käyttäjän antama yksilöivä tunniste on virheellinen*. Ko. tapauksissa kysymys voi olla esimerkiksi siitä, että maksajan ilmoittama maksunsaajan maksutilin numero on ollut virheellinen ja maksu on tämän vuoksi päätyntä väärän henkilön tilille.<sup>195</sup> Palveluntarjoaja ei ole tällaisessa tapauksessa MPL 64 tai 65 §:n mukaisesti velvollinen palauttamaan maksutapahtuman rahamäärää, 66 §:n mukaisesti jäljittämään maksutapahtumaa eikä 67 §:n mukaisesti velvollinen palauttamaan kuluja tai korvaamaan korkoa. Pykälän 2 momentissa säädetään kuitenkin maksajan palveluntarjoajalle velvollisuus pyrkiä *kohtuullisin toimenpitein* saamaan maksutapahtuman varat takaisin. Momentissa oikeutetaan lisäksi palveluntarjoajaa perimään maksupalvelun käyttäjältä kulut maksutapahtuman varojen takaisin hankkimisesta, jos tällaisesta oikeudesta on puitesopimuksessa sovittu. Perittävien kulujen on oltava asianmukaiset eivätkä ne saa ylittää palveluntarjoajan tosiasiallisia kustannuksia.

Lainkohtaa voidaan pitää ainakin osittain yleisten sopimusperusteisen korvausvastuun periaatteiden mukaisena sikäli kun palveluntarjoaja on saanut maksupalvelun käyttäjältä virheellisen tiedon eli tässä tapauksessa väärän tilinumeron tai vastaavan. Maksumääräyksen antajan virhettä ei ole yleensä tarpeen arvioida myötävaikutusnäkökulmasta, vaan pankin tai muun palveluntarjoajan

---

<sup>194</sup> HE 169/2009vp, s.63.

<sup>195</sup> HE 169/2009vp, s.80.

suoritusta voidaan pitää oikeana sikäli, kun se on maksajan antamien tietojen mukainen, vaikka lopputulos olisikin maksajan kannalta epätydyttävä.<sup>196</sup>

Toisaalta voidaan kuitenkin myös katsoa, että yksilöivän tunnisteiden merkitys maksutapahtuman suorittamisessa suhteessa muihin maksutietoihin on varsin korostunut. Yksilöivän tunnisteeseen liittyvä lainsäädäntö lisää maksupalvelun käyttäjien vastuuta ja vastaavasti vähentää maksupalvelun tarjoajan vastuuta maksun oikeellisesta suorittamisesta. Vaikka laissa on säädetty myös palveluntarjoajan velvollisuudesta pyrkiä saamaan virheellisesti suoritettujen maksutapahtumien varat takaisin kohtuullisin toimenpitein, laki jättää varsin epäselväksi sen, minkälaisia toimenpiteitä palveluntarjoajilta voidaan tosiasiallisesti tilanteissa edellyttää. Lain esitöissä mainitaan ainoastaan, että ”se minkä laatuista ja laajuisia toimenpiteitä palveluntarjoajalta voidaan kohtuudella edellyttää maksutapahtuman varojen takaisinmaksuksi, riippuu olosuhteista, joita ovat esimerkiksi maksutapahtuman rahamäärä ja se onko kyseessä kotimaan maksutapahtuma vai rajat ylittävä maksutapahtuma.”<sup>197</sup> Tästä voi vetää johtopäätöksen, että esim. pienempien tai rajat ylittävien maksutapahtumien osalta palveluntarjoajan velvollisuus varojen takaisin hankkimiseen olisi lainsäätäjän mielestä jotenkin lähtökohtaisesti erilainen. Tätä näkemystä voidaan pitää mielestäni varsin yllättävänä ja jopa niitä maksupalvelunkäyttäjiä syrjivänä, jotka käyttävät ko. maksupalvelua ensisijaisesti pienempiin maksuihin tai vastaavasti rajat ylittävien maksujen suorittamiseen.

#### **5.2.1.1.1 Perusteettoman edun palautus oikeuskeinona virheiden korjaamiseksi**

Virheellisen yksilöivän tunnisteiden käyttö sähköisessä maksutapahtumassa ei sinänsä oikeudellisesti katsottuna johda kuitenkaan vielä siirrettyjen varojen menettämiseen, koska varojen erehdyksellisellä saajalla on yleisten siviilioikeudellisten periaatteiden mukainen *perusteettoman edun palautusvelvollisuus*. Se on kansainvälisesti todettu oikeuskeino, jolla tiettyjen aiheettomien suoritusten vaikutukset voidaan poistaa silloin, kun vaatimusta ei voida perustaa sopimusoikeudellisiin sääntöihin eikä vahingonkorvausnormistoon. Sähköiseen maksamiseen liittyen tyypillinen tilanne minkä yhteydessä oikeuskeinon käyttö voi tulla kysymykseen on siis tilisiirto, jossa maksaja merkitsee maksutoimeksiuntoonsa virheellisen tilinumeron, jonka seurauksena siirrettävät varat päätyvät väärän henkilön tilille. Tilanteessa palautusvelvollisuutta ei voida perustaa sopimusoikeudellisiin sääntöihin, koska maksajan ja suorituksen saajan välillä ei ole sopimussuhdetta, eikä myöskään vahingonkorvausnormistoon, koska varojen saaja ei ole menetellyt

<sup>196</sup> Saarnilehto – Hemmo – Kartio, 2001, s.602.

<sup>197</sup> HE 169/2009vp, s.80.

mitenkään tuottamuksellisesti. Kuitenkin oikeudenmukaisuuden ja kohtuuden vaatimukset näyttäisivät edellyttävän ko. tahattomien varallisuudensiirtymien oikaisemista.<sup>198 199</sup>

Perusteettoman edun palautus on Suomen, kuten usean muunkin valtion oikeudessa vailla yleistä lainsäädäntöä. Kondiktio-opit ovatkin oikeuskäytännössä kehittyneiden sääntöjen ja oikeuskirjallisuuden antaman tuen varassa. Yleensä perusteettoman edun palautuksella on katsottu olevan kolme edellytystä, joiden tulee täytyä ennen kuin palautusvelvollisuus voidaan vahvistaa:

- a) edun saaminen
- b) edun perusteettomuus
- c) hyötymisen tapahtuminen toisen kustannuksella

*Edun saaminen* voidaan objektiivisesti katsoa taloudelliseksi hyödyksi, tässä tilisiirrossa tulleiksi ylimääräisiksi varoiksi. Etu on *perusteeton*, koska sillä ei ole vastasuoritusta. Lisäksi maksunsaaja *hyötyy* tapauksessa maksajan kustannuksella, joten virheellisen tilisiirron voidaan katsoa täyttävän kaikki kolme vaadittavaa kriteeriä. Näiden edellytysten täytyminen riittää palautusvelvollisuuden syntymiseen, ilman erityistä erehdystä tai virhettä koskevaa selvitystä. Myöskään tuottamuksen osoittaminen ei ole tarpeen, ja palautus voikin tulla sovellettavaksi myös niissä tapauksissa, joissa edun saaja on menetellyt moitteettomasti.<sup>200</sup> Tappion kärsijä voi yleisten palautusoppien mukaisesti siis vaatia menettämänsä varallisuutta takaisin, vaikka menetyksen syynä olisi ollut puhtaasti ainoastaan hänen oma huolimattomuutensa. On myös esitetty, että teoriassa jopa harkitusti ja tarkoituksellisesti tehdyt perusteettomat suoritukset tulisi palauttaa, mikäli vain em. yleiset edellytykset täyttyvät.<sup>201</sup>

Jos palveluntarjoajan aiemmin mainitut takaisinsaantitoimenpiteet eivät siis johda tulokseen, maksupalvelun käyttäjän oikeuskeinona on virheellisen yksilöivän tunnisteiden sisältävissä maksuissa perusteettoman edun palautus. Kuitenkin käytännössä ko. oikeuskeinon käyttäminen on varsin

---

<sup>198</sup> Aurejärvi – Hemmo, 2007, s.152.

<sup>199</sup> Yhtenäisen ja johdonmukaisen säännösten luominen aiheettomien maksusuoritusten oikaisemiseen on kuitenkin ollut työlästä. Yleisesti ko. tilanteiden hahmotus ja korjausten toteutustavat ovatkin vaihdelleet eri maiden välillä huomattavasti: Vaikka Suomen ohella usean muunkin valtion oikeudessa oikeuskonstruktiona käytetään perusteettoman edun palautusta, esimerkiksi angloamerikkalaisissa maissa kondiktio-opin sijasta on käytetty lähinnä fiktiivistä sopimusmenettelyä ja pohjoismaissa ko. tapauksissa on pikemminkin pyritty laajentamaan vahingonkorvauksen käyttöalaa. (Aurejärvi – Hemmo, 2007, s.152 - 154.)

<sup>200</sup> Hemmo, 2007, s.99 - 102.

<sup>201</sup> Aurejärvi – Hemmo, 2007, s.173.

monimutkaista. Se edellyttää kanteen nostamista virheen oikaisemiseksi, johon liittyy sekä suoria että epäsuoria kustannuksia. Lisäksi velvoiteoikeudellisten periaatteiden mukaisesti myös perusteettomuuden todistaminen kuuluu pääsääntöisesti suorituksen palauttamista vaativalle kondiktiovelkojalle: ellei riittävää näyttöä suorituksen aiheettomuudesta pystytä esittämään, asianosaisten väliset varallisuussuhteet jätetään ennalleen.<sup>202</sup>

Esimerkiksi tietosuojavaltuutetun toimisto katsoo, että kyseiset oikeudenkäytön kustannukset voivat olennaisesti nostaa kynnyistä tällaisen viimekätisen oikeusturvatie käyttööseen. Sen mielestä tarvittaisiinkin mutkattomampi oikeusturvakeino varojen takaisin saamiseksi, jonka lisäksi tulisi myös kiinnittää huomiota palveluntarjoajan ennaltaehkäiseviin toimiin joilla käyttäjä voisi havaita omat kirjoitusvirheensä.<sup>203</sup> Tietosuojavaltuutetun toimisto huomauttaa myös, että toisaalta henkilötietolain näkökulmasta kyse on rekisterinpitäjän vastuusta huolehtia tietojen oikeellisuudesta.<sup>204</sup> Kuitenkaan, koska maksupalvelulaissa tällaista vastuuta ei nimenomaisesti ole mainittu, voidaan katsoa lakien antavan jopa ristiriitaisen tulkinnan oikeudentilasta ja siitä, mihin palveluntarjoajan vastuu tilanteessa rajoittuu. Lisäksi on syytä kysyä, onko perusteltua, että yksilöivälle tunnisteelle on annettu aiemmin selvitetyn korostunut merkitys suhteessa muihin maksusta annettaviin tietoihin, jos kuitenkin kondiktion käyttö oikeusturvakeinona on virheen sattuessa em. monimutkaista?

Näkökulmaa asiaan voidaan hakea kansainväliseltä alueelta. Esimerkiksi myös Australiassa on käytössä luottolaitosten välinen sähköinen maksujärjestelmä, jossa on mahdollista suorittaa rahansiirtoja eri luottolaitosten asiakkaina olevien järjestelmän käyttäjien välillä. Vastaavasti kuin täällä, huolimatta siitä että järjestelmät hyväksyvät sekä vastaanottajan nimen että tilinumeron, varojen siirto tapahtuu myös ko. järjestelmässä tehokkuussyistä pelkästään tilin numeron perusteella.<sup>205</sup> Myös siellä vastuu on perinteisesti jakautunut virheellisesti syötettyjen maksutapahtumien osalta siten, että maksupalvelun käyttäjä vastaa omista virheistään maksujen syöttämisessä ja maksujen palautuksessa joudutaan turvautumaan kondiktio-oppeihin.

---

<sup>202</sup> Aurejärvi – Hemmo, 2007, s.168. Toisaalta, tekijöiden mukaan myös vastaajan täytynee kyetä kysyttäessä jotenkin selittämään, millä perusteella hän on oikeutettu saamaan ko. suorituksen.

<sup>203</sup> Gauriloff, 2009, s.40.

<sup>204</sup> Gauriloff, 2009, s.39 - 40.

<sup>205</sup> Tyree, 2003, s.1.



Menettelyn hankaluus kuluttajien kannalta on kuitenkin herättänyt keskustelua<sup>206</sup>, ja syyskuussa 2008 Australian Securities and Investments Commission (ASIC), joka hallinnoi sähköisten varojen siirtokoodia (EFT), julkaisi konsultaatiopaperin jossa se otti kantaa virheellisesti tehtyjen rahansiirtojen kysymykseen. Toimielin myösi lausunnossaan, että käytännössä nykyisten kondiktiosäännösten nojalla kuluttajien on erittäin vaikeaa saada virheellisesti tehdyn suorituksen varoja takaisin, koska a) virheen tehnyt taho ei yleensä tiedä kenelle varat on maksettu, ja b) virheellisen maksunsaajan maksupalvelun tarjoaja ei usein suostu paljastamaan tätä tietoa luottamuksellisuussyihin vedoten. Lisäksi suuressa osassa ko. tapauksia oikeudenkäyntikulut ovat suurempia kuin menetetty rahamäärä, joten käytettävissä olevan oikeuskeinon käyttö voi osoittautua kannattamattomaksi maksupalvelun käyttäjille.<sup>207</sup>

Mainittiin myös, että virheellisiä sähköisiä maksuja elektronisissa järjestelmissä tapahtuu kahdesta syystä: joko kuluttajat tekevät näppäilyvirheen syöttäessään vastaanottajan tilinumeroa, tai kuluttaja on saanut virheellisen tilinumeron maksun tarkoitettulta vastaanottajalta. ASIC: in kannanoton mukaan perusteettoman edun palautusta voidaan soveltaa ainakin silloin, kun virhe johtuu näppäilyvirheestä. Virheellisen tiedon saamisen tapauksessa oikeuskeinon soveltamisesta ei ole toimielimen mukaan kuitenkaan edes täyttä varmuutta.<sup>208</sup> Tyree kuitenkin perustelee kannanotossaan konsultaatiopaperista, että myös tällaisissa tapauksissa käyttäjillä olisi oikeuskäytännön perusteella oikeus palautukseen.

Joka tapauksessa, myös ASIC katsoi, että prioriteettina asiassa olisi tarjota kuluttajille tehokas järjestelmä virheellisten rahansiirtojen takaisinsaamiseksi syystä riippumatta. Tämä edellyttäisi toisaalta sitä, että järjestelmiä parannettaisiin siten että virheen tekemisen mahdollisuus pienenesi ja toisaalta myös sitä, että kuluttajat joille kuitenkin sattuisi ko. virheitä voisivat saada rahansa takaisin ilman tarvetta käynnistää oikeusprosessia ei-tarkoitettua vastaanottajaa kohtaan.<sup>209</sup> Kuitenkin, siirtokoodin mahdollisesta muuttamisesta nousi myös huolia asianosaisten keskuudessa. Katsottiin, että se voi johtaa uusien juridisten oikeuksien syntymiseen, väärinkäytösten ja huolimattomuuden lisääntymiseen sekä kustannusten kasvuun.<sup>210</sup>

---

<sup>206</sup> mm. Tyree, 2003.

<sup>207</sup> ASIC, 2008, s.49.

<sup>208</sup> ASIC, 2008, s.48.

<sup>209</sup> ASIC, 2008, s.48.

<sup>210</sup> ASIC, 2008, s.49 - 50.

Siis myöskään ko. maan oikeusjärjestelmässä palveluntarjoajia ei ole juridisesti asetettu maksupalvelulakia tiukempaan vastuuseen virheellisten maksujen osalta. Näyttäisi kuitenkin siltä, että ainakin mutkattomammalle oikeusturvakeinolle tai järjestelmäratkaisulle olisi kuitenkin selkeästi tilaus virheellisten maksusuoritusten palauttamisprosessin helpottamiseksi. Perusteettoman edun palautus on oikeuskeinona kuitenkin nimenomaan toissijainen, väistytävä instituutio, jota voidaan oikeusjärjestyksessä pitää lähinnä täydentävänä oikeusturvakeinona, mikäli tilanteessa ei voida nojata muihin varallisuussiirtojen korjauskeinoihin.<sup>211</sup> Vaikka maksupalvelulain 68§:n mukaisesti palveluntarjoajilla ei ole nimenomaista vastuuta virheellisen yksilöivän tunnisteiden seurauksena toteutetuista virheellisistä rahansiirroista, tulisi heidän kuitenkin lähtökohtaisesti olla vastuussa ainakin siitä, että maksamisessa toteutetut järjestelmäratkaisut minimoisivat käyttäjien virheiden tekemisen mahdollisuuden. Tätä on peräänkuuluttanut myös mm. Oikeusministeriön Maksupalvelut-työryhmä lausunnossaan, jonka mukaan palveluntarjoajilta edellytettävään huolelliseen toimintaan voidaan katsoa kuuluvan esimerkiksi sen, että ne ylläpitävät sellaisia järjestelyjä, ”*joiden avulla voidaan pyrkiä vähentämään virheiden syntymistä*”.<sup>212</sup> Tarkentava kannanotto asiaan myös lainsäätäjän taholta olisi mielestäni toivottavaa.

Asiaa tarkastellessa on lisäksi syytä huomioida se, että maksuissa tapahtuvilla virheillä saattaa olla merkittävä vaikutus myös varsinaiseen maksun taustalla olevaan perussuhteeseen: virheellisen suorituksen tehnyt maksaja voi elää pitkäänkin siinä uskossa, että hän on suorittanut maksun täysin oikeellisesti tarkoittamalleen henkilölle. Ko. perussuhteen osalta niin viemävelkaperiaatteen kuin oikeuskäytännönkin<sup>213</sup> mukaisesti vaara maksun viivästyisestä tai katoamisesta on *sillä, joka on syyllinen viivästykseen*. Näin ollen sikäli kun velallisen eli maksajan antamat maksutiedot ovat erheelliset, viemävelkaperiaatteen mukaisesti riski maksun viivästyisestä tai katoamisesta ja sen seurauksista on myös maksajalla. Mikäli taas velkoja on antanut maksajalle erheelliset maksutiedot, voidaan katsoa että velkojan myötävaikutus suorituksen puuttumiseen on niin merkittävä, että perussiviilioikeudellisten periaatteiden mukaan on puolestaan hän lähtökohtaisesti vastuussa maksun viivästyisestä tai suorittamatta jäämisestä: sopimuksen edellyttämän suorituksen puuttumista ei pidetä ko. tapauksissa lainkaan velallisen eli maksajan sopimusrikkomuksena, vaan velallinen on saattanut velkojan laiminlyönnin vuoksi esimerkiksi saada lisäaikaa suoritukselleen tai peräti vapautua kokonaan velvoitteestaan.<sup>214</sup> Perussuhteen osalta molemmat osapuolet vastaavat

---

<sup>211</sup> Aurejärvi – Hemmo, 2007, s.210.

<sup>212</sup> Oikeusministeriö, 2008, s.31.

<sup>213</sup> Ks. esim. KKO 1994:80

<sup>214</sup> Saarnilehto – Hemmo – Kartio, 2001, s.602.

itse myös rahalaitostensa virheistä: jos maksun perille menemättä jääminen johtuu vastakkaisen osapuolen rahalaitoksesta, tämä katsotaan kuuluvan maksun vastaanottajan vastuualueelle. Näin ollen voidaankin puhua ns. modifioidun viemävelkaperiaatteen olemassaolosta.

### 5.2.1.2 Velkoja-aloitteisten maksujen erityinen palautusoikeus

Eräissä tilanteissa maksunpalautukseen on kuitenkin annettu maksupalvelulaissa selkeä juridinen oikeus: uusi maksupalvelulaki sallii maksajalle tietyin ehdoin suoraveloituksen tai muun vastaavan *maksunsaajan* käynnistämisen maksutapahtuman peruutuksen ja maksun palautuksen. MPL 79§ mukaisesti maksajan palveluntarjoajan on maksajan pyynnöstä palautettava maksutapahtuman rahamäärä hänelle kokonaisuudessaan, jos seuraavat edellytykset täyttyvät:

- 1) Maksutapahtuman rahamäärä ei ilmene täsmällisesti maksajan antamassa suostumuksessa
- 2) Maksutapahtuman rahamäärä on suurempi kuin maksaja on *kohtuudella voinut odottaa* ottaen huomioon hänen aikaisempi kulutuskäyttäytymisensä, puitesopimuksen ehdot sekä muut olosuhteet.

Hallituksen esityksen mukaan em. edellytysten täyttymistä arvioidaan objektiivisesti sekä tapauskohtaisesti. Kyseiset edellytykset täyttävästä sähköisestä maksutapahtumasta voidaan antaa esimerkkinä tilanne, jossa maksupalvelun käyttäjä on antanut suoraveloitusvaltakirjan, joka koskee tulevien sähkölaskujen veloittamista hänen maksutililtään, mutta lopullisten veloitusten määrä poikkeaa huomattavasti siitä, mitä maksaja on voinut kohtuudella olettaa.<sup>215</sup>

Maksajan on pyydettävä maksupalautusta palveluntarjoajalta kahdeksan viikon kuluessa maksutapahtuman rahamäärän veloittamisesta. Puitesopimuksessa voidaan kuitenkin sopia, että maksupalautusoikeutta ei ole, jos maksaja on antanut suostumuksensa suoraveloituksesta palveluntarjoajalleen ja palveluntarjoaja tai maksunsaaja on ilmoittanut maksajalle veloittamisesta ennakkoon, vähintään neljä viikkoa ennen eräpäivää. Tällöin oletettavasti katsotaan, että maksajalla on riittävästi aikaa peruuttaa suostumuksensa veloitukseen. Korttimaksujen osalta samanlaista mahdollisuutta sopimiseen ei ole. Jos ennakoilmoitus on saapunut maksajalle myöhemmin kuin neljä viikkoa ennen eräpäivää, voidaan katsoa että palautusoikeus on voimassa.

---

<sup>215</sup> HE 169/2009, s.86.

Säännös on ongelmallinen siltä osin, että se jättää varsin tulkinnanvaraiseksi sen, mitä tulee sen sanamuodon vaatimusten mukaisesti pitää ”suurempana kuin maksaja on kohtuudella voinut olettaa”. Se on myös sikäli mielenkiintoinen, että ko. maksunpalautus ei koske pelkästään liikaveloitettua summaa, vaan *koko maksutapahtuman rahamäärää*. Lainkohdassa ei oteta kantaa siihen, miten asianmukainen suoritus maksajan ja maksun vastaanottajan välillä jälkikäteen määritetään. Lain esitöissä on kuitenkin mainittu, että kysymykset maksajan velvollisuudesta suorittaa asianmukainen vastikkeen määrä taikka maksajan oikeudesta peruuttaa tai purkaa kauppa ratkaistaan erikseen asianomaiseen sopimussuhteeseen sovellettavien säännösten ja sopimusoikeudellisten periaatteiden nojalla.<sup>216</sup> Lisäksi mainitaan ettei säännös merkitse sitä, että palautuksen rahamäärän tulisi jäädä lopullisesti palveluntarjoajan tappioksi vaan palveluntarjoaja voi esimerkiksi sopimusjärjestelyin turvata sen, että se voi vaatia palauttamaansa rahamäärää maksunsaajan palveluntarjoajan välityksin maksunsaajalta.<sup>217</sup>

Velvoiteoikeudellisesta näkökulmasta ko. velvoitteita, joissa osapuolten välisiä suhteita ei ole yksilöity täsmällisesti vaan kauppa on jätetty ns. avoimeksi, kutsutaan täydentämisenvaraisiksi velvoitteiksi. Ongelmallista ko. tapauksissa on, kenelle ja missä rajoissa maksujen täydentäminen kuuluu. Jotta sopimuksen täydentäminen olisi mahdollista, osapuolten on tullut sopia ns. olennaisista ainesosista, joiden osana ainakin toisen osapuolen pääsuoritusvelvollisuus on tullut täsmentää riittävän tarkasti. Jos näin ei ole, katsotaan että osapuolia velvoittavaa sopimusta ei ole syntynyt. Tätä voidaan pitää osaltaan perusteluna sille, että maksupalautus koskee koko veloitettua summaa tapauksissa, joissa osapuolet ovat erimielisiä varsinaisen pääsuoritusvelvollisuuden, eli maksetun suoraveloituksen tai vastaavasti saadun hyödykkeen suhteen.<sup>218</sup>

Kyseinen palautusoikeus suoraveloitusten osalta parantaa kuitenkin huomattavasti kuluttajan asemaa ko. maksutapahtumissa. Sen ensisijainen tarkoitus on oletettavasti ollut suojata kuluttajia tilin liikaveloitustilanteissa. Kuitenkin jo maksupalvelulain esitöissä ilmeni elinkeinonharjoittajien taholta huolia säännökseen liittyen: arvioitiin, että kyseinen säännös olisi maksajien kannalta liian edullinen ja tulisi johtamaan herkästi palautusvaatimusten tekemiseen ja siten myös siihen, että kuluttajien palautusvaatimukset suoraveloitusten osalta tulisivat lisääntymään huomattavasti. Tämä vastaavasti tulisi kasvattamaan palveluntarjoajien kustannuksia, ja todennäköisesti epävarmuus

---

<sup>216</sup> HE 169/2009, s.86 - 87.

<sup>217</sup> HE 169/2009, s.86 - 87.

<sup>218</sup> Aurejärvi – Hemmo, 2007, s.14.

velkoja-aloitteisten maksujen käytön alueella lisääntyisi. Säännös voi pahimmillaan johtaa siihen, että joidenkin ko. tyyppisten maksujen käytöstä tultaisiin luopumaan. Tämä ei varmaankaan ole ollut lainsäätäjän tarkoituksena.

### **5.2.1.3 Kuluttajan ja kauppiaan väliset sopimuskiistat: maksutapakohtaiset eroavaisuudet yhteisvastuun osalta myyjää tai palveluksen suorittajaa kohtaan**

EU:n lainsäädännössä ei ole ollut erityisiä säännöksiä maksupalvelun tarjoajan roolista kuluttajan ja kauppiaan välisissä sopimuskiistoissa. Tämä pätee sekä myyntipisteissä tehtäviin kauppoihin että etäkauppoihin.<sup>219</sup> Kuitenkin kotimaan lainsäädännöstä tällainen säännös löytyy: kuluttajansuojalaissa on säädetty erikseen luotonantajan ja myyjän yhteisvastuusta maksutapahtumien osalta, joissa niihin liittyvä kauppa ei toteudukaan niin kuin on alun perin suunniteltu. KSL 7.39§:n mukaan kuluttajalla, jolla on oikeus pidäytyä maksusta taikka saada hinnan palautusta, vahingonkorvausta tai muu rahasuoritus myyjältä tai palveluksen suorittajalta tämän sopimusrikkomuksen johdosta, on tämä oikeus myös sitä luotonantajaa kohtaan, joka on rahoittanut kaupan tai palveluksen. Momentissa mainitaan lisäksi, että luotonantaja ei ole kuitenkaan velvollinen maksamaan kuluttajalle enempää kuin on tältä saanut maksuina.<sup>220</sup>

Esimerkkinä tästä tapaus KKO 2007:6, jossa kuluttaja oli maksanut Yhdysvalloista hankkimiaan kulutushyödykkeitä luottokunnan myöntämällä Visa-kortilla, mutta myyjä ei huomautuksista ja tiedusteluista huolimatta ollut toimittanut ostettuja tuotteita. Tapaus meni korkeimpaan oikeuteen, joka antoi päätöksen jonka mukaan Luottokunta oli silloisen KSL 7.13§:n<sup>221</sup> 1.momentin nojalla vastuussa myyjän sopimusrikkomuksesta. Luottokunta veloitettiin palauttamaan kuluttajalle hänen maksamansa kauppahintaa vastaava rahamäärä.<sup>222</sup> Riskin myyjän toiminnasta kantaa siis osittain myös kortinmyöntäjä. Kyseistä menettelyä voidaan pitää varsin oikeudenmukaisena, koska palveluntarjoajilla on viime kädessä paremmat edellytykset valvoa myyjiä asiakkainaan.

---

<sup>219</sup> MARKT/208/2001, s.27.

<sup>220</sup> Maksupalvelulain myötä tätä säännöstä on lisäksi tarkennettu seuraavasti: ”Jos myyjä ottaa tavaran takaisin tai jos kauppa muutoin puretaan myyjän ja kuluttajan välisin sopimuksin, kuluttaja voi vedota takaisinotosta toimitettuun tilitykseen tai kaupan purkuun myös kaupan rahoittanutta luotonantajaa kohtaan. Kuluttajalla ei kuitenkaan ole tällaista oikeutta, jos: 1) luotonantaja on ajoissa selkeällä tavalla ilmoittanut kuluttajalle, ettei myyjällä ole takaisinotto-oikeutta tai muuta oikeutta määrätä sopimuksesta ja, jos kaupan kohteena on lain mukaan rekisteröitävä tavara, rekisteriin on merkitty omistajaksi luotonantaja; tai 2) luotonantaja voi muutoin osoittaa kuluttajan tienneen myyjän oikeuksien rajoittamisesta.”

<sup>221</sup> Nyttemmin KSL 7.39§

<sup>222</sup> KKO 2007:6

Tämäntyyppinen yhteisvastuu ulottuu kuitenkin ainoastaan luottoon pohjautuviin palveluihin. Muilla sähköisillä maksutavoilla, kuten tilisiirrolla tai sähköisellä rahalla maksettaessa ko. yhteisvastuuta ei palveluntarjoajilla ole. Hallituksen esityksessä maksupalvelulaista 169/2009 tarkennetaan nimenomaisesti, että ”maksutoimeksiantojen perustana olevaan oikeussuhteeseen liittyvät erimielisyydet ratkaistaan erikseen maksajan ja maksunsaajan välillä. Jos esimerkiksi kauppa puretaan sen jälkeen, kun kauppahinnan suorittamista koskeva maksutoimeksianto on tullut peruuttamattomaksi, kauppahinnan palauttamiseksi ostajalle tarvitaan uusi, alkuperäiseen maksutapahtumaan nähden käänteinen maksutapahtuma.” Useimmiten palveluntarjoajat ovat myös tähdentäneet palvelua koskevissa sopimuksissaan, että he eivät vastaa muiden palveluntarjoajien toiminnasta, palveluista tai tuotteista.<sup>223</sup>

Tuotteita tai palveluita kansainvälisistä verkkokaupoista ostettaessa tämänlaisen sääntelyn alla voidaan katsoa, että ko. sääntely ohjaa maksuvälineiden käyttöä varsin merkittävästi. Koska maantieteelliset välimatkat toisiaan tuntemattomien ostajan ja myyjän välillä voivat olla suuriakin, erityisesti ongelmatilanteissa ostajien pääseminen yhteyteen sekä mahdollinen reklamointi esim. maksusuorituksen taustalla olevan tavaran tai palvelun virheeseen liittyen voi käytännössä osoittautua varsin hankalaksi. Näin ollen ostajalla onkin huomattavasti suurempi riski käyttää maksun suorittamisessa esim. tilisiirtoa kuin luottoon perustuvaa maksutapaa palveluntarjoajien hyvitysvelvollisuuden erilaisuudesta johtuen. Voidaan kysyä, onko perusteltua, että säännös ei ole maksuvälineeneutraali ja edesauttaako luottokortin muita maksumuotoja edullisempi asema sen suosiota sähköisessä maksamisessa?

Mm. komission tiedonannossa on katsottu, että muulla kuin käteisrahalla maksetun tuotteen tai palvelun jäädessä toimittamatta maksupalvelun tarjoajalla tulisi olla vastuu maksuvälinettä käyttänyttä asiakasta kohtaan.<sup>224</sup> Palveluntarjoajan hyvitysvelvollisuutta asiakkaan ja kauppiaan välisissä kiistoissa on pohdittu myös Euroopan komission valmisteluasiakirjassa ”Sisämarkkinoiden yhtenäisen maksualueen mahdolliset sääntelypuitteet”. Sen mukaan olisi varmistettava, että kaikkia käteisrahan ulkopuolisia maksuvälineitä kohdellaan mahdollisimman tasapuolisesti. Sääntelyn kannalta on tärkeää, että oikeudelliset puitteet eivät aseta maksuvälineitä eriarvoiseen asemaan. Kuluttajan pitäisi saada yhtä hyvä suoja riippumatta siitä, maksaako hän luotolla vai jollain muulla

---

<sup>223</sup> Ks. esimerkiksi Nordea, 2010<sup>b</sup> tai APE- sähkörahasovelluksen yleiset käyttöehdot osoitteessa <https://www.apepayment.com/faq/ehdot>

<sup>224</sup> KOM (2001)66, s.17.

käteisrahan ulkopuolisella maksuvälineellä.<sup>225</sup> Myös kuluttajavirasto on huomionnut ko. epäkohdan: se on todennut lausunnossaan, että luottokortittomat kuluttajat ovat huonommassa asemassa kuin luottokortin omaavat kuluttajat, jotka voivat käyttää chargeback- järjestelmiä ja katsoi, että tällainen epätasapaino saattaa maksujärjestelmät eriarvoiseen asemaan. Yhteisvastuun tulisikin myös kuluttajaviraston kannanoton mukaan kattaa tasapuolisesti kaikki maksutavat.<sup>226</sup> Näistä näkemyksistä huolimatta uuteen sisämarkkinalainsäädäntöön ei ole otettu säännöksiä, joilla otettaisiin kantaa tähän eriarvoisuuteen. Toisaalta, maksupalvelun tarjoaja ei yleensä voi kuitenkaan vaikuttaa siihen, lähettääkö kauppias tuotteen vai ei. Näin ollen sellaisten maksujen osalta, joissa palveluntarjoajalla ei ole erillistä sopimusta kauppiaan kanssa, olisikin toisaalta mielestäni varsin kohtuutonta asettaa maksupalvelun tarjoajia edes toissijaiseen vastuuseen.

Tietyt tahot ovat ehdottaneet ratkaisuksi ongelmaan eräänlaista maksun viivyttämismenettelyä: esimerkiksi valmisteluasiakirjassa yhtenä vaihtoehtona on esitetty kaikkiin sähköisen kaupan maksutapoihin tasapuolista järjestelyä, jossa maksunvälittäjä ei välitä maksua lopullisesti saajalle ennen kuin kuluttaja on varmistunut tuotteen sopimuksenmukaisuudesta.<sup>227</sup> Myös kuluttajaviraston kannanoton<sup>228</sup> mukaan ”perusteltu ratkaisumalli voisi olla se, että maksu odottaa välittäjällä, kunnes maksunvälittäjä saa tiedon tavaran sopimuksenmukaisuudesta tai lähettamisestä/saapumisesta kuluttajalle. ” Maksupalvelulain 5. Luvun maksutapahtuman toteuttamisaikaa koskevat säännökset estävät kuitenkin tämän tyyppisen järjestelyn käyttämisen, joten eriarvoisuus maksutapojen välillä näyttäisi säilyvän ennallaan.

### 5.2.2 Tekniset ongelmatilanteet

Sähköisten maksujärjestelmien tekniset ongelmat ovat usein nousseet esiin keskustelussa sähköisten maksujärjestelmien luotettavuudesta. Yksi erityisalue vastuunjaon kannalta on maksuverkko ja sen tekniset häiriöt. Ensinnäkin, maksuinfrastruktuurin toimintojen keskeytykset kuten televiestintäyhteyden tai tietokoneen käsittelykyvyn väliaikainen katkeaminen voivat aiheuttaa riskialttiita tilanteita, joissa joudutaan pohtimaan vastuukysymyksiä. Jos taas koko maksuverkko

---

<sup>225</sup> MARKT/208/2001, s.29.

<sup>226</sup> Kuluttajavirasto, 2004, s.4.

<sup>227</sup> MARKT/208/2001, s.28

<sup>228</sup> Kuluttajavirasto, 2004, s.4.

pettää, käyttäjät eivät pääse käyttämään tilejään eivätkä suorittamaan maksuja tai muitakaan transaktioita.<sup>229</sup>

Niin maksupalvelujen käyttäjät kuin tarjoajatkin ovat alttiita maksuverkon teknisille häiriöille.<sup>230</sup> Sähköisessä kaupassa ja maksuliikenteessä tietoliikenteen merkitys korostuu fyysisiin maksutapahtumiin verrattuna. Tietoliikenneyhteyksien toiminnan virheistä voi aiheutua useita erilaisia seuraamuksia osapuolille, kuten pääsy maksuvälineeseen tai maksun suorittaminen voi estyä, maksutoimeksiantoon voi tulla virhe, maksun välitys viivästyy, tieto suorituksesta viivästyy tai maksutapahtuman turvallisuus vaarantuu.<sup>231</sup> Näissä tilanteissa voi usein olla vaikeaa osoittaa mitä seuraamuksia maksupalvelun käyttäjille on aiheutunut. Yleisesti voidaan todeta, että viestin lähettäjällä on riski viestin perillemenosta ja vastaanottajalla viestiin sisältyvän tahdonilmaisun sisällön mahdollisista muutoksista. Käytännössä maksuliikepalveluihin liittyvät sopimusehdot kuitenkin sisältävät usein osapuolten vastuunjakoon vaikuttavia nimenomaisia ehtoja.

### **5.2.2.1 Yhteyden katkeaminen / tilapäinen maksuverkon pettäminen**

Maksupalvelulaissa on määritelty vastuusta tilanteissa, jossa maksajan tai maksunsaajan *jo käynnistämä* maksutapahtuma on jäänyt toteutumatta tai se on toteutettu virheellisesti. Tähän kategoriaan voidaan lukea siis ainoastaan ne tilanteet, joissa virhe on tapahtunut maksutoimeksiannon antamisen *jälkeen*. Vastuu maksutapahtumien virheistä näissä tilanteissa kohdistetaan MPL 7. Luvussa palveluntarjoajille: niiden on palautettava maksajan/maksunsaajan tili siihen tilaan, joissa se olisi ollut ilman veloitusta, tai vastaavasti osoitettava että maksu on välitetty määräajan puitteissa virheestä huolimatta. Lisäksi palveluntarjoajien on maksualoitteen suorittajan pyynnöstä ryhdyttävä välittömästi jäljittämään maksutapahtumaa. Palveluntarjoajat ovat myös velvollisia palauttamaan mahdolliset kulut, jota maksutapahtumista on peritty sekä korvaamaan mahdollisen koron, jonka maksupalvelun käyttäjä joutuu suorittamaan tai joka häneltä jää saamatta maksutapahtuman toteuttamatta jäämisen tai virheellisen toteuttamisen vuoksi.

Toisaalta, välillisten vahinkojen osalta maksupalvelulaki ei ole näin ehdoton. MPL 69§ mukaan maksupalvelun käyttäjälle aiheutuneen välillisen vahingon, kuten esim. tulon menetyksen tai

---

<sup>229</sup> KOM (2003)718, liite 21.

<sup>230</sup> KOM (2003)718, liite 21.

<sup>231</sup> Terämaa, 2001, s.291.



sopimusvelvoitteen laiminlyönnin, palveluntarjoaja on velvollinen korvaamaan *vain*, jos vahinko johtuu *huolimattomuudesta* palveluntarjoajan puolella. Lisäksi mainitaan, että vastuu välillisistä vahingoista voidaan sopimuksella sulkea pois tai sitä voidaan rajoittaa sikäli, kun vahinkoa ei ole aiheutettu tahallisesti tai törkeästä huolimattomuudesta palveluntarjoajan, tai jonkun jonka menettelystä se vastaa, puolesta.

Vastuuta virhetilanteissa palveluntarjoajalle ei lain mukaan synny myöskään välittömien vahinkojen osalta, mikäli palveluntarjoaja voi osoittaa, että sille kuuluvan velvoitteen täyttämisen on estänyt sellainen epätavallinen ja ennalta-arvaamaton syy, ns. *ylivoimainen este*, johon se ei ole voinut vaikuttaa ja jonka seurauksia se ei kaikkea huolellisuutta noudattaen olisi voinut välttää. Hallituksen esityksessä tarkennetaan, että ylivoimaisen esteen on nimenomaisesti oltava siihen vetoavan tahon vaikutuspiirin ulkopuolella.<sup>232</sup> Tällaisia esteitä ovat esityksen mukaisesti mm. yleisen tietoliikenteen tai sähkönjakelun keskeytykset ja muut vastaavan kaltaiset seikat.<sup>233</sup> Toisaalta sanamuotonsa mukaisesti ylivoimainen este tarkoittaa nimenomaan *ylivoimaista* tapahtumaa, jota ei ”voi voittaa”: esimerkiksi Saarnilehto et al. ovat kannanotossaan sitä mieltä, että esim. lyhytaikaista tietoyhteyksien katkosta sen syystä riippumatta ei voitaisi pitää ylivoimaisena esteenä, vaan niitä käyttävien eli tässä tapauksessa palveluntarjoajien tulisi olla varautunut ko. tapahtumien varalle.<sup>234</sup> Ylivoimaisen esteen käsitettä voidaan pitää oikeustieteessä sen verran epäselvänä, että palvelusta solmittavaan sopimukseen onkin yleensä syytä ottaa lisäksi ehto siitä, mitä käsitteellä juuri nimenomaisessa sopimussuhteessa tarkoitetaan.<sup>235</sup>

Myös oikeuskäytännössä on arvioitu sitä, mitä voidaan pitää em. *force majeure* – tyyppisinä tekijöinä, joilla pystytään rajoittamaan palveluntarjoajien vastuuta. Tästä esimerkkinä tapaus KKO 1989:98, jossa luottokorttiyhteisön jäsenyritys oli kieltäytynyt hyväksymästä asiakkaan luottokorttia maksuvälineenä, koska yritys tietoliikenteessä selvittämättömästä syystä sattuneen tilapäisen häiriön vuoksi ei ollut saanut tarkistetuksi kortinhaltijan luottorajan enimmäismäärää. Tästä oli aiheutunut kortinhaltijalle huomattavia lisäkustannuksia, sillä hän oli tapauksen johdosta joutunut muuttamaan matkasuunnitelmiaan. Raastuvanoikeus hyväksyi kortinhaltijan valituksen, jonka HO kuitenkin myöhemmin kumosi. Lopulta kyseistä häiriötä tietoliikenteessä ei tapauksessa pidetty kuitenkaan ylivoimaisena esteenä ja näin ollen

---

<sup>232</sup> Näin ollen este ei saa johtua esimerkiksi palveluntarjoajan sisäisistä olosuhteista, kuten tuotantoprosessista tai toiminnan organisoimisesta. Palveluntarjoajan vaikutuspiirissä olevina esteinä voidaan lähtökohtaisesti pitää kaikkia sellaisia seikkoja, joihin se voi vaikuttaa toiminnan suunnittelulla, organisoinnilla ja valvonnalla.

<sup>233</sup> HE 169/2009, s.84.

<sup>234</sup> Saarnilehto – Hemmo – Kartio, 2001, s.456.

<sup>235</sup> Saarnilehto – Hemmo – Kartio, 2001, s.455.

luottokorttiyhteisö velvoitettiin korvaamaan kortinhaltijalle sekä kaikki oikeudenkäyntikulut että myös kortin käytön epäämisestä aiheutuneet kustannukset, jotka tosin arvioitiin oikeudessa jonkun verran pienemmiksi mitä kortinhaltija oli vaatinut.<sup>236</sup> Tilanne tapahtui fyysisessä maksuympäristössä, mutta sen ratkaisuperiaatteita voidaan soveltaa myös sähköisessä ympäristössä tapahtuviin maksutapahtumiin, vaikkakin sähköisessä ympäristössä asioitaessa vastaavanlaisen tapauksen todistelu osoittautuisikin todennäköisesti huomattavasti hankalammaksi. Se kuitenkin osoittaa, että yleistä linjaa häiriöiden osalta voi olla hankalaa vetää, vaan useimmiten tapauskohtainen arviointi voi olla paikallaan.<sup>237</sup>

Joka tapauksessa maksupalvelulain vastuunjakosäännökset jättävät maksuyhteyden katkeamistilanteissa ja tilapäisissä maksuverkon pettämistilanteissa tilanteen varsin näytönvaraiseksi ja lisäksi riippuvaiseksi siitä, onko palveluntarjoajalla syy-yhteyttä ongelmaan tai onko se voinut jollain tavalla vaikuttaa asiaan. Käytännössä tämänlainen sääntely antaa palveluntarjoajille varsin suuret mahdollisuudet rajoittaa vastuutaan teknisissä ongelmatilanteissa. Usein näin myös tehdään: esimerkiksi Nordean verkkopankkipalvelujen yleisissä sopimusehdoissa pankki ilmoittaa, että se ei vastaa palvelussa mahdollisesti esiintyvien häiriöiden tai virheiden takia aiheutuvista välillisistä tai epäsuorista vahingoista. Lisäksi ehdoissa mainitaan, että pankki ei vastaa ylivoimaisista esteistä aiheutuvista vahingoista. Tällaisiksi yksilöidään mm. pankista riippumattomat häiriöt automaattisessa tietojenkäsittelyssä, tiedon siirrossa tai sähköön saannissa.<sup>238</sup> Lähtökohtaisesti palveluntarjoaja siis vastaa omista virheistään, mutta muissa tilanteissa vastuu on maksupalvelun käyttäjillä. Kuitenkin, koska maksupalvelun käyttäjälle voi joissain tilanteissa olla hankalaa osoittaa, milloin virhe johtuu nimenomaisesti palveluntarjoajan toiminnasta ja milloin esim. verkon häiriöistä, pankin vastuuseen saaminen ko. tilanteissa saattaa käytännössä olla varsin hankalaa.

### 5.2.2.2 Maksuverkon pettäminen

Viime aikoina on esiintynyt myös kotimaassa useita julkisuutta saaneita tapauksia, jossa maksupalvelun tarjoajan koko maksuverkko on pettänyt. Tietoliikennehäiriö kaatoi esimerkiksi OP-Pohjolan verkkopankin tammikuussa 2011, jonka seurauksena palveluntarjoajan verkkopankki oli kokonaan pois käytöstä noin 3 tunnin ajan, jonka jälkeen saman päivän iltaan asti käytettävissä oli

---

<sup>236</sup> KKO 1989:98

<sup>237</sup> Vastaavanlaisia yksittäisiä tapauksia vastuunjaon osalta löytyy myös mm. arvopaperilautakunnan selvityksistä ks. esimerkiksi APL132/2008, saatavilla osoitteessa [http://www.fine.fi/apl\\_ratkaisut/?2&case=158](http://www.fine.fi/apl_ratkaisut/?2&case=158)

<sup>238</sup> Ks. Nordea, 2010<sup>b</sup>, s.5. <http://www1.nordea.fi/appx/solo/1/pdf/MMST960DL.pdf> Haettu 10.4.2011.

pelkkä pankin tekstiversio, eli ainoastaan peruspalvelujen käyttö kuten laskujen maksaminen oli mahdollista.<sup>239</sup>

Maksuverkon pettäessä maksujärjestelmän käyttö estyy. Tämä ei ole taloudellisesta näkökulmasta kenenkään osapuolen intressissä. Erityisesti maksujärjestelmän käyttäjien kannalta kyseiset tilanteet voivat olla varsin ongelmallisia: heille voi aiheutua merkittäviäkin *välillisiä* taloudellisia vahinkoja siitä syystä, ettei haluttuja maksutapahtumia päästä suorittamaan. Vahinkojen laajuus riippuu usein myös tilanteen kestoista. Kuten edellä mainittiin, palveluntarjoaja vastaa maksupalvelulain mukaan välillisistä vahingoista vain siinä tapauksessa, että se ei ole rajoittanut vastuutaan sopimuksella ja vahinko aiheutuu palveluntarjoajan huolimattomuudesta tai jos vastuunrajoituksesta on sovittu, vain tapauksissa, joissa vahinko aiheutuu tahallisesti tai törkeästä huolimattomuudesta.

Palveluntarjoajat ovatkin usein ottaneet myös maksuverkkoon ja sen toimintaan liittyviä vastuunrajoitusehtoja maksupalveluita koskeviin sopimuksiinsa. Yleensä niissä täsmennetään, etteivät maksunvälittäjät vastaa maksuverkon pettämistapauksissa välillisistä vahingoista, kuten tulonmenetyksistä tai saamatta jääneestä tuotosta. Joissain sopimuksissa selvennetään lisäksi käyttäjille, että palveluntarjoaja ei takaa, että maksupalvelu olisi asiakkaiden käytössä keskeytyksettä, vaikka siihen yleensä pyrittäisiinkin.<sup>240</sup> Usein maksupalveluiden tarjoajilla on myös heidän tietoverkkonsa toimittajan kanssa sopimus, jossa määritellään osapuolten vastuista esim. tietoverkon rakentamisen, toiminnan ja mahdollisten virheiden korjaamisen osalta.

Käytännössä näin siis maksuverkon pettämistilanteissa palveluntarjoajan vastuu tilanteesta aiheutuvista seurauksista käyttäjille on varsin kattavasti rajattu, ja lähtökohtaisesti maksujärjestelmän käyttäjät vastaavat itse maksuverkon pettämisestä aiheutuvista välillisistä seurauksista. Näin ollen esimerkiksi asiakas, joka ei ole voinut antaa pätevää maksumääräystä sen takia, että hän ei ole päässyt käyttämään maksulaitettaan ja on kärsinyt tästä syystä taloudellista vahinkoa, kuten esim. joutunut maksamaan viivästyskorkoa maksun myöhästymisestä<sup>241</sup>, vastaa itse vahingosta jos maksulaitteen käytön estyminen ei ole johtunut palveluntarjoajan tahallisesta toiminnasta tai törkeästä huolimattomuudesta. Myös kauppias, joka on menettänyt potentiaalisia tuloja sen takia, että maksuvälineitä ei ole voitu käyttää ostotransaktioihin verkon ongelmien vuoksi

---

<sup>239</sup> OP-Pohjola, 2011. <https://www.op.fi/op?cid=151424569&srcpl=4> Haettu 29.1.2011.

<sup>240</sup> Ks. esim. Nordea, 2010<sup>b</sup>, kohta 13. Saatavilla osoitteessa <http://www1.nordea.fi/appx/solo/1/pdf/MMST960DL.pdf>

<sup>241</sup> KOM 2003(718), s.71.

<sup>242</sup>, vastaa itse ko. vahingoista samojen periaatteiden mukaisesti. Toisaalta valtionvarainministeriön kannanoton mukaan tällaisissa tilanteissa maksupalvelun käyttäjän voisi olla joka tapauksessa vaikeaa todistaa, kuinka moni asiakas tai yleensä yksikään asiakas olisi yrittänyt ostaa myyjän tuotteita tai palveluita tänä aikana. <sup>243</sup> Myös maksujen viivästymisen osoittaminen nimenomaan teknisten ongelmien syyksi ja sen todistelu ei ole kovinkaan helppoa. Euroopan talous- ja sosiaalikomitean mukaan maksuverkon pettämistilanteet eivät onneksi kuitenkaan ole kovin tavanomaisia. <sup>244</sup>

Perussiviilioikeudellisesta näkökulmasta niin kahden vastuuperusteen käyttö kuin myös vastuunrajoitusehtojen yleisyys ilmentävät hyvin yleistä sekä delikti- että sopimusperusteiseen korvausvastuuseen liittyvää käsitystä siitä, että välillisten vahinkojen korvauskelpoisuuden on syytäkin olla alhaisempaa kuin välittömien vahinkojen: sopimuskomppanin välilliset vahingot käsittävä vastuu merkitsisi usein (tässä tapauksessa etenkin palveluntarjoajille) hyvinkin mittavia vastuuriskejä, joita ko. toimijat eivät ole valmiita kantamaan. <sup>245</sup> Jos palveluntarjoajat laitettaisiin välittömän vastuunsa lisäksi myös välilliseen vastuuseen maksuverkon toiminnasta ja sen mahdollisista häiriötilanteista, etenkin pienempien maksunvälittäjien kohdalla toimintaan liittyvät riskit saattaisivat muodostua kohtuuttoman suuriksi ja rajoittaa palveluiden tarjoamista.

Kaikesta huolimatta voidaan mielestäni kuitenkin katsoa että maksupalveluiden tarjoamiseen sisältyy tietty ennaltaehkäisyvastuu, jotta tilanteisiin, joissa palveluita ei voida käyttää, ei jouduttaisi. Tähän viittaa myös Euroopan talous- ja sosiaalikomitean lausunto, jossa todetaan aluksi että maksupalvelujen tarjoajia ei tulisi asettaa vastuuseen sellaisista maksuista, jotka eivät kirjautuneet maksujärjestelmään sen pettämisen aikana. Komitea lisää kuitenkin, että ”maksupalvelun tarjoajan on kuitenkin näytettävä ryhtyneensä kaikkiin tarpeellisiin toimiin maksuverkon pettämisen estämiseksi”, jonka lisäksi huomioon on vastuun arvioinnissa otettava se, kuinka hyvin ko. luottolaitos on noudattanut pankkivalvontaviranomaisten sille asettamia vaatimuksia systeemiriskeistä ja liiketoiminnan jatkuvuudesta. <sup>246</sup> Lausunnossa ei määritellä kuitenkaan sen tarkemmin, mitä tällaiset *tarpeelliset* toimet sisältävät. Voidaan mm. nostaa esille kysymys, olisiko mahdollisesti tarpeellista että maksuverkon pettämistilanteita varten palveluiden

---

<sup>242</sup> KOM 2003(718), s.71.

<sup>243</sup> VM, 2004, s.72.

<sup>244</sup> Euroopan talous- ja sosiaalikomitea, 2004, kohta 3.21.1.

<sup>245</sup> Saarnilehto – Hemmo – Kartio, 2001, s.598-599.

<sup>246</sup> Euroopan talous- ja sosiaalikomitea, 2004, kohdat 3.21.1 - 2.

tarjoajilla olisi jonkinlainen varajärjestelmä käytössään, ja voitaisiinko varajärjestelmän puuttumista pitää jopa ratkaisevana perusteena sille, voiko palveluntarjoaja vedota ylivoimaiseen esteeseen välittömien vahinkojen korvausvastuun välttämiseksi? Esimerkiksi Saarnilehto et. al katsovat, että varajärjestelmien ylläpito ei olisi niin hankalaa, että ainakaan lyhytaikainen tietoyhteyksien katkos ei oikeuttaisi palveluntarjoajia pidättymään sopimuksen täyttämisestä ylivoimaiseen esteeseen vedoten ilman em. varajärjestelmän olemassa oloa.<sup>247</sup>

Asiaa on osittain sivuttu mm. valtioneuvoston päätöksessä huoltovarmuuden tavoitteista, jonka mukaan ”maksuliikennejärjestelmien toimivuus sekä ajantasaisten tietojen saaminen ja säilyminen on varmistettava myös tilanteissa, joissa järjestelmät siirtyvät kansallisten rajojen yli. Pankkien välisen maksuliikenteen hoitamiseksi on oltava riittävät varajärjestelyt, erityisesti yhtenäiseen euromaksualueeseen siirtymisen jälkeen.”<sup>248</sup> Ko. päätös koskee siis ainoastaan pankkeja. Ainakin merkittävimmillä kotimaisilla pankeilla onkin käytössään varayhteys verkkopankkiin siltä varalta, että ensisijainen verkko pettää tai sitä joudutaan huoltamaan. Kuitenkin voidaan kysyä, olisiko tämä velvollisuus sovellettavissa myös muihin maksujenvälittäjiin, mikäli heidän ylläpitämässään maksujärjestelmässä suoritettavien transaktioiden arvo on kansantaloudellisesti riittävän suuri. Asiaan olisi mielestäni hyvä saada selvitystä myös viranomaisten taholta.

---

<sup>247</sup> Saarnilehto – Hemmo – Kartio, 2001, s.456.

<sup>248</sup> 21.8.2008/539, kohta 2.2.

### 5.3 MUUT ERITYISKYSYMYKSET

Maksujen suorittamiseen ja turvallisuuteen liittyvien kysymysten lisäksi sähköisen maksamisen osalta voidaan nostaa esiin muutamia muitakin kysymyksiä. Nykyinen, ylikansallisesta lainsäädännöstä johdettu sähköisen maksamisen sääntelykokonaisuus ohjaa paikoin maksualan kehitystä varsin vahvasti tai vastaavasti aiheuttaa oikeudellista epävarmuutta tietyille palveluntarjoajille. Toisaalta voidaan myös pohtia, olisiko maksumarkkinoilla tarvetta paikoin kenties nykyistä vahvemmallekin ohjaukselle tiettyjen yhteiskuntaryhmien maksupalveluiden turvaamiseksi.

#### 5.3.1 Sääntelystä tai muusta toimintaan liittyvästä oikeudellisesta epävarmuudesta aiheutuvat kysymykset

Informaatioteknologian nopean kehittymisen myötä nykyään myös muilla yrityksillä kuin talletuspankeilla on teknologiset valmiudet harjoittaa maksujenvälitystä.<sup>249</sup> Erityisesti tele- ja internet-operaattoreilla olisi edellytykset laajamittaiseenkin maksujenvälitykseen lähitulevaisuudessa, sillä niillä on ko. teknologisten valmiuksien lisäksi myös laaja asiakaskunta jolle ne voisivat tällaisia uudentyypisiä maksujenvälityspalveluita tarjota.<sup>250</sup> Kuitenkin, asiakkaiden hitaan uusien maksutapojen omaksumisen ohella myös muutamat lainsäädännölliset kysymykset luovat tiettyjä haasteita uusien teknologioiden täysipainoiselle hyödyntämiselle maksumarkkinoilla.

##### 5.3.1.1 Pienmaksuvälineen määritelmä ja pienmaksuvälineitä koskevien erityissäännösten tarkoituksenmukaisuus

Uusille maksujenvälityspalveluille ja sähköisen rahan liikkeeseenlaskulle on ominaista, että ne eivät muodosta helposti luokiteltavaa palveluiden ryhmää<sup>251</sup>, mikä on ollut ongelmallista juridisesta näkökulmasta. Kuitenkin yhteistä näille uudemmille maksamisen muodoille on lähtökohtaisesti ollut se, että maksutapahtumat ovat useimmiten kooltaan varsin pieniä. Tämä vallitseva käyttötarkoitus on yritetty ottaa huomioon myös uudessa maksupalvelualan lainsäädännössä. Maksupalvelulakiin on sisällytetty erityissäännökset, jotka koskevat erityisellä *pienmaksuvälineellä* suoritettavaa maksamista. MPL 8.11§ määrittelyn mukaan pienmaksuvälineellä tarkoitetaan maksuvälinettä,

---

<sup>249</sup> Majuri, 2005, s.1.

<sup>250</sup> Majuri, 2005, s.3.

<sup>251</sup> Majuri, 2005, s.2.

a) jota puitesopimuksen mukaan voidaan käyttää enintään 30€ tai, jos maksuvälinettä voidaan käyttää vain kotimaan maksutapahtumiin, enintään 60€ määräisiin maksutapahtumiin;

b) jonka käyttöraja puitesopimuksen mukaan on enintään 150€ tai, jos maksuvälinettä voidaan käyttää vain kotimaan maksutapahtumiin, enintään 300€; taikka

c) jolle tallennettujen varojen määrä ei puitesopimuksen mukaan voi ylittää 150€, tai jos maksuvälinettä voidaan käyttää vain kotimaan maksutapahtumiin, 500€. <sup>252</sup>

Pienmaksuvälineisiin kohdistuvassa erityissäätelyssä on ensisijaisesti lähtökohtana antaa osapuolille laajempi sopimusvapaus maksupalvelun ja sen käytön osalta: sopia voidaan vapaammin mm. ennakkotiedonantovelvollisuuksista (17§), toteutettujen maksutapahtumien tiedonantovelvollisuuksista (21§) , maksutoimeksiannon peruuttamisesta ja toteuttamisesta kieltäytymisestä (43§), toteuttamisajoista (50§), katoamisilmoituksen tekemisestä (61§) sekä vastuunjaosta pienmaksuvälineen oikeudettoman käytön tapauksissa (77§).

Maksupalveludirektiivin esipuheessa perustellaan näiden erityissäännöksen perusteita. Sen mukaan *”Pienmaksuvälineiden olisi oltava halpa ja helppokäyttöinen vaihtoehto hinnaltaan edullisten tavaroiden ja palvelujen maksamiseen, eikä niihin pitäisi kohdistaa liiallisia vaatimuksia. Niitä koskevat tietojenantovaatimukset ja niiden toteuttamista koskevat säännöt olisi sen vuoksi rajoitettava koskemaan olennaisia tietoja ottaen samalla huomioon tekniset ominaisuudet, joita pienmaksuvälineillä voidaan oikeutetusti odottaa olevan. Kevyemmistä vaatimuksista huolimatta maksupalvelunkäyttäjien suojan pitäisi olla riittävántasoinen ottaen huomioon, että kyseisiin, erityisesti ennalta maksettuihin välineisiin liittyy rajoitettu riski.”* <sup>253</sup> Nämä uudet maksujenvälityspalvelut on pyritty siis ottamaan huomioon siten, että lainsäädännöllä ei ainakaan tarpeettomasti rajoitettaisi ko. palveluiden leviämistä yhteiskunnassa. Kuitenkaan tiettyjä turvallisuuteen liittyviä näkökohtia ei ole voitu täysin sivuuttaa.

---

<sup>252</sup> Hallituksen esityksen mukaisesti b-kohdalla tarkoitetaan jälkikäteen laskutettavia, ”post-paid” maksuvälineitä, ja c-kohdalla etukäteen maksettavia, ”pre-paid” maksuvälineitä. Rajat eroavat toisistaan siksi, että direktiivin mukaan jäsenvaltiot saavat itse päättää, soveltavatko kaksinkertaisia rajoja, kuten Suomi on päättänyt toimia kotimaan maksutapahtumien osalta. (HE 169/2009, s. 38)

<sup>253</sup> EY/2007/64, s.5.

Lähtöajatuksen lain valmistelussa voidaan katsoa olleen oikeansuuntainen. Kyseinen pienmaksuvälineluokittelu nostaa siitä huolimatta esille muutamia kysymyksiä, joiden osalta voidaan pohtia säännösten tarkoituksenmukaisuutta.

Ensinnäkin, pienmaksuvälineen määritelmä on annettu siis ensisijaisesti matkapuhelimen käyttöä maksuvälineenä sekä erilaisia sähköisen rahan sovelluksia silmällä pitäen. Kuitenkin kuluttajaviraston näkemyksen mukaan periaatteessa mitkä tahansa maksuvälineet voidaan laskea pienmaksuvälineiksi, jos niiden käyttö on rajoitettu vain ns. pienmaksamiseen.<sup>254</sup> Tämä tarkoittaa, että myös esim. yhdistelmäkorttien osalta pienmaksuvälineen määritelmä voi täytyä osittain: samalla maksukortilla voi puitesopimuksen mukaan olla useita erilaisia käyttötapoja, jolloin sitä voidaan oikeudellisessa mielessä pitää useana eri maksuvälineenä. Tällöin myös maksupalvelulakia tulee hallituksen esityksen mukaan soveltaa sen perusteella, miten maksukorttia käytetään.<sup>255</sup> Käytännössä tämäntyyppinen jaottelu voi aiheuttaa tulkinnallisia kysymyksiä lain soveltamisesta.

Toinen, vähintään yhtä merkittävä näkökulma liittyy siihen, onko tämäntyyppisellä määrittelyllä liian suuntaa-antava vaikutus maksuvälinetyypin kehitykseen? Vaikka määritelmän tarkoituksena on ollut edistää kyseisten välineiden käytön lisääntymistä maksamisessa, asialla voidaan katsoa olevan myös kääntöpuoli: pienmaksuvälineen määritelmään sisältyvien euromääräisten rajojen on toisaalta myös arvioitu saattavan rajoittaa mm. matkapuhelimen laajempaa käyttöä maksuvälineenä.<sup>256</sup> Tämä voi esimerkiksi vaikuttaa maksuvälineen ominaisuuksien ja maksutapojen kehittämiseen: on vaarana, että uudet tekniset innovaatiot tapahtuvat myös osittain sitä tosiasiaa silmällä pitäen, minkä tyyppisiin maksuihin väline soveltuu lainsäädännöllisesti parhaiten. Tämä ei ole varmastikaan ollut lainsäätäjän tarkoituksena.

### **5.3.1.2 Soveltamisalaan liittyvät epäselvyydet mobiilimaksamisen osalta sekä muut maksupalvelulain vaikutukset mobiilimaksamiseen**

Maksupalvelulain 1. luvun 1§:ssä säädetään lain soveltamisalasta. Sen kohdan 2 mukaan lakia sovelletaan ”maksutapahtuman toteuttamiseen tilisiirtona, varojen siirtona palveluntarjoajan maksutilille, suoraveloitukseen taikka maksukortilla tai muulla maksuvälineellä maksamiseen”.

---

<sup>254</sup> Kuluttajavirasto, 2010, s.6.

<sup>255</sup> HE169/2009vp, s.38.

<sup>256</sup> HE169/2009vp, s.25.



Lisäksi kohdan 6 mukaan lakia sovelletaan, kun ”maksutapahtuma toteutetaan siten, että maksajan suostumus maksutapahtuman toteuttamiseen annetaan matkapuhelimella tai tietokoneella taikka muulla telepäätelaitteella tai tietoteknisellä laitteella ja maksu suoritetaan sellaiselle televiestintä- tai tietotekniikkajärjestelmää tai -verkkoa hoitavalle yritykselle, joka toimii *ainoastaan maksutapahtuman välittäjänä* maksupalvelun käyttäjän ja tavarana, palvelun tai muun hyödykkeen toimittajan välillä.”

Kyseinen soveltamisalamäärittelmä on siis varsin kattava kaikenlaisien sähköisten maksupalvelujen osalta: sen alle menevät niin tilisiirrot, suoraveloitukset, korttimaksut (mukaan lukien luottokorttimaksut), rahansiirrot sekä mobiililaitteiden ja internetin välityksellä suoritettavat maksut siltä osin, kun maksutapahtuman välittäjän toiminta rajoittuu ainoastaan maksun välittämiseen, ts. välittäjä ei tuo palvelukokonaisuuteen lisäarvoa. Mobiilimaksamisen osalta soveltamisalan ulkopuolelle jäävät siis esim. ns. sisältöpalvelut sekä muut lisäarvolla katsotut maksutapahtumat<sup>257</sup>.

Soveltamisalaa koskeva määrittely on erityisen merkittävässä asemassa ns. uusien maksujenvälittäjien näkökulmasta. Maksupalvelulaki sisältää esim. tiedonantoon, vastuunjakoon sekä muihin seikkoihin olennaisesti vaikuttavia säännöksiä, joista seuraa huomattavia järjestelmä- ja sopimusmuutostarpeita jo olemassa oleviin palvelukokonaisuuksiin. Palveluntarjoajat ovat mm. velvoitettu toimittamaan (maksu)tietoja pysyvällä tavalla, joksi tekstiviestiä ei lain mukaan pidetä riittävänä, koska sitä ei voi yleensä tallentaa ja toisintaa.<sup>258</sup> Lisäksi huolellisuusvelvoitteet maksuvälineen säilyttämisestä ovat matkapuhelimen ja muiden maksuvälineiden osalta ovat lain näkökulmasta erilaiset, ts. kevyemmät matkapuhelimen osalta. Mm. elinkeinoelämän keskusliitto onkin kommentoinut, että maksupalveludirektiivin valmistelussa ei olisikaan riittävästi onnistuttu huomioimaan erilaisten maksupalveluiden ominaispiirteitä.<sup>259</sup>

Liikenne- ja viestintävaliokunnan mukaan asiantuntijakuulemisessa on tuotu esille, että ko. sääntelyllä voi olla merkittäviä kustannusvaikutuksia teleoperaattoreiden toimintaan ja mobiilimaksamiseen.<sup>260</sup> Valiokunnan saaman selvityksen mukaan edes pienmaksamisvälinettä

---

<sup>257</sup> Palvelut, joissa itse maksettava sisältö voidaan ottaa vastaan ainoastaan päätelaitteeseen eli esimerkiksi uutiset, logot ja soittoäänet.

<sup>258</sup> FiCom, 2009<sup>b</sup>. [http://www.ficom.fi/lausunnot/index\\_1.html?Id=1243960481.html](http://www.ficom.fi/lausunnot/index_1.html?Id=1243960481.html) Haettu 1.12.2010.

<sup>259</sup> Gauriloff, 2009, s.10.

<sup>260</sup> LiVL 2/2010vp

koskevat kevyemmät velvoitteet eivät ratkaise näitä ongelmia,<sup>261</sup> ja useiden mobiilimaksupalveluita tarjoavien yhtiöiden mielestä lain piiriin joutumisesta koituukin liikaa kustannuksia suhteessa kännykkämaksuista saataviin tuloihin.<sup>262</sup> Näiden lain edellyttämien muutosten aiheuttamien kustannusvaikutusten on jopa esim. arvioitu olevan teleyritysten tarjoamien maksamispalvelutoiminnan laajuuteen nähden niin suuria, että soveltamisalan piiriin tulevien palvelujen tarjonta voidaan joutua lopettamaan,<sup>263</sup> jonka lisäksi ne voivat myös vaikuttaa kielteisesti telealan yritysten mahdollisuuteen tarjota uusia maksupalvelutuotteita.<sup>264</sup> Vähintäänkin muutokset aiheuttavat tn. merkittäviä muutoksia mobiilimaksupalveluiden hinnoitteluun.

Soveltamisalan ja siten myös sääntelyn piiriin joutumisesta seuraa siis merkittäviä vaikutuksia teleyrityksille. Näin ollen kriittisen, jopa ratkaisevan keskeiseksi kysymykseksi teleyritysten näkökulmasta muodostuukin se, milloin teleyritysten tarjoamat maksupalvelut tuottavat käyttäjälleen laissa tarkoitettua lisäarvoa ja milloin eivät? Jo lain valmisteluvaiheessa monet lausunnonantajista (mm. MTV Media, Teleforum Ry, FICOM) toivoivat, että operaattoreiden tuottamaa lisäarvoa maksupalveluun tulkittaisiin mahdollisimman laajasti, mikä mahdollistaisi ainakin tiettyjen lisäarvopalvelukokonaisuuksien tarjonnan jatkumisen.<sup>265</sup> Näin direktiiviä myös tulkittaisiin ja sovellettaisiin samoin kuin muualla EU:ssa, jolloin suomalaiset teleyritykset eivät joutuisi muita sisämarkkinoilla toimivia yrityksiä merkittävästi poikkeavaan asemaan, jonka lisäksi myös tuettaisiin viestintävälinettä hyväksikäyttävien uudenaikaisten palvelukokonaisuuksien ja pienille käteismaksuille vaihtoehtoisten sähköisten maksutapojen kehitystä.

Maksupalvelulain esitöissä on pyritty selkeyttämään ko. lisäarvon käsitettä. Selvityksen mukaan muiden kuin digitaalisten hyödykkeiden, kuten logojen, soittoäänien, datapalvelujen ym. kohdalla lisäarvoa tuottaakseen viestintäverkon haltijan on tarjottava sellaista lisäpalvelua, jota ei ole saatavilla muutoin tai palvelu on räätälöity ulkopuolisen elinkeinonharjoittajan kanssa tehdyn sopimuksen perusteella. Tällaista lisäpalvelua voisi esityksen mukaan olla esimerkiksi palvelu, jossa asiakas voi itse määritellä tekstiviestimatkalipun voimassaoloajan tai alkamisajankohdan.<sup>266</sup>

---

<sup>261</sup> LiVL 2/2010vp

<sup>262</sup> Kauppalehti 3.6.2010, <http://www.kauppalehti.fi/5/i/talous/uutiset/etusivu/uutinen.jsp?oid=2010/06/34073&sort=false> Haettu 3.3.2011.

<sup>263</sup> Mm. FiCom, 2009<sup>b</sup>.

<sup>264</sup> LiVL 2/2010vp

<sup>265</sup> FiCom, 2010. [http://www.ficom.fi/lausunnot/index\\_1.html?Id=1265701806.html](http://www.ficom.fi/lausunnot/index_1.html?Id=1265701806.html) Haettu 7.1.2011.

<sup>266</sup> HE 169/2009vp, s.28.

DNA Oy:n lausunnon mukaan kuitenkin tämänlaisen palvelun toteuttaminen ei ole edes mahdollista teleyrityksen järjestelmissä, vaan sopeuttamisen voisi tehdä ainoastaan matkalipun tarjoava palveluntuottaja. Yritys katsoikin, että teleyritys tuottaisi käyttäjille lisäarvoa jo palveluiden käytettävyyttä edistävien pääsy-, haku- ja jakelumahdollisuuksien avulla.<sup>267</sup>

Tyhjentävä lisäarvon käsitteen määrittely ei mobiilimaksupalveluiden monimuotoisuudesta johtuen kuitenkaan ollut lain yhteydessä mahdollista. Koska myös lain implementointi on ollut vielä kesken, yhtenäistä eurooppalaistakaan soveltamiskäytäntöä ei ole vielä syntynyt. Näin ollen sääntelyn soveltumisesta tiettyihin matkapuhelimella maksettaviin palveluihin ei olekaan vielä täyttä varmuutta, vaan arviointi on tapauskohtaisen harkinnan varassa. Jo tämä on ongelmallista sen takia, että mobiilimaksupalvelut on vielä kehitysvaiheessa oleva alue, josta odotettavissa olevat tuotot eivät ole suuria. Palveluntarjoajat eivät varmastikaan halua kehittää palveluita, joista ei ole varmuutta täyttävätkö ne lisäarvon käsitteen vai eivät.

Näin ollen yhtiöt ovatkin nykyisen epäselvän tilanteen vallitessa joutuneet päättämään, jatkavatko ne toimintaansa lain vaatimusten alla, muokkaavat tarjoamiaan palveluita tai kenties lopettavat toimintansa kannattamattomana. Ainakin osa mobiilimaksupalveluita tarjoavista yrityksistä on maksupalvelulain voimaantulon jälkeen muuttanut palveluaan siten, että maksupalvelulain edellyttämä lisäarvon vaatimus täyttyy. Muun muassa HSL uudisti joukkoliikennevälineissä toimivaa kännykkälippuaan siten, että lipun ostajilla on nyt mahdollisuus viivästyttää voimassaoloajan alkamisajankohtaa, jolloin yritys tuottaa palveluun lain edellyttämää lisäarvoa, ja näin ollen jää maksupalveludirektiivin ja -lain soveltamisalan ulkopuolelle.<sup>268</sup> Tämä kuvastaa hyvin sitä, kuinka ratkaisevasta asiasta on kysymys.

### **5.3.1.3 Sähköiseen rahaan liittyvät juridiset kysymykset**

Sähköisen rahan markkinat ovat kasvaneet odotettua verkkaisemmin Euroopassa. Sähköistä rahaa käytetään nykyisin epätyydyttävän vähän pääosin siksi, että sähköistä rahaa koskevan direktiivin hyväksymisen jälkeen maksumarkkinoille on tullut uusia toimijoita odotettua vähemmän. Vuoden 2007 lopussa sähköisen rahan liikkeeseenlaskijoita oli globaalilla tasolla ainoastaan 20, jonka

---

<sup>267</sup> Gauriloff, 2009, s.16 - 17.

<sup>268</sup> Nupponen, Taloussanomien 27.4.2010.

lisäksi 127 yritykselle oli myönnetty poikkeuslupa liikkeeseenlaskuun.<sup>269</sup> Suomessa ei tällä hetkellä ole finanssivalvonnan tietojen mukaan voimassa yhtään sähköisen rahan liikkeeseenlaskijaa koskevaa toimilupaa,<sup>270</sup> ja ainoastaan kaksi yhteisöä harjoittaa poikkeusluvan mukaista rajoitettua luottolaitostoimintaa.<sup>271</sup>

Monet tahot ovat syyttäneet kehityksestä vanhaa sähkörahadirektiiviä (EY/2000/46). Sillä pyrittiin avaamaan markkinoita sähköisen rahan liikkeeseenlaskulle: tavoitteena oli luoda selkeä oikeudellinen kehys, jolla vahvistettaisiin sähköisten maksujen yhtenäismarkkinoita ja edistettäisiin kilpailua samalla varmistuen toiminnan vakauden riittävä valvonta. Kuitenkin, valtioneuvoston kannanoton mukaan tietyt direktiiviin sisältyvät heikkoudet estivät näiden toivottujen tulosten saavuttamisen: ensinnäkin, sekä sähköinen raha että direktiivin soveltamisala olivat epäselvästi määritelty, mikä heikensi oikeusvarmuutta ja haittasi markkinoiden kehitystä. Toinen vanhan sähkörahadirektiivin puute oli oikeudellisen kehysten epäjohdonmukaisuus: toiminnan vakauden valvontajärjestelmä oli suhteeton jonka lisäksi myös poikkeus- ja toimilupamenettelyissä oli epäjohdonmukaisuuksia.<sup>272</sup>

Varsinkin pienten liikkeeseenlaskijoiden kannalta ko. sääntelyjärjestelmä oli harjoitettuun toimintaan nähden ylimitoitettu ja käytännössä pikemminkin hidasti siirtymistä sähköisiin maksupalveluihin.<sup>273</sup> Se epäonnistui myös tasaväkisen peli/toimintakentän luomisessa pankkien ja muiden sähköisen rahan liikkeeseenlaskijoiden välille (esim. matkapuhelinoperaattorit). Lisäksi vanha direktiivi oli minimiharmonisointidirektiivi, joka puolestaan johti siihen, että eroavat tulkinnat ja sisällytys kansallisiin lakeihin jäsenvaltioissa heikensivät sen menestystä edelleen. Viimeistään maksupalveludirektiivin myötä oli selvää, että sähkörahadirektiiviä on välttämätöntä tarkastaa, koska jotkin sen säännökset erosivat merkittävästi sähkörahadirektiivin vastaavista säännöksistä.<sup>274</sup>

---

<sup>269</sup> KOM (2008)627, s.2.

<sup>270</sup> Rekisteri valvottavista finanssivalvonnan internetsivuilla osoitteessa <http://www.finanssivalvonta.fi/fi/Fiva/Valvottavat/Pages/Valvottavat.aspx> Haettu 9.4.2011.

<sup>271</sup> Niistä toinen, APE Paymets Oy, tarjoaa sähkörahasovellusta, joka on tarkoitettu juuri pienten verkko-ostosten maksamiseen. Toinen on HYY:n sähköinen Lyyra- opiskelijakortti, johon voidaan ladata rahaa ja maksaa ainoastaan rajoitetussa ympäristössä.

<sup>272</sup> Valtioneuvosto, 2009, s.2.

<sup>273</sup> Majuri, 2005, s.247.

<sup>274</sup> Esimerkiksi sähköisen rahan liikkeeseenlaskijat eivät direktiivin EY/2000/46 nojalla saaneet harjoittaa muuta liiketoimintaa kuin sähköisen rahan liikkeeseenlaskua, mutta direktiivin EY/2007/64 nojalla saavat.

Uusi sähkörahadirektiivi (EY/2009/110) annettiin syyskuussa 2009. Sillä pyrittiin tarkistamaan vanhaa direktiiviä ja korjaamaan sen edellä mainittuja heikkouksia. Uudessa sähkörahadirektiivissä sähköisen rahan määritelmää on pyritty muokkaamaan selkeämmäksi ja teknisesti neutraalimmaksi, ja lisäksi linkittämään paremmin muun uuden maksualan sääntelyn kanssa. Lisäksi direktiivin soveltamisalaa on pyritty rajaamaan: rajoitettujen sähköisen rahan välineiden<sup>275</sup> liikkeeseenlaskijat sekä ns. lisäarvoa tuottavien palveluiden<sup>276</sup> tarjoajat on jätetty direktiivin ulkopuolelle. Myös toiminnan vakauden valvontajärjestelmää on tarkasteltu uudelleen, jonka seurauksena mm. liikkeeseenlaskijoiden alkupääomavaatimuksia lasketaan miljoonasta eurosta 350000 euroon. Sähköisen rahan liikkeeseenlaskijat saavat jatkossa myös mm. harjoittaa lisäksi muutakin liiketoimintaa kuin sähköisen rahan liikkeeseenlaskua.

Näiden muutosten pitäisi helpottaa uusien innovatiivisten ja turvallisten sähköisen rahan palveluiden suunnittelua, lisätä kilpailua markkinoilla sekä mahdollistaa uusien toimijoiden markkinoille pääsemisen.<sup>277</sup> Tämän pitäisi edelleen edesauttaa sähköisen rahan käyttöönottoa. Mm. valtioneuvosto arvioi kannanotossaan, että liikkeeseenlaskijoiden määrä saattaisi lisääntyä uuden direktiivin myötä.<sup>278</sup> Euroopan komissio arvioi, että uusi sääntelykehikko tarjoaa sähköisen rahan markkinoille toisen mahdollisuuden: sen mukaan markkinoiden volyymi voisi nousta (nykyisestä miljardista) jopa 10 miljardiin muutaman vuoden sisällä.<sup>279</sup> Uusi täysharmonisoiva sähkörahadirektiivi on pantava kansallisesti täytäntöön viimeistään huhtikuun 2011 loppuun mennessä. Sähköisen rahan sääntely tullaan siirtämään luottolaitoslaista maksulaitoslakiin.<sup>280</sup> Jää nähtäväksi, miten uuden direktiivin mukanaan tuoma sääntely vaikuttaa sähköisen rahan suosioon tulevaisuudessa.

Kuitenkin, myös uuden sähkörahadirektiivin osalta on noussut esille huolia siitä, miten sen jotkut säännökset saattavat toisaalta osittain myös vaikeuttaa tiettyjen, jo olemassa olevien

---

<sup>275</sup> Välineet, joita voi käyttää vain rajallisessa verkostossa. Tällaisiin välineisiin voivat kuulua kauppojen omat kortit, polttoainekortit, jäsenkortit, matkakortit, ateriasetelit tai palvelusetelit. Kuitenkin kun tällaisesta erityiseen käyttötarkoitukseen osoitetusta välineestä kehittyy yleisväline, siihen ei pitäisi enää soveltaa poikkeussäännöistä direktiivin soveltamisalasta. (EY/2009/110, kohta (5))

<sup>276</sup> Palvelut, joissa palvelua hoitava yritys ei toimi ainoastaan maksun välittäjänä.

<sup>277</sup> Euroopan komission internetsivut, [http://ec.europa.eu/internal\\_market/payments/emoney/index\\_en.htm](http://ec.europa.eu/internal_market/payments/emoney/index_en.htm) Haettu 5.2.2011.

<sup>278</sup> Valtioneuvosto, 2009, s.4.

<sup>279</sup> KOM (2010)245, s.12.

<sup>280</sup> VM, 2010.

palvelukokonaisuuksien tuottamista. Kotimaassa tärkein näistä liittyy sähköisen rahan uuteen lunastettavuusveloitteeseen. Sähkörahadirektiivin 11 artikla velvoittaa sen liikkeeseenlaskijat lunastamaan ”sähköisen rahan haltijan pyynnöstä minä hetkenä hyvänsä nimellisarvosta haltijan hallussa olevan sähköisen rahan rahallisen arvon”. Kyseisen säännöksen tarkoituksena on ilmeisesti ollut kasvattaa luottamusta sähköisen rahan liikkeeseenlaskijoihin sekä sähköiseen rahaan. Asiaa valmisteltaessa ei välttämättä ole kuitenkaan huomioitu riittävästi miten se vaikuttaa tiettyihin, jo olemassa oleviin sähköisen rahan järjestelmiin, joita ei välttämättä ole suunniteltu ko. ominaisuutta silmällä pitäen.

Muutos vaikuttaa Suomessa erityisesti teleyrityksiin ja niiden prepaid – liittymiin<sup>281</sup>, jotka uusi direktiivi katsoo sähköiseksi rahaksi. Järjestelmät on suunniteltu suomessa siten, että tällä hetkellä liittymän haltijoilla ei ole mahdollisuutta saada ladattua saldoa takaisin teleyritykseltä. Näin ollen direktiivin säännös aiheuttaa sen, että järjestelmiä täytyisi uuden sähkörahadirektiivin myötä muuttaa, josta aiheutuisi teleyrityksille merkittäviä kustannuksia. Esimerkiksi tietoliikenteen ja tietotekniikan keskusliitto FiCom katsoi lausunnossaan sähkörahadirektiivin muutosehdotuksesta, että artiklaa sähköisen rahan lunastettavuudesta ei voida hyväksyä. Ottaen huomioon prepaid – liittymien vähäisen markkinaosuuden suomessa sekä ko. liittymätyypin pääasiallisen kohderyhmän, lunastettavuusvaatimusta ei voida heidän mielestään pitää kohtuullisena eikä tarkoituksenmukaisena.<sup>282</sup>

### 5.3.2 Erityisryhmien huomiointi

Taloudellisten intressien ohella sähköiseen maksamiseen ja sen sääntelyyn liittyy myös tärkeitä yhteiskunnallisia kysymyksiä. Teknologinen kehitys ja maksuympäristön muuttuminen ovat johtaneet siihen, että myös maksulaitosten perinteiset toimintamallit ovat muuttuneet ja kehityksessä yhä enenevässä määrin sähköistä maksamista tukevaan muotoon. Kustannustehokkuussyihin vedoten useat kotimaiset pankit ovat viime aikoina sulkenet konttoreitaan tai lyhentäneet niiden asiointiaikoja. Esimerkiksi osa pankeista on siirtynyt toimintamalliin, jossa laskuja ei voi maksaa eikä käteistä nostaa konttoreista enää klo 13 jälkeen.<sup>283</sup>

Maksuautomaatit poistuivat käytöstä vuoden 2011 alusta, suoraveloituksesta luovutaan ja vähitellen

---

<sup>281</sup> Aiemmin, toisin kuin suuressa osassa muita EU:n jäsenvaltioita, Suomessa teleyritysten pre-paid liittymiä ei ole pidetty sähköisenä rahana. Uusi direktiivi tuo nämä liittymät direktiivin soveltamisalaan siltä osin kuin ne kuuluvat myös maksupalveludirektiivin soveltamisalaan.

<sup>282</sup> FiCom, 2009<sup>a</sup>.

<sup>283</sup> Kuluttajavirasto, 2010, s.2.

käyttöön otetaan myös e-lasku.<sup>284</sup> Lisäksi pankit ohjaavat myös palveluiden hinnoittelulla asiakkaitaan verkkopankkiin.<sup>285</sup>

Vaikka onkin ymmärrettävää ja useiden maksuympäristön toimijoiden kannalta myös toivottavaa, että maksuympäristö kehittyy teknologisen kehityksen rinnalla, on huomioitava että ko. kehityksestä voi aiheutua myös joitakin ongelmia. On esitetty, että sähköiset maksujärjestelmät eivät olisi välttämättä tarpeeksi käyttäjäneutraaleja ja siirtäessään suurimman osan asiointipalveluistaan verkkoon palveluntarjoajat syrjisivät joitain tiettyjä erityisryhmiä, joiden mahdollisuudet tai taidot sähköiseen maksamiseen ovat lähtökohtaisesti heikommalla kuin muilla maksujärjestelmien käyttäjillä. Maksupalvelut ovat kuitenkin lain mukaan ns. välttämättömyyspalveluita, joita ei voi rajata tietyille asiakkaille, vaan niiden on oltava kaikkien saatavilla.<sup>286</sup>

### **5.3.2.1 Tietoyhteiskunnan vaikeasti saavuttavien mahdollisuus sähköisten maksupalveluiden käyttöön**

Eduskunnassa on nostettu esille kirjallisen kysymyksen (KK564/2010vp) muodossa erityisesti *vanhusten sekä toimintarajoitteisten mahdollisuus sähköisten maksujärjestelmien käyttöön*. Ko. kysymyksessä alleviivattiin muun muassa, että varttuneesta väestöstä suuri osa on jäänyt tietoyhteiskuntakehityksen ulkopuolelle: kaikilla ei ole käytössään tietokonetta ja verkkoyhteyksiä eikä myöskään riittäviä taitoja verkkoasiointiin.<sup>287</sup> Tilastokeskuksen lokakuussa 2010 tekemä tutkimus tukee tätä näkemystä: mukaan 65–74 vuotiaista vain 36 % oli käyttänyt verkkopankkia viimeisten 3 kuukauden aikana, ja ostoksia verkon kautta tehnyt 9 %.<sup>288</sup> Tätä vanhemmilla ko. luvut ovat todennäköisesti vielä pienempiä.

Lain luottolaitostoiminnasta 134§ perusteella kaikilla on oikeus peruspankkipalveluihin. Laki määrittelee ko. peruspankkipalveluiksi tavanomaisen talletustilin, tarvittavat tilinkäyttövälineet ja mahdollisuudet laskujen maksamiseen tililtä.<sup>289</sup> Säännös ei kuitenkaan velvoita pankkeja sen yksityiskohtaisemmin tältä osin, joten käytännössä laissa ei ole pakottavaa estettä sille, että suuri

---

<sup>284</sup> KK 564/2010vp, s.1.

<sup>285</sup> Kuluttajavirasto, 2010, s.4.

<sup>286</sup> Kuluttajavirasto, 2010, s.2.

<sup>287</sup> KK 564/2010vp, s.1.

<sup>288</sup> Tilastokeskus, 2010. [http://tilastokeskus.fi/til/sutivi/2010/sutivi\\_2010\\_2010-10-26\\_tie\\_001\\_fi.html](http://tilastokeskus.fi/til/sutivi/2010/sutivi_2010_2010-10-26_tie_001_fi.html) Haettu 12.4.2011.

<sup>289</sup> Kuluttajavirasto, 2010, s.4.

osa maksupalveluista siirretään sähköiseen ympäristöön. Näin ollen palveluntarjoajat voivatkin varsin vapaasti määritellä kehityksen suuntaa. Koska asiointipalveluiden ylläpito konttoreissa tai paperilaskutus eivät ole korkeampien kustannustensa vuoksi yhtä kannattavaa toimintaa kuin niiden siirtäminen sähköiseen muotoon, palveluntarjoajien intressi on vastakkainen ko. erityisryhmien kanssa. Tämän lisäksi erityisryhmien osuus kokonaismaksuliikenteestä on todennäköisesti varsin pieni, joten ko. käyttäjäryhmät tuskin tuovat myöskään tulopuolella mitään merkittäviä hyötyjä palveluntarjoajille.

Mielestäni kehitystä alueella ei välttämättä voida jättää ainoastaan palveluntarjoajien valvontaan. Kysymyksen vastauksessa allekirjoitettiin, että vaikka teknologinen kehitys onkin välttämätöntä maksamisen kokonaiskustannuksien vähentämiseksi, on ko. erityisryhmien raha-asioiden hoitamisen turvaaminen erittäin tärkeää, samoin kuin se, että heille tarjottavien maksamispalveluiden palvelutaso säilyy korkeana. Esimerkiksi e-laskutukseen siirtymisen osalta mainittiin, että osa pankeista tulee tarjoamaan automaattisen maksamisen palvelua asiakkaille, joiden käytössä ei ole verkkopankkia.<sup>290</sup> Kuitenkaan selkeitä toimenpiteitä vanhusten ja toimintarajoitteisten raha-asioiden hoitamisen turvaamiseksi hallituksen osalta ei vastauksessa esitetty. Voidaan kuitenkin pohtia, pitäisikö lainsäädännöllä kenties ottaa vahvemmin kantaa asiaan: olisiko syytä esimerkiksi luoda selkeämmät reunaehdot sille, missä määrin palveluita olisi tarjottava myös perinteisessä muodossa? Vai pitäisikö vaihtoehtoisesti antaa markkinoiden hoitaa ko. kannan muodostamisen? Omasta mielestäni ko. palveluiden tarjonta muihin vaihtoehtoihin verrattuna olisi vähintäänkin suhteutettava erityisryhmän kokoon. Kuitenkin viime kädessä lainsäädäntö olisi varsin tehokas väline puolustamaan yhtäläisyysperiaatteen toteutumista.

### **5.3.2.2 Eriarvoisuus sähköisten tunnisteiden, erityisesti verkkopankkitunnusten osalta**

Myös sähköiseen tunnistautumiseen ja erityisesti verkkopankkitunnisteiden käyttöön liittyy tällä hetkellä piirteitä jotka asettavat kansalaiset eriarvoiseen asemaan.<sup>291</sup> Lain luottolaitostoiminnasta 134§ peruspankkipalveluita koskeneen hallituksen esityksen perustelujen mukaan *tarvittaviin tilinkäyttövälineisiin* kuuluivat automaattikortti, pankkikortti ja verkkopankkitunnukset.<sup>292</sup> Eduskunnan talousvaliokunta muutti kuitenkin ehdotettua säännöstä lisäämällä sinne rajoituksia. Näin ollen pankkiala ei tällä hetkellä katso verkkopankkitunnusten kuuluvan

---

<sup>290</sup> KK 564/2010vp, s.2

<sup>291</sup> KK 620/2010vp, s.1

<sup>292</sup> Ks. HE 33/2002, s.59, 75.



peruspankkipalveluiden joukkoon, vaan pitää niitä lisäpalveluna pankin asiakkaille.<sup>293</sup> Tämä aiheuttaa mm. sen, että heidän näkökulmastaan verkkopankkitunnuksia ei ole välttämätöntä tarjota tai myöntää tasapuolisesti kaikille asiakkaille kuten esim. maksuhäiriöisille, tai jo alun perin luottokelvottomille. Tämä puolestaan taas aiheuttaa sen, että nämä ryhmät uhkaavat jäädä ilman toimivia pankkipalveluita ja heidän talouteen osallistumisensa hankaloituu: ilman pankkitunnuksia mahdollisuudet sähköiseen tunnistautumiseen ja esim. maksuautomaattien poistuttua myös laskujen maksamiseen heikkenevät huomattavasti. Pankkitunnusten asema ja niiden vaihtoehtoisten sovellusten rajoitettu käyttö tunnistautumisvälineenä muissakin yhteiskunnan palveluissa hankaloittaa edelleen näiden erityisryhmien toimintaa. Esimerkiksi maksuhäiriömerkintöjä on tällä hetkellä jo 319 000 suomalaisella yksityishenkilöllä<sup>294</sup>, joten kysymys on yhteiskunnallisesti varsin merkittävästä asiasta.

Esimerkiksi Kuluttajavirasto pitää tilannetta ongelmallisena. ja ko. sähköisen tunnistautumisen eriarvoisuus on kyseenalaistettu kirjallisen kysymyksen (KK620/2010vp) muodossa myös eduskunnassa. Vastauksessa mainittiin, että ”pankkien oman ilmoituksen mukaan pankkitunnisteita on mahdollista joissain tilanteissa saada myös verkkopankista irrallisena palveluna. Vähintään yhdellä pankilla on tällainen tuote, PrePaid -tunnisteet, hinnoiteltuna ja tarjolla kaikille, joiden ensitunnistus voidaan tehdä luotettavasti.” Lisäksi todettiin että väestökisterikeskuksen ylläpitämä varmenne on pankeista riippumaton tunnistusratkaisu ja että uusia vaihtoehtoja varmentamispalveluiden osalta tutkitaan.<sup>295</sup> Vastauksen perusteluja voidaan mielestäni pitää toisaalta oikeutettuina, toisaalta voidaan kuitenkin myös katsoa, että nämä verkkopankkitunnisteille vaihtoehtoiset tunnistusmenetelmät eivät korjaa riittävästi tätä eriarvoisuutta, koska em. irralliset tunnistukset ovat maksullisia ja kansalaisvarmenne käytettävyydeltään puutteellinen.

Myös siis tämän kysymyksen osalta voidaan pohtia, pitäisikö lainsäädännöllä ottaa vahvemmin kantaa siihen, ovatko verkkopankkitunnukset osa peruspankkipalvelukokonaisuutta vai eivät. Pitemmällä aikavälillä ratkaisuna ko. eriarvoisuuden korjaamiseen voisi vaihtoehtoisesti nähdä myös mobiilivarmenteet niiden käyttömahdollisuuksien lisääntyessä. Maksuhäiriömerkinnän tai luottokelvottomuuden ei pitäisi kuitenkaan tarpeettomasti rajoittaa tai hankaloittaa peruspankkipalveluiden käyttöä tai muuta verkkoasiointia, kuten tällä hetkellä näyttäisi tapahtuvan.

---

<sup>293</sup> KK 620/2010vp, s.2

<sup>294</sup> Suomen Asiakastieto Oy, 2011. <http://www.asiakastieto.fi/asiakastieto/ajankohtaista/index.jsp?T=nu&A=422>  
Haettu 13.4.2011.

<sup>295</sup> KK 620/2010vp, s.2.

## 6. LOPUKSI

Tässä tutkielmassa on pyritty tekemään selvitys yleisimmin käytössä olevista sähköisistä maksutavoista ja sähköiseen maksamiseen liittyvästä sääntelystä kotimaisessa lainsäädäntökehikossa. Sen lisäksi olen pyrkinyt selvittämään, minkälaisia ongelmia sähköisen maksuympäristön erityispiirteistä tai vastaavasti alueen varsin monitahoisesta sääntelystä mahdollisesti aiheutuu maksujärjestelmien osapuolille ja miten oikeudellinen vastuu em. ongelmatilanteissa jakautuu maksutapahtumaan liittyvien osapuolten kesken.

Maksutapahtumien suorittamiseen on siis nykyään olemassa monia vaihtoehtoisia järjestelmiä, joista useimmat ovat sähköisiä. Riippuu sekä maksujärjestelmän ominaisuuksista, maksamisen kustannuksista sekä maksun luonteesta mikä järjestelmä soveltuu kunkin tyyppiin maksutapahtumiin parhaiten. Maksaminen kansainvälisessä verkkokaupassa on perinteisesti tapahtunut luottokortin avulla, kotimaassa lisäksi mm. tilisiirrot ja suoraveloitukset ovat vakiinnuttaneet asemansa maksukäytännöissä. Vaikka sähköisen maksamisen vaihtoehdot ovat viime aikoina monipuolistuneet, nämä maksutavat ovat säilyttäneet asemansa suosituimpina maksutapoina ihmisten maksutottumusten muuttuessa verkkaisesti. Sähköisen rahan menetelmistä odotettiin vielä vuosituhatien vaihteessa uutta vauhdittajaa alalle, mutta niiden käyttö on vielä toistaiseksi ollut vaisua. Viime aikoina matkapuhelinten käytön yhä kasvaessa ja laitteiden teknisten ominaisuuksien parantuessa, on kehittynyt erilaisia mobiilimaksamisen muotoja, jotka tosin ovat jääneet vielä varsin paikallisiksi. Erityisesti pienten maksujen maksutavat kehittyvät kuitenkin kaiken aikaa. Uudet palveluntarjoajat lisäävät kilpailua, ja kehittyvä tekniikka mahdollistaa maksupalvelujen tarjoamisen eri kanavien kautta. Internetin ja matkapuhelimen käyttöön perustuvia maksusovelluksia kehitetään jatkuvasti.<sup>296</sup>

Maksamisen monimuotoistuuessa sekä kaupankäynnin edelleen kansainvälistyessä myös oikeudellisen sääntelyn tarve maksumarkkinoilla osapuolten aseman selkeyttämiseksi on kasvanut. Eurooppalaisia integraatiotavoitteita vahvasti silmällä pitäen Euroopan komissio on ottanut johtavan roolin maksualan sääntely-ympäristön kehittämisessä ja yhtenäistämässä etenkin maksutapahtumien toteuttamiseen sekä tarjoamiseen liittyen. Kuitenkin sääntely on viime vuosina lisääntynyt esim. henkilön tunnistamisen osalta myös puhtaasti kansallisten aloitteiden turvin. Toimintaympäristöstä johtuvien erityispiirteiden takia yhtenäisen ja toimivan

---

<sup>296</sup> Jyrkönen – Paunonen, 2003, s.4.

sääntelykokonaisuuden rakentaminen sähköisen maksamisen alueelle on kuitenkin osoittautunut varsin haastavaksi, ja paikoin keskeinen rooli alueen oikeudellisen sääntelyn lisäksi onkin myös lain vaatimuksia täydentävillä maksualakohtaisilla standardeilla sekä toisaalta maksupalvelusta tehdyillä sopimuksilla. Tietyissä tilanteissa joudutaan turvautumaan myös osittain velvoiteoikeudellisiin periaatteisiin sekä alueen ennakkoratkaisukäytäntöihin.

Kysymykset sähköisen maksamiseen liittyen voidaan jakaa pääpiirteittäin varsin luontevasti kolmeen osa-alueeseen: maksamisen turvallisuuteen, maksutapahtumaan ja sen toteuttamiseen sekä alueen sääntelyyn ensisijaisesti liittyviin kysymyksiin. Maksamisen turvallisuuden osalta korostuvat erityisesti henkilön oikeelliseen tunnistamiseen eli identifiointiin sekä tietoturvallisuuteen liittyvät kysymykset. Viime aikoina identiteettivarkaudet, erilaiset maksuhuijaukset ja tietojen kalastelu kuin myös suorat hyökkäykset maksujärjestelmiin ovat lisääntyneet ja tulleet entistä sofistikoituneemmiksi, ja jopa vahvan tunnistamismenetelmän statuksen saaneet henkilön tunnistamiskäytännöt ovat osoittautuneet paikoin haavoittuvaisiksi näiden uhkien edessä. Lisääntynyt verkkorikollisuus onkin noussut merkittäväksi huolenaiheeksi ja sähköisten maksupalveluiden käyttöä rajoittavaksi yksittäiseksi tekijäksi: mm. keskusrikospoliisin mukaan sähköisessä muodossa olevan tiedon fyysiseen suojaamiseen, tiedon syöttämisen suojaamiseen, laitteiden ja tiedon käsittelyyn sekä haavoittuvuuksien nopeaan korjaamiseen tulisikin kiinnittää erityistä huomiota.<sup>297</sup>

Mitä tulee henkilön tunnistamiseen, palveluntarjoajilla on aina, myös anonyymejä maksutapahtumia sisältävissä asiakkuussuhteissaan, asiakkaidensa tuntemisvelvollisuus. Näin ollen vastuu osapuolten luotettavan tunnistamisen järjestämisestä myös sähköisten maksutapahtumien yhteydessä on lain mukaan lähtökohtaisesti maksun välittäjällä. Lainsäädännössä edes ns. vahvoilta sähköisen tunnistamisen menetelmiltä ei kuitenkaan edellytetä aukottomuutta vaan ainoastaan riittävää luotettavuutta. Näin ollen useimmilla tällä hetkellä käytössä olevilla sähköisillä tunnistamismenetelmillä ei voida luoda oikeudentilaa, jossa henkilö tulee kaikissa tilanteissa sidotuksi ko. sähköisellä menetelmillä tehtyihin oikeustoimiin, vaan arviointi on tapauskohtaista. Identiteettierohdyksen seuraukset ja riskinjako siihen liittyen voivat vaihdella jonkun verran käytetyn maksuvälineen ja palvelusta tehtyjen sopimusten perusteella. Etenkin maksutapahtumissa, joissa ei suoriteta ns. vahvaa tunnistamista, vastuuta voidaan vierittää sopimuksin myös myyjille. Pienmaksuvälineiden osalta palveluntarjoajien riskiä voidaan siirtää myös muille käyttäjille, mukaan lukien kuluttajille, mikäli välineet ovat sellaisia että niiden käyttöä ei voida estää. Kaikkien

---

<sup>297</sup> Keskusrikospoliisi, 2009, s.1.

oikeudettomien maksutapahtumien osalta on syytä kuitenkin huomata, että ratkaisevin merkitys vastuunjaon kannalta tapauskohtaisessa arvioinnissa on osapuolten sopimuksenmukaisten velvoitteiden, kuten huolellisuus- sekä ilmoitusvelvollisuuksien oikea-aikaisella täyttämällä.

Tietoturvallisuuteen liittyvät kysymykset voidaan jakaa kahteen osaan. Yksittäisten maksutapahtumien osalta sääntelyssä on lähtökohtana, että jokainen maksutapahtumaan liittyvä osapuoli vastaa omalta osaltaan siitä, että maksutapahtumasta muodostuu turvallinen: palveluntarjoajat ja myyjät kantavat vastuun omista järjestelmistään, maksupalvelun käyttäjien vastuu on puolestaan yleensä määritelty palveluntarjoajan ja käyttäjän välisissä sopimuksissa ja rajoittuu usein yleisiin huolellisuus-, tietoliikenneyhteyden salaus- sekä päätelaitteen suojausvelvoitteisiin. Ko. lähtökohdista huolimatta joissakin tilanteissa, kuten esimerkiksi tietynlaisten uudentyypisten verkkohyökkäysten yhteydessä voi kuitenkin käytännössä olla varsin hankalaa osoittaa kuka on vastuussa tietoturvaan kohdistuvasta loukkauksesta, etenkin kun kaikki osapuolet ovat toimineet pääasiassa heiltä kohtuudella vaadittavissa olevien edellytysten mukaisesti. Tietojen säilyttämisen osalta tilanne on vastuunjaon kannalta selkeämpi, mutta siltä osin tilannetta on puolestaan hankaloittanut rekisterinpitäjien vaihteleva asenne alueen ongelmiin sekä se, että käyttäjien on usein vaikeaa todentaa kuinka turvallisia palveluntarjoajien ja myyjien käyttämät järjestelmät oikeastaan ovat.

Tietoturvan saralla palveluntarjoajilla voidaan joka tapauksessa nähdä huomattavasti suurempi kokonaisvastuu suhteessa muihin osapuoliin, sillä he ovat turvallisten järjestelmäratkaisujen suunnittelun ja toteuttamisen lisäksi vastuussa myös riittävän tietoturvaohjeistuksen sekä asiakas- ja käyttäjätietojen turvallisen säilyttämisen toteuttamisesta. Lain tasoinen sääntely on kuitenkin alueella varsin yleisluontoista ja teknologiariippumatonta, mikä antaa palveluntarjoajille varsin suuret vapaudet teknologioiden valintaan ja itseohjautuvaan toiminnan suunnitteluun. Koska tekniset turvallisuusvaatimukset voivat muuttua nopeastikin uusien menetelmien syntyessä, lainsäädäntö ei välttämättä olekaan paras vaihtoehto teknisen turvallisuuden lisäämiseksi, vaan avainasemassa ovat vastuulliset maksuliikennealan elinkeinonharjoittajat. Tietoturvasääntelyä onkin usein täydennetty erillisillä maksuyhteisöjen laatimilla standardeilla. Toisaalta myös vastuunjaon kontrollointi voitaneen jättää varsin vahvasti itsesääntelyn varaan, sillä tietoturvaongelmat ja niihin suhtautuminen vaikuttavat olennaisesti käyttäjien valintoihin. Lainsäädännöllä on syytä kuitenkin varmistaa vähintään riittävän tiukkojen rangaistussäännösten olemassa olo: viime aikoina rikoslainsäädäntöä tietoturvarangaistusten osalta onkin tiukennettu, mitä pidän oikeansuuntaisena kehityksenä.

Toisen kokonaisuuden alueen kysymysten osalta muodostaa maksujen suorittamiseen liittyvä sääntely. Viime aikoina lisääntynyt yhteismarkkinalainsäädäntö on yhtenäistänyt sääntelyä eri maksuvälineiden välillä. Myös osapuolten asemaa ja vastuuta heidän omasta toiminnastaan on selkeytetty: esimerkiksi maksupalveluiden käyttäjillä on juridisesti aiempaa täsmällisemmin määritelty vastuu mm. maksutietojen oikeellisesta syöttämisestä, maksuvälineiden ja niihin liittyvien tunnistustietojen säilyttämisestä sekä myös muiden huolellisuus- ja tiedonantovelvollisuuksien täyttämistä. Vaikka kaikkien toimijoiden vastuuta onkin paikoin kasvatettu, mielestäni sääntelyssä on kuitenkin toisaalta otettu varsin hyvin huomioon myös osapuolten neuvotteluasema ja toimintaedellytykset. Näin ollen palveluntarjoajien vastuu suhteessa maksupalvelun käyttäjiin on lähtökohtaisesti laajempi. Erityisesti kuluttajien näkökulmasta nykyinen sääntely on varsin suotuisaa: sikäli kun kuluttajat ovat toimineet riittävän huolellisesti ja lainsäädännön sekä palvelusta tehtyjen sopimusten mukaisesti, heidän asemansa ja varallisuutensa suhteessa maksutapahtuman muihin maksutapahtuman osapuoliin on varsin kattavasti turvattu. Lisäksi mm. luottoon perustuvien sekä velkoja-aloitteisten maksujen osalta palveluntarjoajat on asetettu toissijaiseen vastuuseen kuluttajia kohtaan, mikäli myyjät eivät täytä sopimuksenmukaisia velvoitteitaan. Muiden käyttäjien sekä pienmaksuvälineiden osalta palveluntarjoajilla on mahdollisuus rajoittaa vastuutaan sopimuksin huomattavasti enemmän. Kyseisenlainen vastuunjako voidaan nähdä koko maksuliikealan luottamuksen edistämisen kannalta tarkoituksenmukaisena, sillä se kannustaa myös palveluntarjoajia kehittämään palveluitaan edelleen. Toisaalta alueella on kuitenkin myös huolehdittava siitä, ettei maksupalveluiden tarjoaminen ja niihin liittyvien velvollisuuksien täyttäminen muodostu palveluntarjoajille kokonaisuudessaan kohtuuttoman raskaaksi näiden toimintaedellytykset huomioiden. Tämä on huomioitu ainakin maksutapahtumien teknisiin ongelmiin liittyvien vastuukysymysten osalta: palveluntarjoajat ovat lain mukaan lähtökohtaisesti vastuussa vain välittömistä, itse aiheuttamistaan vahingoista, välillisten vahinkojen jäädessä käyttäjien maksettaviksi – myös kuluttajien osalta – sikäli kun palveluntarjoajat eivät ole itse menettäneet huolimattomasti ja ovat pyrkinet ennaltaehkäisemään riittävässä määrin tilanteen syntymistä.

Kuitenkin, jos tarkastelua kohdennetaan kokonaisuuden sijasta yksittäisiin säännöksiin, voidaan myös maksujen suorittamiseen liittyvässä sääntelyssä nähdä paikoin tiettyä epäsuhtaa tai potentiaalisia ongelmia. Esimerkiksi yksilöivälle tunnisteelle laissa annettu painoarvo suhteessa muihin maksutietoihin on varsin korostunut takaisinsaantitoimenpiteiden monimutkaisuuteen peilattuna. Velkoja-aloitteisten maksujen osalta on puolestaan ollut pelkona, että maksupalvelulain uusi palautussäännös tulisi johtamaan tietyistä velkoja-aloitteisista maksuista luopumiseen. Myös

nykyiset myyjän ja palveluntarjoajan yhteisvastuusäännökset tilanteissa, joissa myyjä ei täytä sopimuksenmukaisia velvoitteitaan, voidaan toisaalta nähdä luottoon perustuvien maksutapojen käyttöä suosivina. Ainakin em. säännösten osalta sääntelyssä on mielestäni tarkentamisen varaa tai vähintäänkin syytä niiden vaikutusten perusteelliseen tarkasteluun ja arviointiin. Toisaalta on kuitenkin myös huomioitava että alueella on useita, osittain ristiriitaisiakin intressejä punnittavana joten objektiivisen, kaikkia osapuolia tyydyttävän ratkaisun löytäminen näihin kysymyksiin ei ole välttämättä täysin yksiselitteistä.

Turvallisuuden ja maksujen suorittamiseen liittyvien kysymysten lisäksi sähköinen maksuympäristö itsessään nostaa esiin tiettyjä sääntelyyn ja sen tavoitteiden moninaisuuteen liittyviä kysymyksiä. Lainsäätäjät ovat varsin haastavassa roolissa pyrkiessään ylikansalliseen, yhtenäiseen, tasapuoliseen ja toimivaan mutta samalla myös uusien teknologioiden täysipainoisen hyödyntämisen mahdollistavaan sääntelykokonaisuuteen.

Tiettyjen säännösten joilla on pyritty helpottamaan uusien maksutapojen käyttöönottoa, voidaan katsoa tällä hetkellä ohjaavan maksutyyppeiden kehitystä tarpeettomasti. Vaikka uusien palveluntarjoajien toimintaedellytyksiä onkin uudemmassa sääntelyssä pyritty keventämään, voidaan kyseenalaistaa onko tässä sittenkään onnistuttu riittävässä määrin. Lisäksi voidaan myös kyseenalaistaa, onko ylikansallisessa sääntelyssä onnistuttu huomioimaan riittävästi jo olemassa olevat kansalliset palvelukokonaisuudet? Esimerkiksi useiden mobiilipalveluiden tarjoajien näkökulmasta saattaa olla nykyisen sääntelyn alla huomattavasti kannattavampaa pyrkiä jättäytymään maksupalvelulain ulkopuolelle esim. lisäarvon tuottamisen verukkeella kuin muuttamaan järjestelmiään lain vaatimusten mukaisesti. Kotimaisten prepaid – liittymien tarjoajien näkökulmasta taas uuden sähkörahadirektiivin sisältämää lunastusvelvollisuutta ei voida pitää kohtuullisena, mikä saattaa pahimmillaan johtaa jopa ko. palveluista luopumiseen. Myös maksupalvelulain pienmaksuvälinemäärittelyssä käytettävien euromääräisten rajojen asettaminen saattaa ohjata tällä hetkellä ko. pieniin maksuihin käytettyjen maksutapojen kehitystä pitkällä tähtäimellä: on vaarana, että uudet tekniset innovaatiot tapahtuvat osittain sitä tosiasiaa silmällä pitäen, minkä tyyppisiin maksuihin välineet soveltuvat juridisesti parhaiten. Esimerkiksi matkapuhelimella voisi olla tulevaisuudessa sen nykyistä käyttöä suurempaakin potentiaalia maksuvälineenä – nykyisen sääntelyn vallitessa on kuitenkin vaarana, että se jää pienten erityisalueiden maksujen suorittamisen välineeksi.

Toisaalta taas joidenkin kysymysten osalta lainsäädännöltä voitaisiin lainsäätäjiltä nimenomaisesti toivoa myös mahdollisesti nykyistä suurempaa ohjaavaa roolia. Vaikka onkin ymmärrettävää ja useimpien maksuympäristön toimijoiden kannalta myös toivottavaa että maksaminen kehittyä teknologisen kehityksen rinnalla, on huomioitava että ko. kehityksestä voi aiheutua myös joitakin ongelmia: on esitetty, että sähköiset maksujärjestelmät eivät olisi välttämättä tarpeeksi käyttäjäneutraaleja ja siirtäessään suurimman osan asiointipalveluistaan verkkoon palveluntarjoajat syrjivät joitain tiettyjä erityisryhmiä, joiden mahdollisuudet tai taidot sähköiseen maksamiseen ovat lähtökohtaisesti heikommalla kuin muilla käyttäjillä. Voidaankin kysyä, pitäisikö lainsäädännöllä ottaa vahvemmin kantaa ko. eriarvoisuuteen ja pyrkiä ko. tilanteessa mahdollisesti nykyistä suurempaan ohjaavaan rooliin, jos palveluntarjoajien omaehtoisen toiminnan kautta tätä ei tapahdu? Yhteiskunnallisesti on kuitenkin tärkeää varmistaa, että tietty palveluiden vähimmäistaso säilyy riittävänä myös niille, jotka eivät sähköisiä maksujärjestelmiä syystä tai toisesta kykene tasapuolisesti hyödyntämään.

Yhteenvedon voidaan mielestäni todeta, että vaikka sähköisen maksamisen oikeudellinen sääntely on viime aikoina lisääntynyt ja tarkentunut, on siinä toisaalta paikoin myös selkeyttämisen varaa. Dynaaminen ja globaali toimintaympäristö sekä tavoitteiden moninaisuus luovat tulevaisuudessakin haasteita alueen sääntelykokonaisuutta silmällä pitäen. Lainsäätäjien keskeisenä tehtävänä onkin pysyä teknisen kehityksen tasolla, jotta sähköiseen maksamiseen liittyvästä sääntelystä voidaan muodostaa sekä riittävän tehokasta että tasapuolista myös tulevaisuuden kehitysnäkymät huomioiden – niin alueellisesti kuin käyttäjä- ja palveluntarjoajakohtaisestikin tarkasteltuna.