Mikko Liljavirta

Pankin vai asiakkaan vastuu?

Huolimattomuuden arviointi mobiilipankin oikeudettomassa käytössä verkkohuijauksissa

Laskentatoimen ja rahoituksen akateeminen yksikkö
Talousoikeuden pro gradu -tutkielma
Talousoikeuden maisteriohjelma

Vaasa 2026

VAASAN YLIOPISTO
Laskentatoimen ja rahoituksen akateeminen yksikkö
Tekijä: Mikko Liljavirta
Tutkielman nimi: Pankin vai asiakkaan vastuu?: Huolimattomuuden arviointi mobiilipankin oikeudettomassa käytössä verkkohuijauksissa
Tutkinto: Kauppatieteiden maisteri
Oppiaine: Talousoikeus
Työn ohjaaja: Vesa Annola
Valmistumisvuosi: 2026 **Sivumäärä:** **80**

TIIVISTELMÄ:
Digitaalisten pankkipalvelujen yleistyminen on lisännyt tietojenkalasteluun perustuvia verkkohuijauksia, joissa rikolliset pyrkivät aktivoimaan pankin mobiilisovelluksen asiakkaan nimissä ja tekemään oikeudettomia tilisiirtoja. Tämän vuoksi vastuunjako pankin ja asiakkaan välillä on noussut keskeiseksi oikeudelliseksi kysymykseksi, erityisesti kuluttajien ollessa palveluntarjoajaan nähden heikommassa asemassa.

Tutkielman tavoitteena on selvittää, miten vastuu varojen menetyksestä määräytyy tilanteissa, joissa mobiilisovellus on otettu käyttöön oikeudettomasti, ja milloin asiakkaan toiminta täyttää huolimattomuuden tai törkeän huolimattomuuden tunnusmerkit. Lisäksi tarkastellaan pankin tiedonantovelvollisuuden merkitystä vastuun arvioinnissa sekä esitetään suosituksia digitaalisen maksamisen turvallisuuden vahvistamiseksi.

Metodina käytetään oikeusdogmaattista tutkimusotetta. Lähdeaineisto koostuu voimassa olevasta lainsäädännöstä, lainvalmisteluaineistosta, oikeuskirjallisuudesta sekä oikeus- ja lautakuntaratkaisuista, erityisesti FINEn ratkaisusuosituksista ja hovioikeuskäytännöstä. Koska korkeimman oikeuden ratkaisuja ei aiheesta ole, alempien asteiden ratkaisut antavat tärkeää tulkinta-aineistoa huolimattomuuden arvioinnista.

Tutkimuksen keskeisin havainto on, että pankin antaman turvallisuusviestinnän selkeys, ymmärrettävyys ja erottuvuus vaikuttavat ratkaisevasti siihen, voidaanko asiakkaan toimintaa pitää huolimattomana. Jos viestintä on epäselvää tai muistuttaa rutiininomaista tunnistautumisviestiä, asiakkaan erehtymistä voidaan pitää inhimillisenä. Toisaalta ilmeisten varoitusten huomiotta jättäminen voi johtaa vastuuseen. Pankin tekniset ja organisatoriset valmiudet reagoida väärinkäyttöepäilyihin muodostavat olennaisen osan vastuunjakokokonaisuutta.

Johtopäätöksenä todetaan, että vastuunjaon oikeudenmukainen toteutuminen edellyttää sekä pankkien että asiakkaiden huolellista toimintaa. Pankkien tulee selkeyttää turvallisuusviestintäänsä ja tuoda tunnistusvälineisiin liittyvät riskit ymmärrettävästi esiin, kun taas asiakkaiden velvollisuutena on noudattaa annettuja ohjeita ja suhtautua turvaviestintään vakavasti. Lisäksi viranomaisten tulisi asettaa vähimmäisvaatimukset pankkien turvallisuusviestinnälle, jotta kuluttajansuoja ja ratkaisukäytännön yhdenmukaisuus vahvistuisivat.

AVAINSANAT: verkkorikollisuus, verkkohuijaus, huolimattomuus, vastuunjako, maksupalvelulaki, tiliväärinkäytös, riskienhallinta

Sisällys

Taulukot

Kuviot

Kuvat

Lyhenteet

FINE	Vakuutus- ja rahoitusneuvonta
KKO	Korkein oikeus
HO	Hovioikeus
LLL	Laki luottolaitostoiminnasta (610/2014)

Tutkimuksen oikolukuun ja kielenhuoltoon olen käyttänyt avuksi OpenAI:n ChatGPT-ohjelmaa, joka käyttää GPT-5 kielimallia. Olen noudattanut yliopistoni ohjeistuksia tekoälyn käytöstä.

1 Johdanto

1.1 Tutkimuksen tausta ja merkitys

Verkkohuijauksista on tullut niin tuottoisaa rikollisuutta, että ne ovat nykyisin kannattavampia kuin perinteinen huumekauppa.[1] Samaan aikaan pankkiala on keskellä rakennemuutosta, jossa *digitalisaation* [2] myötä konttoriverkostoa on supistettu merkittävästi. Finanssivalvonnan mukaan vuonna 2019 Suomessa oli 790 henkilöasiakkaita palvelevaa konttoria, kun vuonna 2023 niitä oli enää 692. Konttoriverkosto on supistunut neljässä vuodessa lähes sadalla toimipisteellä ja käteispalvelut puuttuivat jo 198 konttorista.[3] Tämä kehitys osoittaa, että rikollisuuden painopiste on siirtynyt voimakkaasti digitaaliseen ympäristöön samalla, kun perinteiset palvelukanavat supistuvat. Samalla se korostaa entisestään, miten keskeistä asiakkaiden suojaaminen ja verkkohuijausten torjunta on pankkialalle.

Konttoreiden ja niissä tarjottavien palveluiden väheneminen ja palveluiden siirtyminen digitaaliseen ympäristöön ohjaa pankkien asiakkaita käyttämään digitaalisia palveluita fyysisen asioinnin sijaan. Koronapandemia vauhditti pankkien digitaalisten palveluiden käyttöä ja monet sijoitus- ja laina-asiat voidaan hoitaa etätapaamisella[4]. Nordea Bank Oyj on todennut vuoden 2023 vuosiraportilla, että digipalveluiden käyttö on noussut vuonna 2023 ennätyslukemiin, sillä kirjautumiset verkko- ja mobiilipankkiin kasvoivat 13 prosenttia edelliseen vuoteen verrattuna[5]. Etäasiointi pankissa on siten lisääntynyt selvästi[6]. Digitaalisten palveluiden ripeä yleistyminen on samalla lisännyt altistusta

[1] Digihuijaukset jo huumerikollisuutta kannattavampia – pankeilta vaaditaan estotoimia sekunneissa, mutta torjuntaan on valjastettava muitakin.
[2] Alasoini 2015, s. 26. Digitalisaatio tarkoittaa digitaalitekniikan hyödyntämistä arjen toiminnoissa siten, että digitaaliset ratkaisut otetaan osaksi elämää kokonaisvaltaisesti.
[3] Selvitys peruspankkipalveluiden saatavuudesta ja hinnoittelusta vuonna 2023, 2024, s. 5.
[4] Palmgren 2020.
[5] Nordea Bank Oyj 2024.
[6] Ks. Wuolijoki 2023, s. 213.Myös Wuolijoki toteaa, että 2000-luvulla pankkiasiointi on digitalisoitunut voimakkaasti ja suurin osa pankkiasiointiin liittyvistä asioista hoidetaan muutoin kuin asioimalla konttorissa.

verkkohuijausten riskeille, sillä asiakkaat toimivat entistä useammin ilman konttorien tarjoamaa henkilökohtaista neuvontaa ja varmistusmekanismeja.

Sisäministeriö on vuonna 2017 nostanut esille, että valtavan digitalisaation seurauksena myös rikollinen toiminta verkossa on mahdollista verrattain nopeasti riippumatta valtioiden rajoista.[7] Puhuttaessa verkossa tapahtuvasta rikollisuudesta tarkoitetaan yleensä kyberrikollisuutta. Kyberrikollisuus eli tietotekniikkarikollisuus viittaa rikoksiin, jotka kohdistuvat tietotekniikkaan tai tietoverkkoihin, tai jotka toteutetaan hyödyntäen näitä teknologioita.[8]

Yksi yleisimmistä kyberrikoksista on tietojenkalastelu (*phishing)*. Siinä rikollinen esiintyy luotettavana henkilönä tai aitona yrityksenä ja houkuttelee rikoksen uhrin painamaan haitallista linkkiä tai avaamaan liitetiedoston. Näiden huijauslinkkien avulla käyttäjä saatetaan väärennetylle verkkosivustolle, jonka tarkoituksena on saada uhri paljastamaan arkaluontoisia tietoja, kuten pankki- ja yhteystietoja.[9] Mikäli asiakas ajautuu antamaan esimerkiksi verkkopankkitunnuksensa sekä mahdollisia vahvistuskoodeja rikollisille, rikolliset voivat saada pääsyn henkilön verkko- ja mobiilipankkiin aktivoimalla pankin mobiilisovelluksen.

Mikäli pankin asiakas on luovuttanut pankkitunnuksensa rikolliselle ja asiakkaan tililtä on siirretty varoja oikeudettomasti, eikä pankki suostu korvaamaan varoja, voi asiakas valittaa pankin päätöksestä Vakuutus- ja rahoitusneuvontaan (myöh. FINE)[10]. FINE on maksuton neuvonta- ja riidanratkaisupalvelu, joka neuvoo asiakkaita heidän vakuutus-, pankki- ja sijoitusasioihin liittyvissä ongelmatilanteissa ja kysymyksissä. Lisäksi FINE ratkoo tapauksia, joissa asiakas on tyytymätön esimerkiksi pankin päätökseen, ja pankin sekä asiakkaan välille on syntynyt riitatilanne.[11] Pankkiasioihin liittyvät yhteydenotot

[7] Tietoverkkorikollisuuden torjuntaa koskeva selvitys 2017, s. 20
[8] Kyberrikollisuus ylittää rajat tietoverkossa. n.d.
[9] Mitä on tietojenkalastelu eli phishing? Näin verkkourkinta toimii 2022.
[10] Maksaminen ja tilit n.d.
[11] FINE, mitä teemme, missä ja miten voimme auttaa? n.d.

FINEen ovat lisääntyneet viime vuosina, pääosin *huijaus*- ja *verkkourkintatapausten*[12] lisääntymisen takia. Yhteydenottoja tämän tyyppisissä tapauksissa oli vuonna 2020 alle 200 ja vuonna 2023 määrä oli yli 500. FINEssä käsiteltävistä verkkopalveluiden väärinkäytöksistä suurin osa liittyy valesivustoihin ja niihin perustuviin tietojenkalasteluihin.[13]

Tosielämän esimerkkinä voidaan käyttää huijaustapausta, johon on haettu ratkaisua FINEn lisäksi käräjä- ja hovioikeudesta. Asiakas X oli etsimässä Omakanta-palvelua ja päätyi hakukonetulosten kautta valesivustolle, jonne hän syötti verkkopankkitunnuksensa. Rikolliset olivat ostaneet mainostilaa hakutulosten kärkeen, mikä lisäsi valesivuston uskottavuutta ja paransi huijauksen onnistumismahdollisuuksia.[14]

X:n syötettyä verkkopankkitunnukset kalastelusivustolle, hän sai tekstiviestin pankin nimissä, jossa kerrottiin, että asiakas oli aktivoimassa pankin mobiilisovellusta [15] . Mobiilisovellus, jonka rikolliset olivat aktivoineet itselleen, oli digitaalinen tunnuslukusovellus, joka toimi älypuhelimella tai tabletilla. Sen avulla pystyttiin vahvistamaan maksuja tai tunnistautumaan verkkopankkiin ja verkkopalveluihin. [16] Pankin lähettämä viesti sisälsi mobiilisovelluksen aktivointikoodin, jonka olisi täytynyt päätyä rikollisille, jotta mobiilisovellus saatiin rekisteröityä onnistuneesti. Pankin tekstiviestissä luki koodin lisäksi muun muassa ”Jos et ole tekemässä aktivointia itse, ota välittömästi yhteyttä [pankkiin] tai sulkupalveluun. Tietosi voivat olla vaarassa.”. X on myöntänyt, että hän ei lukenut viestiä huolellisesti, vaan syötti siinä olleen koodin valesivustolle. [17] Näin ollen rikollisilla oli hallussaan X:n verkkopankkitunnukset sekä

[12] ks. Huijausten selvittäminen ja ratkaisukäytännöt FINEssä 2024. Huijauksella tarkoitetaan tässä yhteydessä sellaista huijausta, jonka avulla pankin asiakkaan verkkopankkitunnukset ja siihen liittyviä vahvistuskoodeja on kalasteltu rikollisten toimesta erilaisin menetelmin. Tällaisia menetelmiä ovat esimerkiksi tietojenkalastelu sähköposti- tai tekstiviestein, tietojenkalastelu verkon osto- ja myyntipaikoilla tai tietojenkalastelu sosiaalisessa mediassa.
[13] FINE vuosikertomus 2023, 2024.
[14] Hämäläinen 2022.
[15] Hämäläinen 2022.
[16] POP Avain n.d.
[17] Hämäläinen 2022.

mobiilisovellus, jonka avulla he pystyivät kirjautumaan verkko- tai mobiilipankkiin ilman avaintunnuskorttia sekä hyväksymään siellä maksuja. Asiakas X on vienyt asian FINEn sekä käräjä- ja hovioikeuden käsiteltäväksi.

Vuonna 2023 Satakunnan käräjäoikeus on antanut tuomion, jossa se on velvoittanut pankin korvaamaan asiakkaalle X tiliväärinkäytöksellä menetetyt varat.[18] FINE oli aiemmin lausunut, että pankki ei ollut tapauksessa korvausvelvollinen, sillä FINEn näkemyksen mukaan pankin asiakas on toiminut törkeän huolimattomasti. Satakunnan käräjäoikeus on tuomiossaan todennut, että pankin asiakas X ei ollut menetellyt törkeän huolimattomasti.

Hovioikeus on antanut tapauksesta tuomion syyskuussa 2024.[19] Vaasan hovioikeuden tuomiolla, on kumottu käräjäoikeuden tuomio, minkä myötä vastuu menetetyistä varoista jää asiakkaalle ja pankki on vapautettu korvausvastuusta. Hovioikeus asettuu tapauksessa huolimattomuuden arvioinnissa FINEn kanssa samaan lopputulokseen äänestyksen (2:1) päätteeksi.

Kuten edellä on todettu, on epäselvää, miten toimitaan huijaustapauksissa, joissa pankkitunnuksia on käytetty oikeudettomasti pankin mobiilisovelluksen aktivointiin ja tämän jälkeen tehty luvattomia tilisiirtoja. Näissä tilanteissa ei ole muodostunut selkeää eikä ennakoitavaa ratkaisukäytäntöä huolimattomuuden ja törkeän huolimattomuuden arvioinnista. Tämän vuoksi sekä pankkien että pankkiasiakkaiden on vaikea arvioida, millaisin edellytyksin vastuu oikeudettomista maksutapahtumista määräytyy ja miten varojen menetyksiin tulisi riskienhallinnallisesti varautua.

Käytännön elämässä sillä on suuri vaikutus siihen, katsotaanko asiakkaan toimineen huolimattomasti tai törkeän huolimattomasti. Maksupalvelulain (290/2010) 62 §:n 2 kohdan mukaan vastuu maksuvälineen oikeudettomasta käytöstä on maksuvälineen

[18] Satakunnan käräjäoikeus 6.9.2023 L 747/2022/1499.
[19] Vaasan HO 19.9.2024 t. 342.

käyttäjälle enintään 50 euroa, mikäli maksuvälineen haltijan katsotaan toimineen huolimattomasti. Mikäli maksuvälineen haltijan katsotaan toimineen törkeän huolimattomasti, siirtyy korvausvastuu kokonaisuudessaan hänelle.

Erilaiset verkossa tapahtuvat petokset ja huijaukset ovat merkittävä yhteiskunnallinen ongelma. Taulukkoon 1 on koottu Finanssiala ry:n keräämiä tilastoja pankkien tietoon tulleista huijauksista. Vuonna 2024 suomalaiset ovat menettäneet tilaston mukaan 62,9 miljoonaa euroa verkkorikollisille, kun vastaava luku vuonna 2022 oli 32,4 miljoonaa euroa. Nousua menetettyjen varojen määrässä on ollut yhteensä noin 94 prosenttia. Vaikka nousu on ollut tilaston mukaan suuri, ovat pankit onnistuneet myös estämään tai pysäyttämään maksuja. Vuonna 2024 estettyjä tai pysäytettyjä maksuja on ollut 44,3 miljoonaa euroa, kun vuonna 2023 luku on ollut vain 14,1 miljoonaa euroa. Verkkorikokset vaikuttavat taulukon 1 perusteella olevan kasvava rikollisuuden trendi. Taulukko pitää sisällään seuraavat petostyypit, joista luvut on kerätty: tietojenkalasteluhuijaukset, sijoitushuijaukset, dokumentti- ja rakkaushuijaukset sekä toimitusjohtajahuijaukset.[20]

Taulukko 1. Pankkien tietoon tulleet huijaukset 2022-2024.[21]

Vuosi	**Suomalaisten menettämät varat verkkorikollisille (milj. euroa)**	**Pankkien estämät ja palauttamat maksut**
2022	32,4 milj.€	14,1 milj.€
2023	44,2 milj.€	32,7 milj.€
2024	62,9 milj.€	44,3 milj.€

[20] Huijaukset rajussa kasvussa vuonna 2024 – pankit saivat pysäytettyä huijattuja maksuja yli 44 miljoonan euron arvosta 2025

[21] Ks. Huijaukset rajussa kasvussa vuonna 2024 – pankit saivat pysäytettyä huijattuja maksuja yli 44 miljoonan euron arvosta 2025; Huijareilla oli aktiivinen vuosi 2023 – Pankit saivat estettyä digihuijauksia lähes 33 miljoonan euron edestä 2024; Varo, varmista, varoita -kampanja: Digihuijausten määrä kasvoi selvästi vuoden 2022 jälkipuoliskolla 2023.

1.2 Tutkimuskysymykset, aiheen rajaus ja tutkimuksen tavoite

Tutkielman tavoitteena on tarkastella ja jäsentää pankin ja asiakkaan välisen sopimussuhteen oikeudellista luonnetta sekä sen perusteella määräytyviä vastuita ja velvollisuuksia tilanteissa, joissa maksuvälineen tiedot ovat joutuneet kolmannen osapuolen haltuun ja asiakkaan tililtä on tehty oikeudettomia siirtoja. Tutkimus keskittyy pankin asiakkaisiin, jotka ovat joutuneet verkkohuijauksen uhriksi, ja siinä analysoidaan Osuuspankin ja Nordean tilien yleisiä sopimusehtoja sekä verkko- ja mobiilipankkisopimusten määräyksiä pankkipalveluiden turvallisuuden näkökulmasta. Pankkien valinta perustuu niiden asemaan Suomen merkittävimpinä talletuspankkeina.[22]

Asiakkaansuoja on yksi pankkisääntelyn keskeisistä tavoitteista. Pankit ovat yleensä kuluttaja-asiakkaisiin verrattuna merkittävästi vahvemmassa asemassa niin taloudellisesti kuin tiedollisestikin, joten asiakkaita suojataan tyypillisesti heikomman suojan periaatteen mukaisesti [23] . [24] Tutkielma on rajattu koskemaan suomalaisten pankkien ja kuluttaja-asiakkaiden välistä sopimussuhdetta erityisesti verkko- ja mobiilipankkisopimusten näkökulmasta. Kuluttaja-asiakkaat on valittu tutkimuskohteeksi, koska he ovat yritysasiakkaisiin verrattuna heikommassa asemassa, ja verkkohuijauksen seuraukset voivat aiheuttaa merkittäviä ja taloudellisesti kohtalokkaita menetyksiä[25].

Tutkielman tutkimusongelma kytkeytyy verkkohuijausten yleistymiseen ja niiden aiheuttamaan oikeudelliseen epävarmuuteen pankin ja asiakkaan välisessä

---

[22] Ks. Suomessa toimivien luottolaitosten markkinaosuudet 2024 ja Näin pankkien markkinaosuudet asuntolainoissa muuttuivat – Yhden pankin siivu kasvoi peräti 48 % 2025. Pankkien suuruus on määritelty kyseisten luottolaitosten markkinaosuuksien mukaan sekä lainakannassa mitattuna.

[23] Ks. Saarnilehto & Annola 2018, s. 23. Heikomman suojan periaatteella pyritään turvaamaan erityisesti kuluttajia, työntekijöitä ja vuokralaisia, ja se vaikuttaa erityisesti sopimuksen syntyvaiheessa. Suoja toteutuu esimerkiksi pakottavien säännösten, tiedonantovelvollisuuksien ja neuvontavelvollisuuden kautta.

[24] Wuolijoki 2022, s. 91.

[25] Nikkanen 2024.

vastuunjaossa. Erityisen tulkinnanvaraiseksi on muodostunut asiakkaan huolimattomuuden arviointi tilanteissa, joissa asiakas on erehdytettynä luovuttanut verkkopankkitunnuksensa ja mahdollistanut pankin mobiilisovelluksen asentamisen rikollisen laitteelle. Oikeuskäytäntö ei myöskään tarjoa vielä selkeää ja ennakoitavaa ratkaisulinjaa, minkä vuoksi tutkimus tarkastelee erityisesti niitä oikeudellisia perusteita, joiden nojalla vastuu oikeudettomista maksutapahtumista määräytyy.

Tutkielman päätutkimuskysymys on: Miten vastuu oikeudettomista maksutapahtumista jakautuu pankin ja asiakkaan välillä maksupalvelulain nojalla tilanteissa, joissa asiakas on verkkohuijauksen uhrina luovuttanut verkkopankkitunnuksensa ja mahdollistanut pankin mobiilisovelluksen asentamisen rikollisen laitteelle maksujen vahvistamista varten?

Pääkysymystä lähestytään seuraavien alakysymysten kautta:

1. Miten pankin ja asiakkaan väliset velvollisuudet jakautuvat sopimussuhteessa ja miten ne luovat perustan vastuunjaon arvioinnille?

2. Millä edellytyksillä asiakas on vastuussa oikeudettomista maksutapahtumista ja milloin pankki kantaa osittaisen tai täyden korvausvastuun?

3. Mitkä ovat pankin ja asiakkaan välisen huolimattomuuden ja törkeän huolimattomuuden rajat, kun asiakas on joutunut verkkohuijauksen uhriksi ja luovuttanut verkkopankkitunnukset rikolliselle?

Tutkielman aiherajaus koskee tapauksia, joissa pankin asiakkaalta on siirretty oikeudettomasti tilivaroja vahvan sähköisen tunnistamisen avulla, ja maksutapahtumat on vahvistettu pankin mobiilisovelluksella, jonka rikollinen on onnistunut aktivoimaan ja rekisteröimään oikeudettomasti. Huolellisuuden arvioinnissa tarkastellaan perusteita, joiden nojalla asiakkaan toiminta voidaan katsoa huolimattomaksi tai törkeän

huolimattomaksi. Lisäksi tutkielmassa vertaillaan suurimpien pankkien tiliehtoja maksuvälineen turvallisen käytön osalta sekä analysoidaan, millaisia velvollisuuksia ja vastuita sopimusehdot asettavat pankille ja asiakkaalle.

Tavoitteena on luoda systemaattinen ja ymmärrettävä kokonaisuus, joka vastaa esitettyihin tutkimuskysymyksiin. Juridisessa kirjoittamisessa sisältö ja argumentaation selkeys ovat keskeisiä[26], minkä vuoksi tutkielmassa painotetaan huolellisesti perusteltua, johdonmukaista ja akateemisesti täsmällistä analyysiä.

Asiakkaalla on osana asiakkaan suojaa oikeus peruspankkipalveluihin, joihin kuuluvat maksutili, maksupalvelut ja sähköisen tunnistamisen palveluiden tarjoaminen.[27] Näiden palveluiden myötä sekä pankilla että pankin asiakkaalla on velvollisuuksia, jotka synnyttävät myös vastuuta.

Tutkielma tuottaa uutta tietoa kolmella tavalla. Ensinnäkin se kokoaa yhteen ja analysoi FINEn ja hovioikeuksien ratkaisuissa käytetyt huolimattomuuden arviointikriteerit nimenomaan mobiilisovelluksen oikeudettoman käyttöönoton yhteydessä. Toiseksi tutkimus tarkastelee pankin turvallisuusviestinnän selkeyden vaikutusta vastuunjakoon ja osoittaa, milloin epäselvä viestintä siirtää vastuuta pankille. Kolmanneksi tutkielma esittää konkreettisia suosituksia viestintä- ja valvontakäytäntöjen kehittämiseksi, mikä tukee ratkaisukäytännön yhdenmukaistamista sekä kuluttajansuojan vahvistamista digitaalisessa toimintaympäristössä.

[26] Viljanen 2024, s. 6.

1.3 Tutkimusmetodit

Valtaosa oikeustieteellisestä tutkimuksesta on lainoppia eli oikeusdogmatiikkaa. Oikeusdogmatiikka perustuu voimassa oleviin oikeuslähteisiin, joita se hyödyntää niiden keskinäistä etusijajärjestystä ja käyttöjärjestystä noudattaen.[28]

Tutkielman tutkimusmenetelmä perustuu lainoppiin, jota voidaan kutsua myös tulkintajuridiikaksi. Tutkimuksen kohteena on voimassa oleva oikeustila, ja tavoitteena on selvittää sovellettavien oikeusnormien sisältöä sekä lain ja muiden oikeuslähteiden merkitystä tutkittavan ilmiön kannalta.[29]

Tutkielmassa verrataan sovellettavaa sääntelyä tutkittavaan ongelmaan ja pyritään hahmottamaan tutkimusongelman ratkaisu oikeuslähteitä tulkitsemalla. Tässä tutkielmassa selvitetään pankin sekä pankin kuluttaja-asiakkaiden oikeuksia ja velvollisuuksia sekä näistä syntyvää vastuunjakoa pankkitunnusten huolellisessa käytössä, minkä vuoksi lainopillinen tutkimusmetodi on perusteltu ja tarkoituksenmukainen.

Tutkimuksen tavoitteena on tulkita ja selventää maksupalveluoikeudellista sääntelyä sekä arvioida sen soveltumista käytännön väärinkäytöstilanteisiin. Vastaus tutkimusongelmaan pyritään löytämään hyödyntämällä oikeuslähde-, tulkinta- ja argumentaatio-oppeja, jotka muodostavat lainopin keskeiset metodit.[30]

Käytännöllisen lainopin avulla tuotetaan perusteltuja tulkintasuosituksia lain soveltajien avuksi. Lainoppi on hyvän ja perustellun argumentaation tiedettä, jossa epäselvän lain säännöstä tulisi lain tutkijan mielestä soveltaa.[31]

---

[28] Husa ja muut 2008, s. 20.
[29] Hirvonen 2011, s. 21–23; Määttä & Paso, 2022, s. 4.
[30] Määttä & Paso 2022, s. 4.
[31] Määttä & Paso 2022, s. 4.

1.4 Lähdeaineisto

Tutkielmassa käytettävä lähdeaineisto perustuu perinteisiin oikeuslähteisiin eli tulkintaperusteisiin[32]. Lainopillisessa tutkimuksessa ei puhuta tutkimusaineistosta vaan oikeuslähteistä, sillä oikeuslähteet ovat tutkimuksen ensisijainen kohde [33] . Oikeuslähdeopin mukaan oikeuslähteet jaotellaan vahvoihin, heikkoihin ja sallittuihin oikeuslähteisiin. [34] Lähdeaineiston muodostaa lainsäädäntö, lainvalmisteluaineisto, oikeuskäytäntö ja oikeuskirjallisuus. Näitä kaikkia oikeuslähteitä tulee käyttää oikeudellisessa tutkimuksessa.[35]

Tutkielman merkittävimmät oikeuslähteet ovat laki luottolaitostoiminnasta, maksupalvelulaki, vahingonkorvauslaki ja rikoslaki sekä edellä mainittujen lakien lainvalmistelutyöt ja Euroopan unionin säädökset liittyen maksupalveludirektiiviin. Aineistoa käsiteltäessä oikeuslähdeoppi on olennainen elementti, sillä se määrittelee oikeuslähteiden käytön ja niiden keskinäisen suhteen. Oikeuslähteitä ei voida pitää varsinaisina tulkintametodeina, vaan ne muodostavat systemaattisen perustan, josta tulkintaprosessin on välttämättä lähdettävä liikkeelle.[36]

Edellä mainittujen vahvasti velvoittavien oikeuslähteiden lisäksi tutkielmassa hyödynnetään heikosti velvoittavia oikeuslähteitä, joita ovat tuomioistuinratkaisut liittyen verkkopankkitunnusten kalasteluun ja siihen, miten eri oikeusasteissa on pankin asiakkaan huolimattomuutta arvioitu. Tutkielmaa kirjoitettaessa aiheeseen liittyvää korkeimman oikeuden ratkaisua ei ollut, joten lähteenä toimii alempien tuomioistuimien tuomiot.

Tutkielmassa hyödynnetään myös FINEn antamia ratkaisusuosituksia liittyen tapauksiin, joissa pankin asiakkaan tililtä on tehty oikeudettomia tilisiirtoja ja maksut on vahvistettu

[32] Hirvonen 2023, s. 38.
[33] Nieminen & Lähteenmäki 2021.
[34] Määttä & Paso 2022, s. 16.
[35] Viljanen 2004, s. 7.
[36] Hirvonen 2011, s. 41–42.

oikeudettomasti. Ne eivät ole oikeudellisesti velvoittavia tuomioistuimen ratkaisuja, vaan luonteeltaan suosituksia[37], jotka perustuvat alan vakiintuneisiin käytäntöihin ja oikeudellisiin tulkintoihin. Ratkaisusuositusten asema oikeuslähteenä on siten heikompi kuin tuomioistuinkäytännön, mutta ne voivat tarjota arvokasta empiiristä aineistoa erityisesti sen arvioimiseksi, millaisia tulkintalinjoja vakuutus- ja rahoitusalalla käytännössä sovelletaan. Tämän vuoksi niitä käytetään tässä tutkielmassa täydentävänä lähteenä yhdessä oikeuskirjallisuuden, lain esitöiden ja tuomioistuinratkaisujen kanssa.

1.5 Tutkimuksen rakenne

Tutkielma rakentuu kuudesta pääluvusta, joiden avulla vastataan esitettyihin tutkimuskysymyksiin ja muodostetaan johdonmukainen kokonaisuus pankin ja asiakkaan välisiin vastuukysymyksiin liittyen. Johdantoluvussa esitellään tutkimuksen tausta ja merkitys, määritellään tutkimuskysymykset ja rajaukset sekä kuvataan käytetty tutkimusmenetelmä ja lähdeaineisto. Lisäksi luvussa asetetaan tutkimuksen tavoitteet ja kuvataan tutkielman kokonaisrakenne.

Luvussa 2 tarkastellaan sähköisen maksamisen ja vahvan tunnistamisen oikeudellista perustaa. Luvussa käydään läpi maksupalvelulain ja tunnistuslain keskeiset säännökset sekä niiden soveltaminen pankkien tarjoamissa digitaalisissa palveluissa. Lisäksi esitellään pankkien tunnistusvälineitä ja analysoidaan mobiilisovelluksen käyttöönoton prosessia sekä siihen liittyviä oikeudettoman käytön riskejä. Luku 3 keskittyy pankin ja asiakkaan väliseen sopimussuhteeseen ja sen oikeudellisiin vaikutuksiin. Siinä tarkastellaan sopimussuhteen syntymistä, osapuolten oikeuksia ja velvollisuuksia sekä hyvän pankkitavan merkitystä asiakkaan suojan kannalta.

Luvussa 4 käsitellään vastuunjakoa tilanteissa, joissa maksuvälinettä on käytetty oikeudettomasti, ja analysoidaan maksupalvelulain mukaisia vastuusäännöksiä pankin ja

[37] Huijausten selvittäminen ja ratkaisukäytännöt FINEssä 2024.

asiakkaan näkökulmasta. Luku 5 puolestaan syventyy huolimattomuuden arviointiin verkkohuijaustapauksissa. Siinä määritellään huolimattomuuden ja törkeän huolimattomuuden käsitteet, tarkastellaan asiakkaan tavanomaista käyttäytymistä sekä arvioidaan, miten viestinnän selkeys ja inhimillinen erehtyminen vaikuttavat huolimattomuuden arviointiin. Viimeisessä luvussa 6 esitetään tutkimuksen johtopäätökset ja toimintasuositukset, joissa kootaan yhteen keskeiset havainnot ja vastaukset tutkimuskysymyksiin sekä esitetään ehdotuksia pankkien ja asiakkaiden toiminnan kehittämiseksi väärinkäytöstilanteiden ehkäisemiseksi.

Tutkielman tavoitteena on lisäksi tarjota käytännön näkökulmia pankkien riskienhallinnan ja asiakkaansuojan parantamiseen sekä tuottaa tulkintasuosituksia, joiden avulla pankit ja asiakkaat voivat varautua paremmin digitaalisen asioinnin väärinkäytöksiin.

2 Sähköinen maksaminen ja vahva tunnistaminen

2.1 Sähköinen maksaminen

2.1.1 Sähköisen maksamisen oikeudellinen perusta

Maksupalvelulaki tuli voimaan Suomessa vuonna 2010 ja se perustuu Euroopan Unionin maksupalveludirektiiviin (the first Payment Services Directive, PSD 1), jossa säännellään maksujenvälitystä. [38] Maksupalveludirektiivin yksi keskeinen tarkoitus on ollut luoda Eurooppaan yhtenäinen maksualue (SEPA, Single Euro Payments Area).[39]

Vuonna 2019 tuli voimaan toinen maksupalveludirektiivi[40] (Payment Services Directive 2, myöh. PSD 2), jonka tavoitteena on ollut saattaa entistä laajemmin erilaiset maksupalvelut sääntelyn piiriin. Suomessa Euroopan unionin direktiivi on saatettu voimaan implementoimalla säädökset osaksi maksulaitoslakia (898/2017) sekä maksupalvelulakia.[41] Tutkielman kannalta merkittävin PSD2-sääntelyn tuoma vaikutus on ollut vaatimus vahvasta tunnistamisesta sähköisissä maksutapahtumissa. Sähköisiä maksutapahtumia ovat esimerkiksi internetmaksut ja maksutilin online-käyttö. Suomessa suosituimmat sähköiset maksutavat ovat tilisiirtoihin ja korttimaksamiseen perustuvia maksutapoja.[42]

On tärkeä selvittää, milloin palveluntarjoajan, eli tutkielman kontekstissa pankin, on käytettävä vahvaa tunnistamista omissa palveluissaan. Maksupalvelulain 85 c §:n mukaan vahvaa tunnistamista tulee käyttää, jos maksaja käyttää maksutiliään verkon välityksellä, käynnistää sähköisen maksutapahtuman tai toteuttaa etäkanavan kautta

---

[38] Euroopan parlamentin ja neuvoston direktiivi 2007/64/EY, annettu 13 paivana marraskuuta 2007, maksupalveluista sisämarkkinoilla, direktiivien 97/7/EY, 2002/65/EY, 2005/60/EY ja 2006/48/EY muuttamisesta ja direktiivin 97/5/EY kumoamisesta

[39] Wuolijoki 2023, s. 284–285

[40] Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/2366 maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/1001/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta.

[41] PSD2 2023.

[42] PSD2 2023; Sähköiset maksutavat n.d.

toimen, johon voi liittyä väärinkäytöksen riski. Mikäli pankin verkkopankkitunnuksia voidaan käyttää sähköiseen tunnistamiseen, tulee pankin huolehtia sääntelyn mukaan siitä, että ne täyttävät tunnistuslain[43] edellyttämät vaatimukset.

Sähköinen maksutapahtuma perustuu pankin sekä asiakkaan väliseen sopimukseen. Maksupalvelulain 8 § 1 mom. 1 kohdan mukaan maksupalvelun käyttäjällä tulee olla sopimus palveluntarjoajan kanssa, jotta käyttäjällä on oikeus käyttää maksupalvelua maksajana tai maksunsaajana. Pankin ja asiakkaan välisiä sopimusehtoja tarkastellaan tarkemmin tutkielman luvussa 3.

Mikäli pankin asiakkaan maksuvälineet ovat päätyneet verkkorikolliselle, yrittävät verkkorikolliset usein siirtää varoja sähköisesti seuraavalle taholle. On tärkeää ymmärtää mikä on sähköinen maksutapahtuma, miten se voidaan vahvistaa ja kuinka verkkorikolliset saavat rekisteröityään itselleen pankin mobiilisovelluksen.

2.1.2 Sähköiset maksutavat ja maksuväline käsitteenä

Talouden digitalisaatio ja reaaliaikaisuuden kehittyminen vaikuttavat myös maksamisen suuntauksiin. Erilaisten maksusovellusten määrä on kasvanut huomattavasti viime vuosina. Uusimmissa maksamisen innovaatioissa maksaminen pohjautuu edelleen pitkälti perinteisten sähköisten maksuvälineiden, kuten tilisiirtojen ja korttimaksujen käyttöön. Suomessa eniten käytetyt maksutavat perustuvat juuri näihin sähköisiin maksuvälineisiin. [44] Uudempia sähköisen maksamisen muotoja ovat esimerkiksi mobiilimaksusovelluksella maksaminen tai korttimaksaminen älykellon avulla.

Maksupalvelulain 8 § 11 kohdan mukaan *maksuvälineellä* viitataan maksukorttiin tai muuhun henkilökohtaiseen välineeseen tai menetelmään, jota maksupalvelun käyttäjä

[43] Tunnistuslailla tarkoitetaan lakia vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009).
[44] Sähköiset maksutavat n.d.

ja palveluntarjoaja ovat sopineet käyttävänsä maksutapahtumissa. Hallituksen esityksessä maksuvälineellä tarkoitetaan aineellista tai aineetonta suojattua välinettä, tietoteknistä ohjelmaa tai tunnistamistietoa tai muuta vastaavaa yksilöivää tietoa taikka niiden yhdistelmää, joka mahdollistaa sen, että maksuvälineen haltija tai käyttäjä voi siirtää rahaa tai rahallista arvoa. Tietotekninen ohjelma tulee olla suojattu teknisin turvajärjestelyin, jolloin varojen siirto edellyttää käyttäjän tunnistamisen. Tunnistamistiedoilla tarkoitetaan yksilöiviä tietoja, joka voi olla PIN-koodi, salasana tai tunnusluku, joita yksin tai yhdessä tarvitaan varojen siirtoon[45]. Nordea määrittelee henkilöasiakkaiden tilien yleisissä ehdoissa, että maksuväline voi olla joko maksukortti tai pankin hyväksymät verkkopankkitunnukset. Oleellista on se, että niiden avulla voidaan antaa maksutoimeksiantoja, joista pankki ja asiakas ovat sopineet.[46]

Sähköinen maksutapa on siis maksutapa, jossa hyödynnetään sähköisiä kanavia, tällainen voi olla esimerkiksi verkko- tai mobiilipankissa tehty tilisiirto tai maksukortilla tehty maksusuoritus.

2.1.3 Vahva sähköinen tunnistaminen

Vahvasta sähköisestä tunnistamisesta on säädetty Euroopan komission ja neuvoston asetus sähköisestä tunnistamisesta ja sähköisiin palveluihin liittyvistä luottamuspalveluista sisämarkkinoilla[47]. Kyseinen asetus tunnetaan paremmin nimellä eIDAS-asetus, jota täydentää Suomessa kansallisesti säädetty laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009), myöh. tunnistuslaki).[48]

[45] HE 52/2021 vp, s. 57–58.
[46] Yleiset ehdot yksityishenkilöt 2024.
[47] Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014 , sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta
[48] Voutilainen 2020, s. 48–49.

Pankkien verkkopankkitunnukset täyttävät usein *vahvan sähköisen tunnistamisen* [49] vaatimukset, jolloin pankit ovat tunnistuslain 2 §:ssä tarkoitettuja tunnistuspalvelun tarjoajia [50]. Sähköisen tunnistamisen avulla kirjaudutaan esimerkiksi viranomaisten palveluihin, joita voivat olla esimerkiksi Verohallinnon tai Kelan palvelut. *Digitaalisiin palveluihin* [51] kirjautuneella käyttäjällä on oikeus saada kyseisen digitaalisen palvelun tietosisältö tai tehdä oikeustoimi digitaalisessa palvelussa [52].

Tunnistuspalvelulain 8 a §:n mukaan tunnistusmenetelmässä on käytettävä vähintään kahta seuraavista todentamistekijöistä:

> 1) tiedossa oloon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan tiedossaan;
> 2) hallussapitoon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan hallussaan;
> 3) luontaista todentamistekijää, joka perustuu johonkin luonnollisen henkilön fyysiseen ominaisuuteen.

Ensimmäisessä kohdassa voidaan tarkoittaa esimerkiksi PIN-koodia tai salasanaa. Toisessa kohdassa todentamistekijällä tarkoitetaan esimerkiksi mobiililaitetta, jossa on tunnistustoiminnallisuus, tunnuslukulaitetta tai sirullista henkilökorttia. Kolmannessa kohdassa luontaisella todentamistekijällä tarkoitetaan esimerkiksi kasvokuvaa tai sormenjälkeä. [53] Pankkien paperiset avainlukukortit eivät täytä yksinään vahvan

---

[49] Ks. Voutilainen 2020, s. 49. Vahvalla sähköisellä tunnistamisella tarkoitetaan henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnistustiedon aitouden sekä oikeellisuuden varmistamista sähköisesti. Tällöin käytettävän menetelmän on täytettävä EU:n sähköisestä tunnistamisesta ja luottamuspalveluista annetun asetuksen vaatimukset. Näihin vaatimuksiin kuuluu joko korotettu varmuustaso (artiklan 8, kohta 2, b alakohta) tai korkea varmuustaso (artiklan 8, kohta 2, c alakohta)

[50] Wuolijoki 2023, s. 358.

[51] Ks. Laki digitaalisten palvelujen tarjoamisesta (206/2019). Digitaalisella palvelulla tarkoitetaan lain mukaan verkkosivustoa tai mobiilisovellusta sekä niihin liittyviä toiminnallisuuksia.

[52] Voutilainen 2020, s. 48.

[53] Voutilainen 2020, s. 50.

tunnistamisen vaatimuksia, vaan tämän lisäksi tulee olla esimerkiksi matkapuhelimeen lähetettävä vahvistusviesti.

Jotta pankki voi myöntää asiakkaalleen tunnistusvälineen, tulee tunnistuslain 17 §:n mukaan tunnistusvälineen hakija tunnistaa henkilökohtaisesti tai sähköisesti. Tämä tarkoittaa sitä, että pankkien tulee varmistua henkilön henkilöllisyydestä joko viranomaisen myöntämästä asiakirjasta, jolla voidaan todentaa henkilöllisyys, tai henkilöllisyys tulee varmistaa vahvalla sähköisellä tunnistusvälineellä. Pelkkä ajokortti ei riitä siihen, että henkilölle voidaan myöntää verkkopankkitunnukset, jotka sisältävät mahdollisuuden vahvaan sähköiseen tunnistautumiseen[54]. Tunnistuslain 2 § 1 momentin 6 kohdan mukaan, tunnistusvälineen haltija on luonnollinen henkilö tai oikeushenkilö, jolle on sopimukseen perustuen myönnetty tunnistusväline tunnistuspalvelun tarjoajan toimesta.

Vahva sähköinen tunnistautuminen on merkittävässä roolissa, kun pankin asiakkaat tekevät digitaalisia maksutapahtumia ja niiden turvallisuudesta halutaan varmistua. Sähköinen tunnistaminen toimii eräänlaisena digitaalisena henkilöllisyystodistuksena, joka mahdollistaa muun muassa sähköisten transaktioiden suorittamisen.[55] Sähköisiä tunnistuspalveluita valvoo Suomessa Liikenne- ja viestintäviraston kyberturvallisuuskeskus, jonka mukaan Suomessa vahvoja sähköisiä tunnistuspalveluita ovat:

- pankkien verkkopankkitunnukset
- teleyritysten mobiilivarmenteet
- Digi- ja väestötietoviraston kansalaisvarmenne poliisin myöntämällä henkilökortilla ja eräät muut tunnistusvarmenteet
- erilaisilla organisaatiokorteilla rekisteröidyt tunnistusvälityspalvelut.[56]

[54] Wuolijoki 2023, s. 364–365.
[55] Electronic identification 2024.
[56] Sähköinen tunnistaminen 2025.

Tutkielmassa on tärkeää huomioida, että lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista soveltamisalaa koskevien säännösten perusteella lakia ei sovelleta tilanteisiin, joissa kyse on yhteisön sisäiseen tunnistamiseen tarkoitetuista palveluista. Käsiteltävissä tapauksissa on kuitenkin kyse asiakkaan maksuvälineen oikeudettomasta käytöstä aiheutuneesta vahingosta, minkä vuoksi vastuunjako asiakkaan ja pankin välillä määräytyy maksupalvelulain vastuusäännösten nojalla.

2.2 Pankin vahva sähköinen tunnistusväline

2.2.1 Pankkien tunnistusvälineiden nimet vaihtelevat

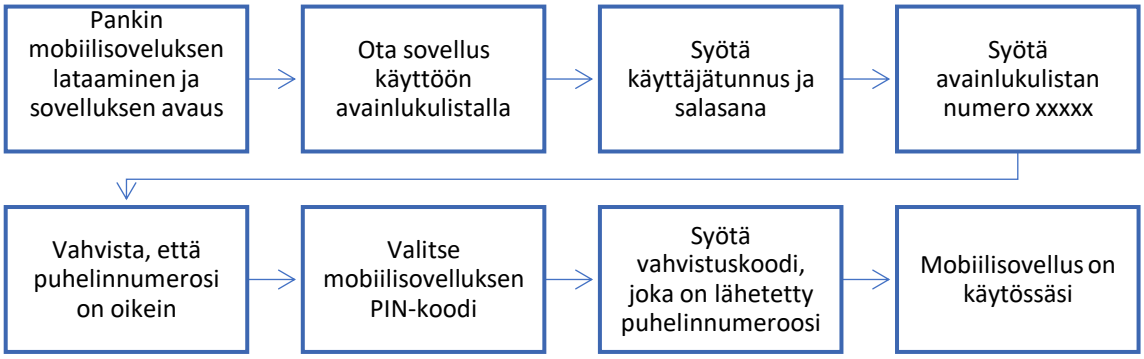
Mikäli rikolliset saavat haltuunsa pankin asiakkaan verkkopankkitunnukset, on heidän siinä tapauksessa mahdollista rekisteröidä käyttöönsä pankin mobiilisovellus, joka toimii henkilökohtaisena tunnistautumisvälineenä. Pankeilla voi olla erilaisia nimityksiä tunnistusvälineestä, jonka avulla on mahdollista esimerkiksi tunnistautua Kelan palveluihin tai vahvistaa maksuja verkkopankissa. Osuuspankki käyttää siitä nimitystä *Mobiiliavain* [57] , Nordea nimeä *Nordea ID -sovellus* [58] ja Säästöpankki nimitystä *Säästöpankki tunnistus*[59]*.* Säästöpankilla on erilliset mobiilisovellukset mobiilipankille sekä tunnistussovellukselle. Kaikilla näillä tunnistussovelluksilla on mahdollista tehdä samoja asioita, ja kaikki edellä mainitut tunnistusvälineet löytyvät Liikenne- ja viestintäviraston ylläpitämästä rekisteristä tunnistuspalveluiden tarjoajista. [60] Tutkielmassa puhutaan yleisesti ottaen *tunnistussovelluksesta*, kun tarkoitetaan tunnistautumisvälinettä, joka toimii älypuhelimella tai tabletilla. Tunnistussovellus voi olla samassa sovelluksessa kuin pankin mobiilisovellus, kuten Osuuspankilla on tai tunnistussovellus voi olla erillinen sovellus mobiilipankista.

---

[57] Mobiiliavain n.d.
[58] Mikä on Nordea ID -sovellus? n.d.
[59] Säästöpankki tunnistus n.d.
[60] ks. Sähköinen tunnistaminen n.d. Sivuston kohdasta ”Tunnistuspalvelurekisteri” löytyy listaus Liikenne- ja viestintävirasto ylläpitää rekisteriä Suomeen sijoittuneista vahvaa sähköistä tunnistamista tarjoavista palveluntarjoajista sekä niiden tarjoamista palveluista.

2.2.2 Mobiilisovelluksen käyttöönotto

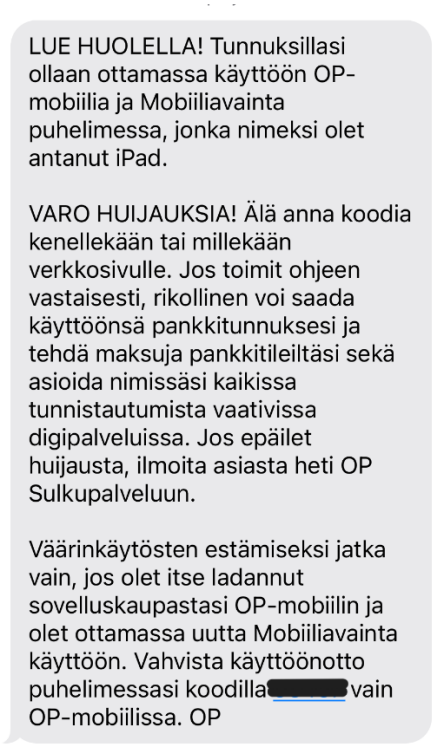
Pankeilla saattaa olla erilaisia prosesseja mobiilisovelluksen käyttöönotosta. Kuviossa 1 käydään läpi prosessi Osuuspankin OP-mobiilin ja Mobiiliavaimen käyttöönotosta. Käyttöönottoon vaaditaan OP-mobiilin lataaminen sovelluskaupasta ja sovelluksen asennus sovelluksen kautta tulevien ohjeiden mukaan. Sovelluksen käyttöönottoon tarvitaan internetin lisäksi verkkopankin käyttäjätunnus, salasana sekä avainlukulistan numerokoodi. Lisäksi matkapuhelimen tulee olla saatavilla, sillä siihen tulee käyttöönottoon liittyvä aktivointikoodi.



Kuvio 1. Pankin mobiilisovelluksen käyttöönoton vaiheet.[61]

Mobiilisovelluksen rekisteröinti on verrattain vaivaton ja nopea toimenpide, varsinkin jos lukee ohjeet hyvin ennakkoon ja tietää mitä rekisteröinti pitää sisällään. Mobiilisovelluksen rekisteröinnin yhteydessä rekisteröijä saa matkapuhelimeensa viestin (kuva 1), joka pitää sisällään koodin, jonka avulla mobiilisovelluksen rekisteröinti onnistuu. Viesti on sisällöltään varoittava ja itse koodi on vasta viestin lopussa. Osuuspankin viestissä kerrotaan mitä juuri sillä hetkellä ollaan tekemässä ja miten tulee toimia, jos ei ole itse ladannut kyseistä sovellusta sovelluskaupasta. Tämän lisäksi viestissä varoitetaan, mitä saattaa tapahtua, jos viestissä olevan koodin antaa rikollisille.

[61] Osuuspankin mobiilisovelluksen rekisteröinti omalle mobiililaitteelle 7.3.2025.



Kuva 1. Tekstiviesti, joka pitää sisällään mobiilisovelluksen rekisteröintiin vaadittavan koodin.

Rekisteröinnin jälkeen käyttäjällä on pääsy mobiilisovelluksen avulla mobiilipankkiin, jossa voi hoitaa verkkopankki- ja vakuutusasioita. Tämän lisäksi käyttäjä pystyy kirjautumaan Mobiiliavaimella verkkopankkiin sekä vahvistamaan verkko-ostosten maksut.[62]

FINE on yhdessä ratkaisussaan todennut, että asiakkaan olisi tullut kyseenalaistaa asiointinsa asianmukaisuus saatuaan pankin mobiilisovelluksen aktivointikoodin poikkeuksellisella tavalla tekstiviestitse. Viestin sisältö huomioiden hänen olisi pitänyt ymmärtää, ettei koodia tule syöttää verkkosivuilla varattuun kenttään, vaan noudattaa ohjeistusta ja olla yhteydessä pankkiin. Näin toimimalla vahinko, joka aiheutui pankkitunnusten oikeudettomasta käytöstä, olisi voitu estää. Pankkilautakunnan mukaan tekstiviesti oli sisällöltään selkeä, yksityiskohtainen ja informatiivinen. Siinä ohjeistettiin tarkasti, mihin tarkoitukseen aktivointikoodi oli tarkoitettu, ja varoitettiin

[62] OP-mobiili n.d.

asianmukaisesti väärinkäytösten varalta.[63] FINE toteaa ratkaisussaan, että asiakkaan pankilta saama viesti mobiilisovelluksen aktivointiin liittyen, on ollut hyvin yksityiskohtainen sisällöltään ja asiakkaan menettely on ollut kokonaisuudessaan arvioiden maksupalvelulaissa tarkoitettua törkeän huolimatonta. Pankkilautakunta suositti, että asiakas vastaa täysimääräisesti pankkitunnukset oikeudettomasta käytöstä ja aiheutuneesta vahingosta. Pankin mobiilisovelluksen aktivoinnilla ja aktivoinnin prosessilla voi olla merkittävä rooli, kun arvioidaan vastuunjakoa pankkitunnusten oikeudettomassa käytössä.

2.2.3 Sähköisen tunnistusvälineen säilyttäminen ja oikeudeton käyttö

Tunnistuslain 22 §:n mukaan tunnistusvälineen haltijan tulee käyttää tunnistusvälinettä ainoastaan sopimuksen ehtojen mukaisesti sekä huolehtia sen asianmukaisesta säilyttämisestä. Velvollisuus huolehtia tunnistusvälineestä alkaa, kun tunnistusvälineen käyttäjä on vastaanottanut sen.

Lain esitöissä on otettu huomioon se, että tavanomaiset tunnistusvälineet on yleensä tarkoitettu käytettäväksi usein ja näin ollen niitä saatetaan kuljettaa mukana. Sähköisen tunnistusvälineen säilyttämistä koskevaa huolellisuutta tarkastellaan kokonaisuutena. Lain esitöissä ei kuitenkaan ole otettu juurikaan kantaa sähköisen tunnistusvälineen luovuttamiseen kolmannelle osapuolelle kalastelusivujen tai muiden sähköisten palveluiden kautta. Pääpaino esitöissä on ollut fyysisten tunnusten säilyttämisessä. Tunnistuslain 22 §:n 2 momentin kohdassa, jossa käsitellään tunnusten luovuttamista, lain esitöissä todetaan, ettei tunnistusvälinettä tulisi luovuttaa toisen käyttöön[64].

Tunnistusvälineen haltijan vastuu sen oikeudettomasta käytöstä on rajattu. Tunnistuslain 27 § 1 momentin mukaan haltija vastaa välineen oikeudettomasta käytöstä vain silloin,

---

[63] FINE-043423.
[64] He 36/2009 vp, s. 60.

kun hän on itse luovuttanut sen toiselle, jos välineen katoaminen, joutuminen ulkopuoliselle tai oikeudeton käyttö johtuu hänen huolimattomuudestaan, joka ei ole lievää, taikka jos hän on laiminlyönyt ilmoittaa välineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai sen oikeudettomasta käytöstä ilman aiheetonta viivytystä havaittuaan tilanteen.

Tunnistuslain 27 §:n 2 momentissa vastuulle asetetaan kuitenkin myös selkeitä rajoja. Haltija ei vastaa välineen oikeudettomasta käytöstä siltä osin kuin käyttö tapahtuu sen jälkeen, kun hän on tehnyt asianmukaisen ilmoituksen tunnistuspalvelun tarjoajalle. Vastuu ei myöskään synny, jos haltijalla ei ole ollut tosiasiallista mahdollisuutta tehdä ilmoitusta viipymättä palveluntarjoajan laiminlyönnin vuoksi. Lisäksi haltija vapautuu vastuusta tilanteissa, joissa palveluntarjoaja on itse jättänyt noudattamatta velvollisuuttaan tarkistaa välineeseen liittyviä käyttörajoituksia tai sen estämistä koskevia tietoja.

Tunnistusvälineen luovutuksella tarkoitetaan vapaaehtoista hallinnan luovutusta, missä tarkoituksessa tahansa[65]. Rikollisten kalastellessa pankkitunnuksia, on huomionarvoista arvioida sitä, missä tilanteessa pankin asiakas on luovuttanut verkkopankkitunnukset rikollisten haltuun. Jotta pankin asiakas on vastuussa pankkitunnusten oikeudettomasta käytöstä, tulee pankkitunnusten joutua oikeudettomasti toisen haltuun ja käytettäväksi siitä syystä, että pankin asiakas on ollut huolimaton tavalla, joka on lievää vakavampaa. Pankin asiakas ei ole vastuussa pankkitunnusten oikeudettomasta käytöstä, mikäli hän on toiminut tunnistuslain 27 § 2 momentin mukaisella tavalla.

[65] HE 36/2009 vp, s. 64.

2.3 Maksuvälineen oikeudeton käyttö mobiilisovelluksella – vastuukysymyksen lähtökohta

2.3.1 Maksupalvelun käyttäjä, palveluntarjoaja ja maksaja

Maksupalvelun käyttäjän ja palveluntarjoajan määritelmistä säädetään maksupalvelulaissa. Maksupalvelulain 8 §:n 1 momentin mukaan maksupalvelun käyttäjä on se, joka on tehnyt palveluntarjoajan kanssa sopimuksen, että voi käyttää maksupalvelua maksajana tai maksunsaajana. Palveluntarjoaja on puolestaan taho, joka tuloa tai muuta taloudellista hyötyä saadakseen tarjoaa maksupalveluita ammatillisessa tarkoituksessa.

Maksajalla tarkoitetaan maksupalvelulain 8 §:n 1 kohdan mukaan maksupalvelun käyttäjää, joka voi palveluntarjoajan kanssa tehdyn sopimuksen perusteella käyttää maksupalvelua maksajana tai maksunsaajana.

2.3.2 Maksuvälineen oikeudeton käyttö

Maksupalvelulain 38 §:n mukaan maksutapahtuma saadaan toteuttaa vain maksajan suostumuksella. Mikäli maksaja ei anna suostumusta sovitulla tavalla, pidetään maksutapahtumaa oikeudettomana. Lain esitöiden mukaan ”sovitulla tavalla” tarkoittaa sekä suostumuksen antamista että muotoa.[66] Esimerkkinä voidaan mainita tilanne, jossa pankin asiakas siirtää varoja tuttavalleen. Vaikka myöhemmin paljastuisi, että tuttava on toiminut petollisesti, ei tällaista tilisiirtoa pidetä oikeudettomasti tehtynä. Tämän kaltaisessa tapauksessa asiakas on itse vastuussa maksutapahtuman toteuttamisesta.[67]

Pankkilautakunta FINEn ratkaisukäytännössä on vakiintuneesti katsottu, että tilanteissa, joissa rikoksen uhri on huijauksen seurauksena itse hyväksynyt riidanalaiset maksut

[66] HE 169/2009 vp, s. 58.
[67] Wuolijoki 2023, s. 360—361.

esimerkiksi mobiilisovelluksessaan ja maksun tiedot ovat olleet nähtävissä ennen vahvistusta, pankkia ei ole suosittu korvaamaan asiakkaalle aiheutunutta vahinkoa. Vaikka asiakas on toiminut rikollisten harhaanjohtamana, hänen on katsottu kuitenkin antaneen maksuille maksupalvelulain 38 §:ssä ja ehdoissa tarkoitetun suostumuksensa. Näin ollen maksutapahtumia ei ole pidetty maksupalvelulaissa tarkoitettuina oikeudettomina, eikä pankille ole muodostunut vastuuta aiheutuneesta vahingosta. Pankkilautakunta on menetellyt edellä mainitulla tavalla muun muassa ratkaisuissa FINE-65394-H0X4X.

Tapauksissa, joissa rikolliset ovat saaneet haltuunsa asiakkaan verkkopankkitunnukset ja ottaneet käyttöön pankin mobiilisovelluksen maksujen vahvistamista varten, ei asiakkaan katsota antaneen suostumustaan maksuihin. Koska maksujen vahvistamiseen tarvittava tunnistusväline on rikollisten hallussa, asiakkaan oma suostumus maksuihin puuttuu. Sen sijaan, jos petolliset maksut olisi vahvistettu asiakkaan omassa puhelimessa olevalla tunnistussovelluksella, olisi arvioitava myös sitä, onko asiakas antanut maksuille suostumuksensa.

3 Pankin ja asiakkaan välinen sopimussuhde vastuunjaon määrittäjänä

3.1 Yleistä sopimuksista ja oikeustoimista

Oikeudellisessa kielenkäytössä sopimus-termiä käytetään useassa merkityksessä. Ensinnäkin sillä voidaan tarkoittaa itse sopimuksen syntymistä eli hetkeä, jolloin osapuolet sitoutuvat sopimusoikeudellisesti toisiinsa. Toiseksi sopimus voi viitata kirjalliseen asiakirjaan, johon sopimusehdot on koottu. Kolmanneksi sopimus käsittää osapuolten välisen oikeussuhteen sisällön eli heidän velvoitteensa ja niihin liittyvät oikeudet.[68]

Sama sopimuksen monimerkityksisyys näkyy myös pankki–asiakassuhteessa. Ensinnäkin asiakas tulee sopimusoikeudellisesti sidotuksi, kun hän hyväksyy pankin tarjoamat palvelut ja niiden ehdot. Toiseksi sopimus ilmenee kirjallisina asiakirjoina, kuten tili-, kortti- ja lainasopimuksina, joihin ehdot on kirjattu. Kolmanneksi sopimus konkretisoituu oikeussuhteena, joka sisältää molemminpuolisia velvoitteita ja oikeuksia. Asiakkaalla on esimerkiksi velvollisuus käyttää palveluita ehtojen mukaisesti, ja pankilla vastaavasti velvollisuus huolehtia varojen säilyttämisestä ja maksujen toteuttamisesta. Nämä sopimuksen eri ulottuvuudet korostuvat tilanteissa, joissa tapahtuu väärinkäytös ja joudutaan arvioimaan pankin ja asiakkaan välistä korvausvastuuta.

Pankin ja asiakkaan välinen sopimus on oikeustoimi[69], jotka ovat yleisesti ottaen vakiosopimuksia. Vakiosopimukset ovat yleisiä vakuutus-, pankki- ja arvopaperitoimialoilla. Vakiosopimusehdot tunnetaan myös nimellä ”yleiset sopimusehdot”.[70]

---

[68] Saarnilehto & Annola 2018, s. 4.
[69] Ks. Saarnilehto & Annola 2018, s. 7–8. Sopimus on kaksipuolinen oikeustoimi, joka edellyttää kahden osapuolen tahdonilmaisua ja muodostuu tyypillisesti tarjouksesta ja sitä seuraavasta hyväksymisestä. Oikeustoimi on tahdonilmaisu, jolla pyritään luomaan muuttamaan tai päättämään oikeussuhde. Oikeustoimen syntyminen edellyttää vapaaehtoisen tahdonilmaisun.
[70] Hemmo & Hoppu 2006.

Tässä tutkielmassa sopimuksen teon oikeussubjekteina toimivat yksityiset ihmiset eli luonnolliset henkilöt ja toisena sopijaosapuolena toimii yksityisoikeudellinen oikeushenkilö eli pankki.[71] Tutkielmassa käsiteltäviä sopimuksia ovat muun muassa:

- Nordea: Pankkitunnuksilla käytettävien palveluiden yleiset sopimusehdot,
- Nordea: Tilin yleiset ehdot ja
- Osuuspankki: OP:n tunnus- ja digisopimuksen ehdot.

3.2 Pankin ja asiakkaan välillä vallitsee sopimussuhde

Pankin ottaessa vastaan asiakkaalta talletusta, tulee pankilla ja tilinavaajan välillä olla sopimus. Tällaista sopimusta kutsutaan yleensä tili- tai talletussopimukseksi, joka on tehtävä kirjallisesti tai sähköisesti. Tilisopimus pitää yleensä sisällään sopimusasiakirjan, tilimuotoa koskevat yleiset ehdot sekä palveluhinnaston.[72]

Pankin ja asiakkaan väliset tilisopimukset jaetaan usein käyttäjäryhmien perusteella. Vaikka tilit ovat usein perusominaisuuksiltaan samanlaisia, jaetaan tilisopimukset kuluttaja-asiakkaiden ja yritys- sekä muiden yhteisöasiakkaiden tilisopimuksiin. Tämä johtuu siitä, että kuluttaja-asiakkaat mielletään selvästi heikompaan asemaan suhteessa pankkiin, ja kuluttaja-asiakkaita koskee maksupalvelulain pakottavat säännökset. Kuluttaja-asiakkaat ovat usein eri asemassa verrattuna yrityksiin, kun tarkastellaan tiliehtojen kohtuullisuusarviointia. [73]

Maksupalvelulain 8 §:ssä säädetään, että puitesopimuksella tarkoitetaan tili- tai muuta sopimusta, jonka perusteella voidaan toteuttaa yksittäisiä tai peräkkäisiä

[71] Saarnilehto & Annola 2018, s. 26–35.
[72] Wuolijoki 2023, s. 185–186.
[73] Wuolijoki 2023, s. 174.

maksutapahtumia. Mikäli kyseessä ei ole *maksutili*[74], sovelletaan maksupalvelulain sijaan tilityyppiin kuuluvaa erityissääntelyä, kuluttajansuojalain yleissääntelyä ja Finanssivalvonnan ohjeistuksia[75]. Tutkielmassa lähtökohtana on se, että asiakkaille on avattu maksu- tai perusmaksutili ja näin ollen yksi sovellettavista laeista on maksupalvelulaki.

3.3 Hyvä pankkitapa ja asiakkaan tuntemisvelvoite pankkitoiminnan keskeisinä velvoitteina

Hyvä pankkitapa ja asiakkaan tuntemisvelvoite muodostavat yhdessä keskeisen oikeudellisen ja eettisen perustan, jolle moderni pankkitoiminta rakentuu. Hyvä pankkitapa luo periaatteet, asiakkaan tunteminen taas konkretisoi riskiperusteiset velvollisuudet.

Laki luottolaitostoiminnasta (610/2014) 15 luku 1 §:ssä säädetään, että luottolaitosten tulee noudattaa hyvää pankkitapaa. Hyvä pankkitapa on pankkitoimintaa ohjaava periaatteellinen kehys, joka täydentää lainsäädäntöä ja viranomaisten määräyksiä. Sen keskeisenä tavoitteena on ylläpitää ja vahvistaa luottamusta pankkijärjestelmään sekä varmistaa toiminnan avoimuus ja pitkäjänteinen kestävyys. Hyvään pankkitapaan sisältyvät ohjeet ja käytännöt määrittelevät, millaista pankkien asiakaslähtöisen ja vastuullisen toiminnan tulisi olla, ja samalla ne täsmentävät pankkien roolia laajemmassa yhteiskunnallisessa kontekstissa. [76] Hyvä pankkitapa voidaan siten ymmärtää sekä eettisiä periaatteita sisältävänä normistona että käytännön toimintaa ohjaavana tulkintakehyksenä, joka antaa suuntaa tilanteissa, joissa lainsäädäntö ei tarjoa yksityiskohtaista ratkaisua.

---

[74] Ks. Maksupalvelulaki 1 luku 8 § 1mom. 5 kohta. Maksutilillä tarkoitetaan tiliä, jota voidaan käyttää maksutapahtumiin.
[75] Wuolijoki 2023, s. 187–188.
[76] Hyvä pankkitapa 2025.

Pankkien ja asiakkaiden välistä suhdetta säätelevät ensisijaisesti lait sekä valvontaviranomaisten antamat määräykset ja ohjeet. Hyvän pankkitavan noudattamisen vaatimus on kirjattu myös lainsäädäntöön, mikä korostaa sen sitovuutta ja merkitystä. Vaikka hyvän pankkitavan periaatteet eivät muuta asiakkaan ja pankin välisiä sopimuksia, ne toimivat käytännön ohjenuorana tilanteissa, joissa laki ei anna yksityiskohtaista ratkaisua tai joissa korostuu pankin velvollisuus toimia luotettavasti ja asiakkaan etua huomioiden.[77]

Hyvän pankkitavan periaatteiden tarkoituksena on myös tehdä näkyväksi se arvopohja, johon pankkitoiminta nojaa. Asiakkaiden, henkilöstön ja muiden sidosryhmien näkökulmasta ne luovat selkeyttä ja ennustettavuutta. Pankkien vastuullisuus ei tällöin rajoitu pelkkään sääntelyn minimivaatimusten täyttämiseen, vaan sisältää myös eettisen velvoitteen toimia rehellisesti, tasapuolisesti ja pitkäjänteisesti. Näin hyvä pankkitapa tukee paitsi yksittäisen asiakkaan oikeusturvaa myös koko rahoitusjärjestelmän vakautta ja legitimiteettiä.[78]

Hyvän pankkitavan noudattaminen ei rajoitu vain henkilöasiakkaisiin, vaan hyvän pankkitavan noudattaminen koskee kaikkia asiakasryhmiä. [79] Erityisesti tallettajan aseman turvaaminen ja asiakkaan edun korostaminen ovat periaatteita, jotka havainnollistavat pankkien vahvempaa asemaa ja sen myötä syntyvää korostunutta huolellisuusvelvoitetta

Pankilla on lisäksi lakisääteinen velvollisuus ehkäistä rahanpesua ja terrorismin rahoittamista. Yksi keskeinen velvoite on asiakkaan *tunnistaminen*[80] ja *tunteminen*[81],

---

[77] Hyvä pankkitapa 2025.
[78] Hyvä pankkitapa 2025.
[79] Wuolijoki 2022, s. 97.
[80] Ks. Wuolijoki 2022, s. 115. Asiakkaan tunnistamisella tarkoitetaan asiakkaan henkilöllisyyden todentamista.
[81] Ks. Määräykset ja ohjeet 2/2023 Rahanpesun ja terrorismin rahoittamisen estäminen. Finanssivalvonta. Asiakkaan tuntemisella tarkoitetaan rahanpesulain 3 luvussa säädettyjä toimenpiteitä, joita ovat: asiakkaan tunnistamine ja henkilöllisyyden todentaminen, tietojen kerääminen asiakkaasta asiakkaan ja tämän toiminnan tuntemiseksi sekä asiakassuhteen jatkuva seuranta, tuntemistietojen päivittäminen ja selonottovelvollisuus.

josta säädetään rahanpesusta ja terrorismin rahoittamisen estämisestä (444/2017) eli rahanpesulassa. Lisäksi laissa luottolaitostoiminnasta (610/2014) 15 luvun 18 §:ssä säädetään, että luottolaitosten tulee tuntea ja tunnistaa asiakkaat tai asiakkaiden lukuun toimiva tosiasiallinen edunsaaja. Asiakkaan tuntemisen tarkoituksena on varmistaa, että pankilla on riittävät tiedot asiakkaan toiminnasta ja sen luonteesta, jotta mahdolliset väärinkäytökset ja rahanpesun riskit voidaan havaita. Asiakkaan tuntemisvelvoite on siten keskeinen osa pankkien riskiperusteista toimintamallia ja toiminnan lainmukaista perustaa.

Rahanpesulain 3 luvun 3 §:n mukaan, asiakkaista kerättävien tietojen ja asiakirjojen tulee olla ajantasaisia sekä olennaisia. Mikäli pankki ei pysty toteuttamaan asiakkaan tuntemista riittävässä laajuudessa, se ei saa ylläpitää liikesuhdetta tai toteuttaa maksutapahtumaa. Pankki voi riskiperusteisesti rajoittaa tai sulkea asiakkaalta tiettyjä palveluita, mikäli puutteet asiakkaan tuntemistiedoissa ovat olennaisia.[82] Tämä korostaa sitä, että asiakkaan tunteminen ei ole muodollinen velvoite, vaan edellytys asiakassuhteen jatkamiselle ja pankkitoiminnan lainmukaisuudelle.

Rahanpesulain 3 luvun 4 §:n nojalla pankkien tulee seurata asiakkaiden ilmoittamia tuntemistietoja näiden tosiasialliseen käyttäytymiseen. Usein pankeilla on apuna erilaisia monitorointijärjestelmiä, joiden avulla pankit pystyvät vertaamaan asiakkaan antamia tietoja todellisiin tietoihin. Mikäli asiakkaan toiminta poikkeaa ilmoitetusta, tulee pankkien täyttää lain edellyttämä selonottovelvollisuus ja tiedustella asiakkaalta tarkempia tietoja maksutapahtumaan liittyen. Pelkkä tietojen kerääminen ei riitä, vaan pankin tulee kyetä analysoimaan ja arvioimaan asiakkaan toimintaa jatkuvasti. Asiakkailta kerättävistä tuntemistiedoista ei ole kovin paljoa hyötyä, mikäli tuntemistietoja ei pystytä vertaamaan asiakkaan todelliseen käyttäytymiseen.[83]

[82] Wuolijoki 2022, s. 117.
[83] Wuolijoki 2022, s. 118.

Mikäli pankilla on käytössään reaaliaikainen maksumonitorointi, saattaa sillä olla kyky havaita poikkeavia maksuja ja pysäyttää tai estää kyseiset maksut. Asiakkaalta on mahdollista tiedustella pysähtyneistä maksuista, onko hän itse tehnyt kyseisen maksun vai onko joutunut mahdollisen rikoksen uhriksi. Maksujen pysäyttäminen saattaa aiheuttaa harmistusta asiakkaissa, mutta pankilla on lakiin perustuva velvollisuus kieltäytyä tietyistä liiketoimista. Maksujen pysäyttämisen perusteena on joko tiliehdoissa mainittu pankin oikeus estää tilinkäyttö väärinkäytöstilanteissa tai pysäyttäminen perustuu rahanpesulain 4 luvun 5 §:ään, jonka mukaan ilmoitusvelvollisen on keskeytettävä liiketoimi tai kieltäydyttävä siitä, jos se on epäilyttävä tai pankki epäilee, että liiketoimeen sisältyviä varoja käytetään terrorismin rahoittamiseen. Vaikka pankit saavat tehdä aktiivista petostorjuntatyötä, ei pankeilla ole velvollisuutta reaaliaikaiseen maksuliikenteen monitorointiin, ainakaan nykylainsäädännön valossa[84].

Asiakkaan tunteminen tukee myös petosten torjuntaa. Tuntemalla asiakkaansa pankit voivat havaita poikkeavuuksia maksuliikenteessä sekä varmistua asiakkaiden oikeista henkilöllisyyksistä. Laadukkaat tuntemisprosessit auttavat tunnistamaan korkeampiriskiset asiakkaat ja kohdentamaan valvontaa tarkoituksenmukaisesti. Asiakkaan tuntemisvelvoitteen asianmukainen toteuttaminen toimii siten sekä rahanpesun estämisen että laajemman talousrikollisuuden torjunnan keskeisenä työkaluna. Se mahdollistaa normaalin ja poikkeavan toiminnan erottamisen ja tukee pankkien velvollisuuksia suojata sekä omaa toimintaansa että asiakkaiden varoja väärinkäytöksiltä.

[84] Wuolijoki 2022, s. 120.

3.4 Pankilla on runsaasti velvollisuuksia

3.4.1 Pankkitoiminnan sääntelyn perusteet ja tarkoitus

Pankkitoiminnan sääntelyn tarpeellisuus johtuu pankkialan erityispiirteistä ja sen keskeisestä roolista yhteiskunnassa. Pankit toimivat keskeisinä toimijoina, jotka myöntävät luottoja kotitalouksille ja yrityksille, vastaanottavat talletuksia, tarjoavat sijoituspalveluita sekä vastaavat maksuliikenteen sujuvuudesta. Näiden toimintojen häiriintyminen voi aiheuttaa laajamittaisia vaikutuksia koko yhteiskuntaan.[85] Lisäksi pankit ovat kuluttaja-asiakkaaseen nähden vahvemmassa asemassa, tämä vuoksi pankkitoimintaa koskevassa sääntelyssä on säännöksiä, jotka koskevat asiakkaiden kohtelua ja heille tarjottavien palveluiden ehtoja[86]

Johtuen runsaasta sääntelystä, on pankkien sekä pankin asiakkaiden oikeuksista ja velvollisuuksista säädetty melko tarkasti. Velvollisuudet ja oikeudet luovat raamit sille, miten asiakkaan tai pankin tulee tietyissä tilanteissa toimia, esimerkiksi silloin, kun pankin asiakkaan verkkopankkitunnukset ovat päätyneet rikollisten haltuun tai kun kuluttaja-asiakas haluaa avata peruspankkipalvelut. Verkkopankkitunnusten joutuminen väärin käsiin, voi aiheuttaa merkittäviä taloudellisia menetyksiä, tästä syystä on tärkeää, että pankit sekä niiden asiakkaat tietävät, miten toimia näissä tilanteissa, jotta väärinkäytöksestä johtuvat mahdolliset varojen menetykset voidaan minimoida.

3.4.2 Pankin velvollisuus tarjota kuluttaja-asiakkaille peruspankkipalvelut

Sopimusoikeudellisesti sopimusvapauteen kuuluu oikeus valita sopimuskumppani vapaasti. Kuluttaja-asiakkailla on kuitenkin oikeus peruspankkipalveluihin, mikä tarkoittaa sitä, että pankilla on sopimuspakko, jos kuluttaja-asiakas täyttää tarvittavat ehdot.[87]

---

[85] Wuolijoki 2022, s. 3.
[86] Wuolijoki 2022, s. 7.
[87] Wuolijoki 2022, s. 98.

Luottolaitostoiminnasta annetun lain (610/2014) 15 luvun 6 §:ssä säädetään, että *talletuspankkien*[88] tulee tarjota maksutiliä, maksupalveluita ja sähköisen tunnistamisen palveluita *ETA-valtioissa* [89] laillisesti asuville, ilman, että ketään syrjitään. Tätä tiliä kutsutaan perusmaksutiliksi. Perusmaksutilihakemus tulee hyväksyä tai hylätä viimeistään 10 pankkipäivän kuluessa siitä, kun hakemus on otettu vastaan. Talletuspankki voi evätä perusmaksutilin avaamisen ja siihen liittyvien maksupalveluiden tarjoamisen ainoastaan, jos päätös perustuu rahanpesun ja terrorismin rahoittamisen estämisestä annettuun lakiin (444/2017) tai eräiden Suomelle Yhdistyneiden Kansakuntien ja Euroopan unionin jäsenenä kuuluvien velvoitusten täyttämisestä annettuun lakiin (659/1967). Lähtökohta on se, että talletuspankkien tulee avata ehdot täyttävälle henkilölle perusmaksutili ja pankki voi kieltäytyä tilin avaamisesta vain painavin syin.

Perusmaksutilin vähimmäispalveluita ovat tilin avaaminen, käyttäminen ja sulkeminen sekä varojen tallettaminen ja nostaminen ETA-alueella. Tämän lisäksi perusmaksutilin käyttäjän tulee voida tehdä maksutapahtumia suoraveloituksina, maksukortilla, tilisiirrolla, pankkipäätteellä luottolaitoksen toimipisteessä ja luottolaitoksen verkkopalvelussa. Perusmaksutilin palveluita tarjoavalla pankilla on myös velvollisuus tarjota asiakkaalle vahvaa sähköistä tunnistuspalvelua.[90]

Vahvan sähköisen tunnistamisen ja verkkopankkitunnusten avulla pankin asiakas voi ottaa käyttöönsä pankin mobiilisovelluksen, jonka avulla on mahdollista tunnistautua eri palveluihin.

---

[88] Laki luottolaitostoiminnasta 1 luku 7 § 1 mom. Talletuspankilla tarkoitetaan luottolaitosta, jonka toimilupa oikeuttaa vastaanottamaan yleisöltä talletuksia.
[89] Euroopan talousalue 2022. Euroopan talousalueeseen (ETA) kuuluvat Euroopan unionin jäsenmaiden lisäksi Islanti, Liechtenstein ja Norja.
[90] Wuolijoki 2023, s. 177–178.

3.4.3 Pankin tiedonantovelvollisuus vaikuttaa huolimattomuuden arviointiin

Tiedonantovelvollisuuden täyttäminen on tutkielman kannalta keskeinen kysymys, sillä sen laajuus ja toteutuminen vaikuttavat siihen, miten asiakkaan huolimattomuutta voidaan arvioida verkkohuijaustapauksissa.

Pankin tiedonantovelvollisuus on osa laajempaa *informointivelvollisuuden* käsitettä, johon kuuluu neuvonta[91] ja tiedonanto. Tässä tutkielmassa tiedonantovelvollisuus on keskeisessä asemassa ja sillä tarkoitetaan standardisoitua informaatiota, joka voidaan toimittaa kaikille sitä tarvitseville asiakkaille samassa muodossa tai samalla tavalla koostettuna.[92] Täten pankki varmistaa, että asiakas saa ymmärrettävää, oikea-aikaista ja päätöksenteon kannalta olennaista tietoa.

Pankeilla on standardisoitu tiedonantovelvollisuus, josta säädetään maksupalvelulain 10–18 §:ssä. Tehtäessä tilisopimusta pankin asiakkaalle annetaan tilinavaamista harkittaessa vakiomuotoinen lomake, joka pitää sisällään tiliehdot ja muut tarvittavat tiedot. Lainsäädäntö edellyttää aktiivista tiedonantotapaa, eli tiedot tulee antaa henkilökohtaisesti, eikä maininta ”katso verkkosivuilta” ole riittävä.[93]

Maksupalvelulain 12 §:n mukaan maksupalvelusta ja maksutilistä tulee antaa riittävästi tietoja, kuten kuvaus maksupalvelun pääominaisuuksista, miten maksupalvelun käyttäjä voi antaa suostumuksen maksutoimeksiannon käynnistämisestä sekä maksupalvelun käyttäjältä perittävien kulujen yhteismäärästä.

Viestinnästä annettavat tiedot käydään läpi maksupalvelulain 13 §:ssä, jonka mukaan tieto tulee antaa viestintävälineestä, jota käytetään tietojen antamiseen ja ilmoitusten tekemiseen. Lisäksi pykälässä velvoitetaan antamaan tieto siitä, millä kielellä

---

[91] Ks. Wuolijoki 2009, s. 30. Neuvonta on jalostetumpaa informaatiota kuin tieto ja neuvontavelvollisuus on juuri asiakkaan tarpeeseen ja tilanteeseen sopivan tiedon antamista.
[92] Wuolijoki 2009, s. 30.
[93] Wuolijoki 2023, s. 187–188.

puitesopimus on tarkoitus tehdä ja miten usein maksupalvelulaissa tarkoitetut tiedot tulee antaa maksupalvelun käyttäjälle.

Maksupalvelulain 14 § on maksupalvelun käyttäjän pankkiturvallisuuden kannalta merkittävä. Lainkohdassa kerrotaan varotoimista, vastuukysymyksistä ja oikeussuojakeinoista annettavista tiedoista. Puitesopimuksessa tulee kertoa, millaisiin toimiin maksuvälineen haltijan tulee ryhtyä pitääkseen maksuvälineen turvassa, miten palveluntarjoajalle tehdään ilmoitus maksuvälineen katoamisesta, sen joutumisesta oikeudettomasti toisen haltuun tai sen oikeudettomasta käytöstä. Puitesopimuksessa tulee myös ilmaista, mikäli palveluntarjoaja ilmoittaa maksupalvelun käyttäjälle petollisesta toiminnasta tai estää maksupalvelun käytön tietyin edellytyksin. Lisäksi tulee antaa tieto maksupalvelun käyttäjän vastuusta maksupalvelun oikeudettomasta käytöstä.

Maksupalvelulaissa säädetään kattavasti tiedoista, joita puitesopimukselta vaaditaan ja mitä asioita siihen tulee kirjata.

3.4.4 Tiedonantovelvollisuus maksujensiirrossa

Mikäli kyseessä on puitesopimukseen perustuva maksutapahtuma, säädetään palveluntarjoajan tiedonantovelvollisuudesta maksupalvelulain 18–19 §:ssä. Puitesopimuksen tekeminen ei siis päätä pankin informaatiovelvollisuutta, vaan velvollisuus on jatkuva. Palveluntarjoajan tulee maksupalvelulain 18 §:n mukaan maksajan pyynnöstä antaa tiedot siitä, minkä ajan kuluessa maksutapahtuma toteutetaan ja mitä kuluja maksajalta peritään.

Maksupalvelulain 19 §:n mukaan maksajalle tulee antaa tiedot puitesopimuksen nojalla toteutetuista maksutapahtumista. Tiedoista tulee käydä ilmi muun muassa maksun yksilöivä tieto ja maksun saaja, maksun määrä siinä valuutassa, jolla maksajan tiliä veloitetaan sekä maksajalta perittävien kulujen tai korkojen määrä. Tavoitteena on, että asiakas kykenee havaitsemaan poikkeamat, kuten oikeudettomat maksutapahtumat,

mahdollisimman aikaisessa vaiheessa. Käytännössä tämä tiedonantovelvollisuus toteutetaan tiliotteella, jonka toimittamisesta sovitaan tilisopimuksessa. Tiliote voitaan toimittaa myös sähköisesti.[94]

3.4.5 Pankin velvollisuus sulkea maksuväline

Maksupalvelulain 56 §:ssä velvoitetaan palveluntarjoaja estämään maksuvälineen käyttö, kun maksuvälineen haltija on ilmoittanut maksuvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai maksuvälineen oikeudettomasta käytöstä. Hallituksen esityksen mukaan maksuvälineen haltijan ei ole pakko tehdä ilmoitusta, vaan ilmoituksen voi tehdä myös esimerkiksi maksuvälineen haltijan laillinen edustaja tai hänen tehtävään valtuuttamansa henkilö. Lisäksi hallituksen esityksessä todetaan, että palveluntarjoajan huolelliseen toimintaan kuuluu, että maksuväline suljetaan mahdollisimman pian ilmoituksen jälkeen. [95] Kun ilmoitus maksuvälineen oikeudettomasta käytöstä on tehty palveluntarjoajalle, katkeaa maksupalvelulain 62 §: 3 momentin 1 kohdan mukainen vastuu maksuvälineen oikeudettomasta käytöstä. Ilmoituksen jälkeen palveluntarjoaja on vastuussa sulkea maksuväline mahdollisimman nopeasti.[96]

Mikäli pankki on saanut asiakkaalta ilmoituksen sulkea maksuväline eli esimerkiksi verkkopankkitunnukset, koska ne ovat joutuneet oikeudettomasti rikollisten haltuun, siirtyy vastuu mahdollisista väärinkäytöksistä ilmoituksen jälkeen pankille.

---

[94] Wuolijoki 2023, s. 303.
[95] HE 169/2009 vp, s. 70.
[96] HE 169/2009 vp, s. 70.

3.5 Pankilla on myös oikeuksia

LLL 15 luvun 6 b §:n mukaan pankilla on oikeus purkaa perusmaksutiliä koskeva puitesopimus vain tietyin tarkkaan rajatuin edellytyksin. Pankki saa purkaa perusmaksutiliä koskevan puitesopimuksen, mikäli tiliä on käytetty laittomaan tarkoitukseen tai asiakas on antanut virheellistä tietoa tai jättänyt tietoja antamatta, jotka olisivat johtaneet perusmaksutilihakemuksen hylkäämiseen.

Pankki saa irtisanoa LLL 15 luvun 6 b §:ään perustuen perusmaksutiliä koskevan puitesopimuksen vain, jos tilillä ei ole ollut tapahtumia 24 peräkkäiseen kuukauteen tai asiakas ei asu enää laillisesti ETA-valtiossa. Irtisanomisesta tulee ilmoittaa asiakkaalle kirjallisesti vähintään kaksi kuukautta ennen kuin irtisanominen tulee voimaan. Irtisanomisen ilmoittamisesta voidaan poiketa vain, jos se olisi kansallisen turvallisuuden tai yleisen järjestyksen vastaista.

Mikäli asiakkaan perusmaksutilin puitesopimus on irtisanottu tai purettu, tulee pankin LLL 15 luvun 6 b §:n mukaan ilmaista asiakkaalle selkeästi, että hänellä on mahdollisuus valittaa asiasta sekä asiakas voi olla yhteydessä toimivaltaiseen viranomaiseen ja vaihtoehtoiseen riidanratkaisuelimeen.

Maksupalvelulain 57 §:n mukaan pankilla on oikeus sulkea maksuväline, mikäli osapuolet ovat puitesopimuksessa näin sopineet. Oikeus estää maksuvälineen käyttö rajoittuu tilanteisiin, joissa maksuvälineen käytön turvallisuus on vaarantunut tai on syytä epäillä, että maksuvälinettä käytetään oikeudettomasti tai vilpillisesti. Tämän lisäksi pankilla on oikeus estää maksuvälineen käyttö tilanteissa, joissa maksuväline oikeuttaa luoton käyttöön ja on vaara siitä, että luoton maksamisesta vastuussa oleva maksupalvelun käyttäjä ei kykene täyttämään maksuvelvoitettaan. Tilanteet, joissa pankki voi sulkea maksuvälineet, ovat esimerkiksi tapaukset, joissa pankki havaitsee maksumonitoroinnissaan poikkeavia tapahtumia, jonka perusteella on syytä epäillä maksuvälineen käytön turvallisuuden vaarantuminen.

Palveluntarjoajalla on oikeus sulkea maksuväline silloin, kun se epäilee, että maksuvälinettä käyttää joku muu, kuin sen laillinen haltija. Maksuväline voidaan sulkea myös silloin, kun maksuvälineen haltija käyttää maksuvälinettä vilpillisellä tavalla. Palveluntarjoajalla tulee olla objektiivisesti perusteltu syy epäillä oikeudetonta tai vilpillistä maksuvälineen käyttöä. [97] Maksupalvelulain 57 § 2 momentti velvoittaa palveluntarjoajan ilmoittamaan maksuvälineen haltijalle etukäteen maksuvälineen käytön estämisestä. Mikäli tämä ei ole mahdollista, tulee ilmoitus tehdä mahdollisimman pian maksuvälineen käytön estämisen jälkeen.

Maksuvälineen käytön estäminen voi tulla kyseeseen tapauksissa, joissa verkkopankkitunnukset ja tunnistautumisväline ovat päätyneet rikollisten haltuun ja rikolliset yrittävät tehdä maksuja ilman maksuvälineen haltijan suostumusta. Tällöin pankki saattaa havaita poikkeavaa maksukäyttäytymistä maksumonitoroinnissaan ja sulkea maksuvälineen.

Osuuspankki kertoo digitaalisten palvelujen ehdoissa, että sillä on oikeus sulkea tunnukset tai rajoittaa niiden käyttöä tilanteissa, joissa tunnusten käytön turvallisuus on vaarantunut tai on syytä epäillä, että tunnuksia tai OP:n digitaalisia palveluita käytetään oikeudettomasti tai vilpillisesti. Esimerkkitilanteita ovat tunnusten luovuttaminen toiselle tai epäilys tunnusten väärinkäytöstä. [98]

3.6 Asiakkaan velvollisuudet ja huolellisuusvaatimus

Asiakkaan velvollisuuksien sisältö on olennainen osa tutkielman analyysiä, sillä niiden noudattaminen tai rikkominen määrittää vastuunjaon lopputulosta.

[97] HE 169/2009 vp, s. 71.
[98] OP:n tunnus- ja digisopimuksen ehdot 2025, s. 10–11 .

Maksuvälineen haltijalla on maksupalvelulain 53 §:n mukaan velvollisuus huolehtia maksuvälineestä ja siihen liittyvistä henkilökohtaisista turvatunnuksista, siten kuin maksuvälineen myöntämistä ja käyttöä koskevissa ehdoissa on sovittu. Maksuvälineen haltijan tulee siis pitää maksukortin ja verkkopankkitunnusten käyttäjätunnukset, salasanat ja pin-koodit omana tietonaan.

Maksupalvelulain 54 §:ssä säädetään toimista, mitä pitää tehdä, jos maksuväline katoaa. Maksuvälineen haltijan tulee ilman aiheetonta viivytystä ilmoittaa palveluntarjoajalle tai sen nimeämälle muulle taholle havaitsemastaan maksuvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä. Muu taho voi olla esimerkiksi sulkupalvelu. Katoamisilmoituksen teosta voidaan sopia pankin ja asiakkaan välillä puitesopimuksessa, eikä ilmoitustapaa säädellä erikseen laissa. [99] Osuuspankin OP:n tunnus- ja digisopimuksen ehdoissa kerrotaan menettelytavasta, miten tulee toimia, jos tunnukset katoavat, joutuvat sivullisen tietoon tai haltuun:

> Sinun on välittömästi ilmoitettava OP:lle tunnuksen tai sen osan katoamisesta tai joutumisesta käyttöön oikeudettoman tietoon tai haltuun taikka, jos epäilet niiden joutuneen käyttöön oikeudettoman tietoon tai haltuun. Ilmoitus on tehtävä myös siinä tapauksessa, että vain osa Tunnuksista on kadonnut tai joutunut käyttöön oikeudettoman tietoon tai haltuun.[100]

Osuuspankin mukaan ilmoitus tulee tehdä puhelimitse Osuuspankin ilmoittaman sulkupalvelun numeroon, joka toimii 24 tuntia vuorokaudessa viikon jokaisena päivänä. Lisäksi ilmoituksen voi tehdä myös Osuuspankin asiakaspalveluun sen aukioloaikoina tai asioimalla konttorilla henkilökohtaisesti.[101]

Nordean vastaavissa ehdoissa asiakasta kehotetaan ilmoittamaan pankkitunnusten joutumisesta sivullisen tietoon tai katoamisesta välittömästi. Ilmoituksen voi tehdä Suomessa sijaitseviin konttoreihin niiden aukioloaikoina tai puhelimitse pankin

[99] HE 169/2009 vp, s. 69.
[100] OP:n tunnus- ja digisopimuksen ehdot 2025, s. 8.
[101] OP:n tunnus- ja digisopimuksen ehdot 2025, s. 8.

asiakaspalveluun. Mikäli asiakaspalvelu ei ole auki, tulee ilmoitus tehdä sulkupalveluun.[102]

Kun pankin asiakas havaitsee, että verkkopankkitunnukset ovat päätyneet oikeudettoman haltuun, tulee hänen lain sekä sopimusehtojen mukaan ilmoittaa tästä välittömästi pankille tai pankin ilmoittamaan sulkupalveluun. Verkkopankkitunnukset voivat päätyä kuulumattomalle taholle esimerkiksi huijaussivuston kautta, jonka avulla rikolliset kalastelevat verkkopankkitunnuksia. Asiakkaalla on velvollisuus ilmoittaa välittömästi pankille siitä, jos pankkitunnukset joutuvat sivullisen tietoon. Huomioitavaa on se, että pankin asiakkaan tulee ymmärtää se, että pankkitunnukset ovat voineet joutua sivullisen haltuun. Pankin asiakkaan on tärkeä ilmoittaa tunnusten joutumisesta toisen käyttöön, sillä verkkopankkitunnusten ja vahvistuskoodien avulla, on mahdollista rekisteröidä pankin mobiilisovellus sekä vahva sähköinen tunnistusväline käyttöön.

[102] Pankkitunnuksilla käytettävien palvelujen yleiset sopimusehdot 2025, s. 3.

4 Vastuunjako maksuvälineen väärinkäytöstilanteissa

4.1 Korvausvastuun määrittyminen

Vahingonkorvauslain (412/1974) 1:1 §:n mukaan kyseistä lakia sovelletaan vain silloin, jos muussa laissa ei toisin säädetä. Maksuvälineen oikeudettomasta käytöstä säädetään Maksupalvelulain 62 ja 63 §:issä, joten vahingonkorvauksia mietittäessä sovelletaan maksupalvelulakia. Hallituksen esityksen mukaan vahingonkorvaussäännöksen sisällyttäminen maksupalvelulakiin on katsottu tarpeelliseksi, jotta sääntely kattaisi myös palveluntarjoajan lain tai sopimuksen vastaisesta menettelystä aiheutuneet vahingot. Ilman tätä säännöstä keskeinen kysymys korvausoikeudesta jäisi yleisten sopimusoikeudellisten periaatteiden varaan, mikä heikentäisi sääntelyn systemaattisuutta.[103]

4.2 Pankin vastuu oikeudettomasta maksutapahtumasta

Maksupalvelulain 63 §:ssä säädetään maksupalvelun tarjoajan eli tutkielman kontekstissa pankin vastuusta oikeudettomassa maksutapahtumassa. Lähtökohtana on se, että mikäli maksutapahtuma on toteutettu oikeudettomasti, palveluntarjoajalla on, jollei 62 §:stä muuta seuraa, velvollisuus palauttaa asiakkaalle veloitettu summa tai oikaista tili ennalleen. Palautus tai oikaisu on tehtävä viipymättä ja viimeistään seuraavana työpäivänä siitä, kun maksutapahtuma on havaittu tai siitä on ilmoitettu, mikä korostaa pankin vastuuta reagoida nopeasti väärinkäytösepäilyihin.

Hallituksen esityksessä todetaan, että näyttövelvollisuus siitä, että maksutapahtuma on ollut oikeudeton, on palveluntarjoajalla. Näin ollen palveluntarjoaja kantaa myös vastuun siitä, ettei se palauta varoja välittömästi, vaan varojen palautuminen viivästyy esimerkiksi selvittelytöiden takia.[104] Viivästyksen takia pankki kantaa myös vastuun siitä,

[103] HE 169/2009
[104] HE 169/2009, s. 77.

että se voi joutua maksamaan palautettavalle rahamäärälle viivästyskorkoa korkolain (633/1982) mukaisesti[105]. Maksupalvelulain 63 § mukaisissa tapauksissa pankilla on velvollisuus palauttaa oikeudettomasti siirretyt varat, ellei maksupalvelulain 62 §:n johdosta muuta johdu. Tämä tarkoittaa sitä, että maksupalvelulain 62 §:ssä on säädetty niistä tilanteista, jolloin vastuu maksupalvelun oikeudettomasta käytöstä siirtyy pankin asiakkaan vastuulle.

Tapauksessa FINE-058023 pankin asiakkaan tytär pyrki kirjautumaan äitinsä puolesta verkkopankkiin, mutta ohjautui rikollisten luomille pankin verkkosivuilta näyttäneille valesivuille ja joutui verkkourkinnan kohteeksi. Asiakkaan tililtä tehtiin useita oikeudettomia tilisiirtoja yhteensä kymmenien tuhansien eurojen arvosta pankin mobiilisovelluksella, joka oli juuri aktivoitu uuteen laitteeseen. Mobiilisovelluksen käyttöönotto edellytti asiakkaan pankkitunnuksia sekä asiakkaan puhelimeen lähetettyä vahvistuskoodia. Pankin viestissä oli nimenomaisesti todettu, ettei koodia tule syöttää verkkosivuille ja että epäselvissä tilanteissa on otettava yhteyttä pankkiin. Asiakas otti yhteyttä pankin asiakaspalveluun, ja pankkitunnukset suljettiin. FINE on ratkaisussaan todennut, että maksutapahtuma on ollut tässä tapauksessa oikeudeton.[106]

Vastuunjaon kannalta olennaiseksi asiaksi jää maksupalvelulain 62 §:n tulkitseminen, joka koskee maksupalvelun käyttäjän vastuuta, kun maksuvälinettä käytetään oikeudettomasti.

4.3 Asiakkaan vastuu oikeudettomasta maksutapahtumasta

Maksupalvelulain 62 §:n mukaan maksupalvelun käyttäjä, joka on tehnyt maksuvälinettä koskevan sopimuksen pankin tai muun palveluntarjoajan kanssa, vastaa maksuvälineen

[105] HE 132/2017, s. 47.
[106] FINE-058023.

katoamisesta tai sen oikeudettomasta käytöstä vain tietyissä tilanteissa. Vastuu syntyy, jos käyttäjä tai muu maksuvälineen haltija on:

1. luovuttanut maksuvälineen henkilölle, jolla ei ole oikeutta käyttää sitä;
2. huolimattomasti laiminlyönyt maksupalvelulain 53 §:n 1 momentissa säädetyt velvollisuudet; tai
3. viivytellyt ilman hyväksyttävää syytä ilmoittaessaan pankille tai sen nimeämälle taholle maksuvälineen katoamisesta, joutumisesta sivullisen haltuun tai oikeudettomasta käytöstä.

Maksupalvelun käyttäjän vastuusta säädetään yksiselitteisesti 62 §:n 1 momentin kohdissa 1-3. Maksupalvelun käyttäjä vastaa maksuvälineen oikeudettomasta käytöstä, jos hän on luovuttanut sen henkilölle, jolla ei ole ollut oikeutta käyttää sitä, jos hän on huolimattomuudesta laiminlyönyt maksupalvelulain 53 §:n 1 momentissa säädetyt velvollisuutensa tai jos hän on jättänyt ilman aiheetonta viivytystä ilmoittamatta palveluntarjoajalle tai sen nimeämälle taholle maksuvälineen katoamisesta, joutumisesta sivullisen haltuun tai sen oikeudettomasta käytöstä. Lain esitöiden mukaan maksupalvelulain 62 §:n 1 momentin 1 kohdassa mainittu tilanne, jossa maksuväline luovutetaan oikeudettomalle henkilölle, ei tarkoita sitä, että käyttäjä olisi automaattisesti ja rajattomasti vastuussa kaikesta myöhemmin tapahtuvasta väärinkäytöstä. Käyttäjä vastaa kyllä sen henkilön toimista ja huolellisuudesta, jolle hän on maksuvälineen antanut, mutta jos maksuväline päätyy tämän jälkeen vielä kolmannen osapuolen haltuun esimerkiksi varkauden kautta, vastuun ja syy-yhteyden arviointi edellyttää tapauskohtaista harkintaa.[107]

Maksupalvelulain 62 §:n 2 momentissa rajataan maksupalvelun käyttäjän vastuuta. Jos vastuu 1 momentin mainittuihin kohtiin 2 tai 3, käyttäjän korvausvastuu on enintään 50 euroa. Tätä enimmäismäärää ei kuitenkaan sovelleta, mikäli käyttäjä tai maksuvälineen haltija on toiminut tahallisesti tai törkeän huolimattomasti.

[107] HE 132/2017, s. 45.

Maksupalvelulain 62 §:n 3 momentin mukaan, maksupalvelun käyttäjä ei ole vastuussa maksuvälineen oikeudettomasta käytöstä, jos:

1. maksuvälinettä on käytetty sen jälkeen, kun katoamisesta, joutumisesta sivullisen haltuun tai oikeudettomasta käytöstä on ilmoitettu pankille tai sen nimeämälle taholle;
2. pankki ei ole huolehtinut siitä, että ilmoituksen voi tehdä milloin tahansa;
3. maksunsaaja ei ole maksua vastaanottaessaan varmistanut asianmukaisesti maksajan oikeutta käyttää maksuvälinettä; tai
4. pankki ei ole edellyttänyt maksajan vahvaa tunnistamista.

Näillä säännöksillä pyritään rajaamaan asiakkaan vastuuta tilanteissa, joissa maksuvälineen oikeudettoman käytön estäminen ei ole enää hänen vaikutusmahdollisuuksiensa piirissä. Ensinnäkin vastuu ei voi seurata sen jälkeen, kun asiakas on tehnyt pankille ilmoituksen maksuvälineen katoamisesta, joutumisesta sivullisen haltuun tai sen oikeudettomasta käytöstä, sillä tästä hetkestä alkaen riskin kantaminen kuuluu palveluntarjoajalle. Toiseksi pankin on huolehdittava siitä, että tällaisen ilmoituksen voi tehdä milloin tahansa. Mikäli pankki ei tätä velvollisuuttaan täytä, asiakkaan ei voida katsoa olevan vastuussa viivästyksestä. Kolmanneksi vastuu ei siirry asiakkaalle myöskään silloin, kun maksunsaaja ei ole maksutapahtumaa vastaanottaessaan varmistanut asianmukaisesti maksajan oikeutta käyttää maksuvälinettä. Näiden rajoitusten tarkoituksena on turvata kuluttajaa ja tasapainottaa vastuunjakoa siten, että se kohdistuu ensisijaisesti niihin tahoihin, joilla on parhaat edellytykset ehkäistä väärinkäytöksiä. Neljännessä kohdassa edellytetään, että maksut tulee tehdä lain edellyttämällä tavalla vahvasti tunnistautuneena.

Pykälän 4 momentin mukaan edellä mainituista poiketen käyttäjä on kuitenkin vastuussa, jos hän tai muu maksuvälineen haltija on tehnyt tahallisesti väärän ilmoituksen tai muuten toiminut petollisesti.

Kyseisen kohdan avulla pyritään turvaamaan pankin asemaa ja ehkäisemään tahallisten väärinkäytösten tekoa. Säännös korostaa riskijaon oikeudenmukaisuutta ja suojaa kuluttajaa silloin, kun hän toimii vilpittömästi ja huolellisesti.

Kun rikollinen onnistuu aktivoimaan asiakkaan pankin mobiilisovelluksen käyttäen asiakkaan tunnistetietoja ja vahvaa sähköistä tunnistamista, tämä ei merkitse sitä, että myöhemmin tehtyjä maksutapahtumia ei pidettäisi maksupalvelulain tarkoittamalla tavalla oikeudettomina. Oikeudeton maksutapahtuma edellyttää, että maksutapahtuma toteutetaan ilman maksajan suostumusta sovitulla tavalla, ja maksupalvelulain 38 §:n mukaan suostumus liittyy nimenomaisesti yksittäiseen maksutapahtumaan tai sen toteuttamiseen, ei maksuvälineen käyttöönottoon. Vaikka asiasta ei ole suoraan korkeimman oikeuden nimenomaista ratkaisua, FINEn ratkaisukäytännöstä on johdettavissa tulkintalinja, jonka mukaan tällaisia maksutapahtumia pidetään oikeudettomina silloin, kun maksaja ei ole niitä nimenomaisesti hyväksynyt. Mikäli rikollinen tekee tilisiirtoja asiakkaan nimissä ilman asiakkaan nimenomaista suostumusta, maksutapahtumia pidetään siten oikeudettomina riippumatta siitä, että mobiilisovellus on aktivoitu asiakkaan omilla tunnistetiedoilla.

Mobiilisovelluksen aktivoinnin olosuhteilla voi kuitenkin olla merkitystä arvioitaessa, onko asiakas laiminlyönyt maksupalvelulain 53 §:n mukaisen huolellisuusvelvollisuutensa turvatunnusten säilyttämisessä ja käytössä. Arvioinnin kohteena on tällöin asiakkaan toiminnan huolellisuus ja sen aste, onko kyse tavanomaisesta huolimattomuudesta, jolloin vastuu rajoittuu 50 euroon, vai katsotaanko asiakkaan menettely osoittavan sellaista vakavaa piittaamattomuutta turvallisuusriskejä kohtaan, että sitä voidaan pitää törkeänä huolimattomuutena. Mikäli asiakkaan katsotaan toimineen törkeän huolimattomasti, asiakas vastaa vahingosta täysimääräisesti.

Edellä tarkastellut säännökset osoittavat, että vastuunjaon perusasetelma tiliväärinkäytöstapauksissa on kaksijakoinen. Pankki vastaa lähtökohtaisesti

oikeudettomista maksutapahtumista ja on velvollinen palauttamaan varat viivytyksettä, mutta maksupalvelulain 62 §:ssä säädetään poikkeuksista, joiden perusteella vastuu voi siirtyä asiakkaalle. Tällöin arvio kohdistuu siihen, onko asiakas luovuttanut tunnuksensa sivulliselle, laiminlyönyt huolellisuusvelvoitteensa tai viivytellyt ilmoittamisessa.

Erityisen ongelmallisia ovat tapaukset, joissa rikollinen onnistuu hyödyntämään asiakkaan omia tunnistetietoja vahvaa tunnistamista edellyttävällä tavalla. Vaikka maksutapahtumat ovat näissäkin tilanteissa oikeudettomia, koska asiakas ei ole antanut niihin suostumustaan, vastuunjako ei määräydy yksinomaan tämän perusteella. Ratkaisevaksi muodostuu asiakkaan huolimattomuuden aste, mikäli asiakkaan katsotaan toimineen törkeän huolimattomasti tunnustietojensa käsittelyssä, vastuu voi siirtyä hänelle täysimääräisesti.

5 Huolimattomuuden arviointi verkkohuijauksissa – rajaveto vastuun siirtymisessä

5.1 Huolimattomuus käsitteenä

Huolimattomuuden arvioinnista puhuttaessa käytetään usein termiä tuottamus, joka kattaa sekä tahallisuuden (*dolus*) että huolimattomuuden (*culpa*). [108] Vahingonkorvauslaissa ei määritellä tarkemmin tahallisuuden ja tuottamuksen sisältöä, vaan näiden tulkinta on jätetty oikeustieteen ja oikeuskäytännön tehtäväksi. [109]

Tahallisuudella tarkoitetaan tilannetta, jossa tekijä on tarkoittanut aiheuttaa vahingon tai on pitänyt vahingon syntymistä varmana tai varsin todennäköisenä ja toiminut tästä huolimatta. Rikosoikeudessa vakiintuneen määritelmän mukaan teko on tahallinen myös silloin, kun seurauksen syntyminen liittyy välittömästi tekijän tarkoittamaan päämäärään tai kun hän tietoisesti ottaa riskin vahingon aiheutumisesta. Vahingonkorvausoikeudessa tahallisuus rinnastuu usein törkeään huolimattomuuteen, eikä rajanveto näiden välillä ole yleensä merkityksellinen vastuun syntymisen kannalta. Tahallisuutta arvioitaessa tarkastellaan tekijän tietoisuutta, tarkoitusta ja suhtautumista seurauksiin, eikä sen edellytyksenä ole täydellinen käsitys tapahtumien kulusta. [110]

Tuottamuksella tarkoitetaan vaadittavan huolellisuuden laiminlyöntiä, joka ilmenee henkilön moitittavana riskinottona tai varomattomuutena hänen toimiessaan tai jättäessään toimimatta. Arvioinnissa lähtökohtana on, miten huolellisesti henkilön olisi tullut toimia ottaen huomioon hänen tietonsa, olosuhteet ja toimintaan liittyvät riskit. Tuottamus on siten objektiivinen mitta henkilön toiminnan huolellisuudesta suhteessa siihen, mitä vastaavassa tilanteessa huolelliselta henkilöltä voidaan edellyttää. Tuottamusta koskevassa harkinnassa huomioidaan myös viranomaismääräysten, lain,

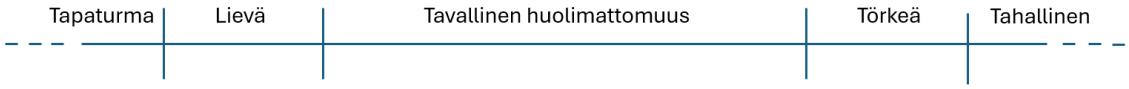
[108] Hemmo 2005, s. 23–24.
[109] Ståhlberg & Karhu 2020, s. 89.
[110] Ståhlberg & Karhu 2020, 89–92.

alan vakiintuneiden käytäntöjen tai muiden käyttäytymisohjeiden rikkominen, jotka voivat osoittaa, ettei edellytettyä huolellisuutta ole noudatettu.[111]

Huolimattomuuden eri asteiden arvioinnissa on yleensä perusteltua lähteä oletuksesta, että kyse on tavallisesta huolimattomuudesta. Lievän tai törkeän huolimattomuuden toteaminen edellyttää erityisiä perusteita, jotka osoittavat poikkeamisen tavanomaisesta huolellisuusstandardista. Tämä lähtökohta on johdonmukainen, koska tavallinen huolimattomuus kattaa suhteellisesti laajimman osan tuottamuksen asteikkoa.[112] Vahingonkorvauslaissa ei käytetä ilmaisua tavallinen huolimattomuus tai tavallinen tuottamus. Vahingonkorvausoikeudessa on kuitenkin eroteltavissa huolimattomuudelle kolme astetta: törkeä huolimattomuus, tavallinen huolimattomuus ja lievä huolimattomuus[113].

Kuviossa kaksi on esitetty huolimattomuuden asteiden jatkumo, joka kuvaa teon moitittavuuden ja vastuun asteittaista lisääntymistä. Jatkumon vasemmassa päässä on tapaturma, joka viittaa seuraukseen ilman syyllisyyttä tai huolimattomuutta. Tapaturman jälkeen seuraavat lievä ja tavallinen huolimattomuus, joissa toiminta poikkeaa huolellisuusvaatimuksesta vähäisessä tai tavanomaisessa määrin. Törkeä huolimattomuus merkitsee vakavaa välinpitämättömyyttä velvollisuuksia tai seurauksia kohtaan, ja jatkumon oikeassa ääripäässä on tahallinen teko, jossa henkilö toimii tietoisesti ja tarkoituksellisesti. [114] Jatkumon avulla havainnollistetaan, kuinka teon moitittavuus kasvaa vähitellen satunnaisesta vahingosta täysin tahalliseen toimintaan.

[111] Ståhlberg & Karhu 2020, 93–95.
[112] Hemmo 2005, s. 49.
[113] Ståhlberg & Karhu 2020, s. 115.
[114] Hemmo 2005, s. 47–49.



Kuvio 2. Tuottamus voidaan jakaa kolmeen eri asteeseen.[115]

Törkeän tuottamuksen ja tahallisuuden välinen raja, samoin kuin lievän tuottamuksen ja tapaturman välinen ero, ei ole helposti määriteltävissä tavalla, joka soveltuisi kaikissa tilanteissa. Sama koskee tuottamuksen eri asteiden välisiä rajoja. Näitä rajoja on usein kuvattu liukuviksi, millä ei kuitenkaan tarkoiteta rajojen muuttuvuutta, vaan sitä, että niiden täsmällinen määrittely on käytännössä haastavaa.[116]

Pankkitunnusten kalastelua ja niiden oikeudetonta käyttöä arvioitaessa korvausvastuun osalta sovelletaan huolimattomuuden arviointia, koska teon tahallisuuteen viittaavaa näyttöä ei ole. Mikäli maksuvälineen haltijan epäillään toimineen tahallisesti, tällöin korvausvastuu määräytyy maksupalvelulain 62 §:n 2 momentin mukaisesti niin, että maksuvälineen haltija vastaa maksuvälineen oikeudettomasta käytöstä.

Huolimattomuutta arvioitaessa on otettava huomioon, millainen velvollisuus henkilöllä on toimia sekä se, missä määrin hänen voidaan ennakoida ymmärtävän, että passiivisuus saattaa johtaa tiettyihin seurauksiin. Lisäksi tuottamus merkitsee tietyissä tilanteissa vaadittavan huolellisuuden laiminlyöntiä. [117] Kun kyseessä on tapaus, jossa verkkopankkitunnukset on saatu petollisesti haltuun, huolellisuutta on arvioitava pankin asiakkaan näkökulmasta sekä sen perusteella, mitä voidaan edellyttää tavanomaiselta pankin asiakkaalta hänen asioidessaan pankin kanssa.

[115] Hemmo 2005, s. 49.
[116] Ståhlberg & Karhu 2020, s. 115.
[117] Ståhlberg & Karhu 2020, s. 93.

5.2 Maksuvälineen haltijan tavanomainen käyttäytyminen

Tavanomaisen käyttäytymisen arviointi on huolimattomuusarvioinnin lähtökohta, sillä asiakkaan toimintaa verrataan siihen, mitä huolelliselta maksuvälineen haltijalta voidaan odottaa.

Huolimattomuuden arviointi ei perustu tarkkarajaisiin määritelmiin, vaan asteikko on luonteeltaan liukuva. Rajaa esimerkiksi lievän ja tavallisen huolimattomuuden tai törkeän tuottamuksen ja tahallisuuden välillä ei voida kuvata yleispätevästi siten, että se soveltuisi kaikkiin tapauksiin. Arviointi riippuu aina olosuhteista ja kulloinkin kyseessä olevasta toiminnasta.[118]

Tämä vaikeus korostuu erityisesti silloin, kun pyritään määrittelemään, mitä voidaan pitää maksuvälineen haltijan tavanomaisena käyttäytymisenä. Kuten luvussa kolme on todettu, sekä pankilla että sen asiakkaalla on useita velvollisuuksia ja oikeuksia, mutta kysymys kuuluu, voidaanko asiakkaan toiminnalle asettaa yhdenmukaisia huolellisuusvaatimuksia vai onko arviointi tehtävä yksilöllisesti esimerkiksi iän, kokemuksen tai muiden henkilökohtaisten tekijöiden perusteella.

On arvioitu, että pankkien järjestelmissä käsitellään kuukausittain yli sata miljoonaa maksutapahtumaa, joista 99,9975 prosenttia toteutuu juuri asiakkaan tarkoittamalla tavalla. Tämä osoittaa, että poikkeamat ovat harvinaisia, mutta myös sen, että yksittäisen tapauksen arviointi saa usein korostuneen merkityksen, kun poikkeama tapahtuu.[119]

Maksupalvelulain esitöissä korostetaan, että asiakkaan huolellisuusvelvollisuuksia arvioidaan olosuhteiden kokonaisuutena ja siten, ettei asiakkaan velvollisuuksista saa muodostua kohtuuttomia. [120] Tämä lähtökohta ohjaa sitä, miten tavanomaista käyttäytymistä tulee määritellä sähköisessä asioinnissa. Arvio ei perustu abstraktiin

[118] Ståhlberg & Karhu 2020, s. 116–117.
[119] Palmgren 2022.
[120] HE 169/2009 vp, s. 75.

mittapuuhun, vaan siihen, miten huolellinen henkilö vastaavassa asemassa olisi toiminut pankin ohjeiden ja viestinnän perusteella.

Itä-Suomen hovioikeuden 13.11.2024 antamassa tuomiossa arvioitiin, oliko pankin asiakkaan menettely poikennut tavanomaisesta huolellisuudesta tilanteessa, jossa hän oli joutunut ammattimaisesti toteutetun verkkohuijauksen uhriksi. Asiakas oli saanut pankin nimissä lähetetyn tekstiviestin, jossa häntä kehotettiin kirjautumaan linkin kautta pankin sivuille ja vahvistamaan toimenpiteitä estääkseen oletetun petoksen. Hän toimi ohjeiden mukaan ja syötti pankkitunnuksensa rikollisten luomalle valesivustolle, minkä seurauksena hänen tililtään siirrettiin 44 000 euroa ulkomaiselle tilille. Hovioikeus katsoi, että asiakas ei ollut antanut tietoista suostumusta maksutapahtumaan ja että hänen menettelynsä, vaikka jossain määrin huolimatonta, ei täyttänyt törkeän huolimattomuuden kriteeriä. [121] Tapaus havainnollistaa, kuinka vaikeaa on määritellä, mitä pidetään maksuvälineen haltijan tavanomaisena ja huolellisena käyttäytymisenä nykyaikaisessa digitaalisessa toimintaympäristössä.

Hovioikeuden kokonaisarvioinnin mukaan asiakkaan toiminta osoitti jonkinasteista huolimattomuutta, mutta ei sellaista vakavaa piittaamattomuutta, joka täyttäisi törkeän huolimattomuuden tunnusmerkit. Tilanne oli ollut poikkeuksellinen, kiireellinen ja ulkopuolisten aiheuttama, mikä johti inhimillisesti ymmärrettävään erehdykseen. Ratkaisun perusteluista on tulkittavissa, että tavanomaisena pidetään sellaista käyttäytymistä, joka vastaa keskimääräisen, kohtuullisen huolellisen verkkopankin käyttäjän toimintaa. Esimerkiksi luottamista pankin nimissä tulevaan viestiin tai aidolta näyttävään sivustoon ei voida lähtökohtaisesti pitää poikkeavana, jos huijaus on toteutettu ammattimaisesti ja viestin ulkoasu muistuttaa pankin viestintää.

Ratkaisussa korostui myös yksilöllisten tekijöiden merkitys huolimattomuusarvioinnissa. Oikeus totesi, että tavanomaisen ja huolellisen käyttäytymisen arvioinnissa voidaan ottaa huomioon asiakkaan henkilökohtaiset ominaisuudet, kuten ikä, digitaalinen

[121] Itä-Suomen HO 13.11.2024 t. 462 s. 7–8, 17–18.

osaaminen ja asiointikokemus. Arviointi ei siten perustu abstraktiin mittapuuhun, vaan siihen, miten huolellinen henkilö vastaavassa asemassa olisi toiminut kyseisessä tilanteessa.[122]

5.3 Törkeä huolimattomuus – milloin vastuu siirtyy kokonaan asiakkaalle?

5.3.1 Törkeä huolimattomuus käsitteenä

Törkeän huolimattomuuden käsite on tutkielman ydinongelman kannalta ratkaiseva, sillä se määrittää rajan, jonka ylittyessä vastuunjako muuttuu olennaisesti.

Euroopan unionin maksupalveludirektiivi PSD2 muodostaa maksupalvelujen sääntelyn perustan ja velvoittaa jäsenvaltiot sisällyttämään sen säännökset kansalliseen lainsäädäntöön [123]. Direktiivin tavoitteena on yhdenmukaistaa sääntelyä erityisesti kuluttajansuojan, vastuunjaon ja maksamisen turvallisuuden osalta, mutta se jättää jäsenvaltioille harkintavaltaa huolimattomuuden arviointikriteerien soveltamisessa. Tämä mahdollistaa kansallisten oikeusperiaatteiden huomioon ottamisen, mutta voi johtaa erilaisiin tulkintoihin eri jäsenmaissa.

PSD2 korostaa, että maksupalvelun käyttäjän huolimattomuuden ja erityisesti törkeän huolimattomuuden arvioinnissa on huomioitava kaikki tapauksen olosuhteet. Näyttö ja sen vakavuusaste arvioidaan kansallisen lainsäädännön mukaisesti. Törkeä huolimattomuus edellyttää merkittävää piittaamattomuutta, kuten tilannetta, jossa maksuväline ja sen tunnukset säilytetään samassa, kolmansien havaittavissa olevassa paikassa. Direktiivi myös kieltää sopimusehdot, jotka kohtuuttomasti lisäävät kuluttajan todistustaakkaa tai keventävät palveluntarjoajan vastuuta. Erityisesti

[122] Itä-Suomen HO 13.11.2024 t. 462 s. 17–18.
[123] ks. Ojanen, s. 63. EU-oikeus on osa jäsenvaltioiden oikeusjärjestystä. Sen ja kansallisen oikeuden välistä suhdetta pidetään monistisena: asetukset ovat suoraan sovellettavia, kun taas direktiivit edellyttävät kansallista täytäntöönpanoa.

etämaksutilanteissa palveluntarjoajaa velvoitetaan osoittamaan väitetty huolimattomuus, sillä maksajan mahdollisuudet esittää omaa näyttöä ovat rajalliset.

Suomessa direktiivin periaatteet on toimeenpantu maksupalvelulaissa. Sen 53 § määrittelee maksupalvelun käyttäjän vastuun luvattomista maksutapahtumista. Vaikka säännös perustuu EU-oikeuteen, sen soveltaminen ja huolimattomuuden arviointi tapahtuvat kansallisen oikeuskäytännön ja yleisten vahingonkorvausoikeudellisten periaatteiden mukaisesti. Törkeällä huolimattomuudella tarkoitetaan poikkeuksellisen vakavaa varomattomuutta, joka osoittaa välinpitämätöntä suhtautumista maksuvälineen hallintaan ja sen käyttöön liittyviin turvallisuusriskeihin. Arviointi perustuu kokonaisharkintaan, jossa huomioidaan muun muassa vahinkoriskin suuruus ja mahdollisuudet toteuttaa tarvittavia varotoimia.[124]

EU-sääntely luo yhteiset vähimmäisvaatimukset, mutta kansallinen lainsäädäntö konkretisoi niiden käytännön soveltamisen. Direktiivin tarkoituksena on estää kuluttajan asemaa heikentävä sääntely ja mahdollistaa parempi suoja. Näin ollen huolimattomuuden ja törkeän huolimattomuuden rajanveto voi painottua jäsenvaltioissa eri tavoin, vaikka säätelyn perusta on yhtenäinen.

Korkein oikeus on ratkaisukäytännössään määritellyt useita seikkoja, joita voidaan käyttää törkeän huolimattomuuden arviointikriteereinä. Näitä ovat muun muassa huolimattoman menettelyn aiheuttama riskin lisääntyminen, mahdollisen vahingon vakavuus, henkilön tietoisuus riskistä ja hänen suhtautumisensa siihen, poikkeamisen merkittävyys huolellisesta toiminnasta, vakiintuneiden toimintatapojen rikkominen sekä mahdollisuudet toteuttaa varotoimenpiteitä. Oikeuskäytännön perusteella nämä kriteerit ovat objektiivisia ja sovellettavissa myös yksityishenkilöiden toiminnan arviointiin. Maksupalvelun käyttäjän vähimmäisvaatimuksena voidaan pitää sitä, että hän lukee ja ymmärtää pankin lähettämät varoitukset tai ilmoitukset sekä toimii niiden edellyttämällä tavalla. Koska näillä varotoimilla pyritään ehkäisemään merkittäviä

[124] ks. HE 169/2019 vp, s. 75 ja KKO 2018:71

taloudellisia riskejä, niiden laiminlyönti osoittaa lähtökohtaisesti välinpitämätöntä suhtautumista vahinkoriskiin.[125]

Korkeimman oikeuden esittämät kriteerit muodostavat viitekehyksen, jonka perusteella huolimattomuutta arvioidaan kokonaisuutena. Törkeän huolimattomuuden toteaminen edellyttää paitsi riskin olemassaolon tiedostamista myös piittaamatonta suhtautumista siihen. Maksupalvelutilanteissa arvioinnissa on huomioitava käyttäjän tiedolliset ja tekniset valmiudet sekä olosuhteet, joissa päätös on tehty. Mitä ennakoitavampi ja helposti vältettävissä oleva riski on ollut, sitä todennäköisemmin huolimattomuutta voidaan pitää törkeänä. Sen sijaan tilanteissa, joissa pankin viestintä on epäselvää tai olosuhteet ovat olleet harhaanjohtavat, tietoisen riskinoton elementti puuttuu ja vastuu kevenee. Näin arviointi on väistämättä olosuhderiippuvaista ja heijastaa digitaalisen toimintaympäristön luomia erityispiirteitä.

Edellä mainittujen lisäksi myös FINE on ottanut kantaa siihen, miten se arvioi huolimattomuuden eri asteita antaessaan ratkaisusuosituksia. FINEn ratkaisukäytännössä arvioidaan usein tietojenkalastelun uhriksi joutuneiden asiakkaiden huolellisuutta. Keskeistä on, miten selkeä pankin lähettämä viesti, esimerkiksi mobiilisovelluksen aktivointikoodi on ollut. Mikäli viesti on informatiivinen ja sisältää varoituksen huijauksista, asiakkaan tulisi keskeyttää asiointi, jos hän saa viestin, joka ei vastaa hänen omaa toimintaansa. Jos asiakas tästä huolimatta syöttää aktivointikoodin kalastelusivustolle, menettely voidaan katsoa törkeän huolimattomaksi. Toisaalta, jos viestin sisältö on epäselvä tai muistuttaa aidosti pankin viestintää, lautakunta ei yleensä pidä asiakkaan toimintaa törkeän huolimattomana. Myös pankilla on velvollisuus varmistaa viestien selkeys ja ymmärrettävyys.[126]

[125] Vaasan HO 19.9.2024 t. 342, s. 6.
[126] Lappi ja muut 2024.

5.3.2 Viestinnän selkeys ja varoitusten merkitys törkeän huolimattomuuden arvioinnissa

Viestinnän selkeys on ratkaisukäytännössä noussut keskeiseksi arviointikriteeriksi. Tässä alaluvussa analysoidaan, miten viestinnän laatu vaikuttaa huolimattomuuden asteeseen.

Törkeän huolimattomuuden arviointi perustuu aina tapauskohtaiseen kokonaisharkintaan, jossa punnitaan maksupalvelun käyttäjän menettelyä suhteessa häneltä kohtuudella edellytettävään huolellisuuteen. Oikeuskäytännössä rajanveto huolimattomuuden ja törkeän huolimattomuuden välillä on osoittautunut haastavaksi, sillä se ei perustu yksittäiseen tekoon, vaan kokonaisvaltaiseen käyttäytymisen arviointiin.

Vaasan hovioikeuden 19.9.2024 antamassa tuomiossa oli kyse pankkitunnusten väärinkäytöstä ja siitä, oliko pankin asiakas toiminut törkeän huolimattomasti maksupalvelulain tarkoittamalla tavalla. Asiakas halusi tarkistaa laboratoriotuloksensa Omakanta-palvelusta. Hän pyysi puolisoaan auttamaan kirjautumisessa, koska ei itse ollut tottunut käyttämään tietokonetta. Puoliso etsi Omakannan sivustoa hakukoneen avulla ja päätyi vahingossa rikollisten ylläpitämälle valesivustolle, joka jäljitteli pankin aitoa palvelua. Tälle sivulle syötettiin asiakkaan verkkopankkitunnukset. Kirjautumisen yhteydessä asiakkaan puhelimeen tuli tekstiviesti pankilta, jossa ilmoitettiin POP Avain -mobiilisovelluksen aktivoinnista ja annettiin aktivointikoodi. Viestissä todettiin selvästi, ettei koodia koskaan kysytä tietokoneen selaimessa. Lisäksi ohjeistettiin ottamaan välittömästi yhteyttä pankkiin, jos asiakas ei ole itse tekemässä aktivointia. Asiakas ei kuitenkaan lukenut viestiä huolellisesti, vaan antoi sen lopussa olleen numerokoodin puolisolleen, joka syötti sen huijaussivustolle. Näin rikolliset saivat aktivoitua pankin mobiilisovelluksen omaan käyttöönsä ja pääsivät asiakkaan tileille. Seurauksena oli, että asiakkaan tileiltä siirrettiin yhteensä 44 900 euroa ulkomaille, josta osa saatiin palautettua, mutta 25 950 euroa jäi kadoksiin.[127]

[127] Vaasan HO 19.9.2024 t. 342, s. 5–6.

Hovioikeus arvioi asiakkaan menettelyä kokonaisuutena maksupalvelulain 53 §:n huolellisuusvelvoitteen perusteella. Tapauksessa asiakas oli joutunut tietojenkalastelun kohteeksi ja kirjautunut valesivustolle. Pelkkää valesivustolle joutumista ei pidetty törkeän huolimattomana, sillä menettely ei olennaisesti poikennut tavanomaisesta huolellisuudesta.[128]

Ratkaisevaa oli pankin lähettämä mobiilisovelluksen aktivointikoodin sisältänyt tekstiviesti, jossa selkeästi todettiin, ettei koodia kysytä tietokoneen selaimessa ja että asiakkaan tuli ottaa yhteyttä pankkiin, mikäli hän ei ollut itse aloittanut aktivointia. Hovioikeus katsoi, että huolellisen asiakkaan olisi tullut lukea viesti ja ymmärtää, ettei se liittynyt käynnissä olevaan asiointiin. Viestin huomiotta jättäminen ja koodin luovuttaminen eteenpäin osoittivat piittaamattomuutta maksuvälineen turvallisuudesta.[129]

Pankin lähettämä viesti mobiilisovelluksen aktivointiin liittyen kuuluu seuraavasti:

> Tietoturvailmoitus. Olet Aktivoimassa POP Avain -sovellusta mobiililaitteellesi. Aktivointi onnistuu viestin lopussa olevalla koodilla. Huomaathan, että koodia ei ikinä kysytä tietokoneen verkkoselaimessa. Jos et ole tekemässä aktivointia itse, ota välittömästi yhteyttä POP Pankkiin tai sulkupalveluumme p. 020 333. Tietosi voivat olla vaarassa. Tarkista viesti-id:1ZNQG. Vahvista POP Avain -sovelluksen aktivointi koodilla: 570939. POP Pankki.[130]

Hovioikeuden mukaan pankin lähettämä tekstiviesti oli sisällöltään riittävän informatiivinen, sillä se sisälsi yksiselitteiset tiedot viestin tarkoituksesta, toimintaohjeet sekä varoituksen mahdollisesta väärinkäytöksestä. Hovioikeus korosti, että viestin sisältö oli niin yksiselitteinen, ettei huolelliselta asiakkaalta voitu kohtuudella odottaa sen ymmärtämistä väärin. Viestissä oli useita varoituksia, jotka ilmensivät selvästi, ettei kyse

[128] Vaasan HO 19.9.2024 t. 342, s. 6–7.
[129] Vaasan HO 19.9.2024 t. 342, s. 7.
[130] Vaasan HO 19.9.2025 t. 342, s. 6.

ollut tavanomaisesta kirjautumisesta, vaan mobiilisovelluksen käyttöönotosta. Lisäksi viestissä kehotettiin ottamaan yhteyttä pankkiin, mikäli asiakas ei ollut itse aloittanut toimenpidettä. Näin ollen viestin informatiivisuus ja varoitusten selkeys muodostivat ratkaisevan perusteen sen arvioimiselle, että asiakkaan menettely poikkesi olennaisesti vaaditusta huolellisuudesta.[131]

Hovioikeus piti pankin asiakkaan menettelyä kokonaisuutena törkeän huolimattomana ja katsoi vahingon olevan välittömässä syy-yhteydessä asiakkaan toimintaan. Ratkaisu korostaa asiakkaan velvollisuutta lukea ja ymmärtää pankin viestit, ja se painottaa viestin selkeyden merkitystä.[132]

Tapaus osoittaa, että törkeän huolimattomuuden arvioinnissa viestin informatiivisuudella ja asiakkaan aktiivisella toiminnalla on keskeinen painoarvo. Mikäli pankin viestintä on yksiselitteistä ja sisältää selkeitä varoituksia, vastuu siirtyy helpommin asiakkaalle. Oikeuden mukaan maksuvälineen haltijalta voidaan tällöin edellyttää erityistä tarkkaavaisuutta ja kykyä tunnistaa poikkeavat tilanteet, vaikka hän ei olisi teknisesti kokenut käyttäjä.

5.3.3 Viestinnän epäselvyys ja inhimillinen erehtyminen huolimattomuuden arvioinnissa

Huolimattomuuden arvioinnissa keskeiseksi kysymykseksi nousee se, missä määrin pankin käyttämä viestintä tukee asiakkaan kykyä ymmärtää toimenpiteen merkitys. Epäselvä, puutteellinen tai rutiiniviestin kaltainen turvaviesti lisää olennaisesti riskiä, että asiakas erehtyy. Tätä viestinnän vaikutusta huolimattomuusarviointiin on käsitelty sekä hovioikeuskäytännössä että FINEn ratkaisuissa.

---

[131] Vaasan HO 19.9.2025 t. 342, s. 7.
[132] Vaasan HO 19.9.2025 t. 342, s. 7.

Itä-Suomen hovioikeuden 13.11.2024 antamassa tuomiossa, jota on käsitelty alaluvussa 5.2, on kiinnitetty huomiota pankin lähettämän viestin sisältöön, jossa kerrotaan maksun vahvistamiseen vaadittava koodi. Asiakkaan saama viesti on ollut sisällöltään seuraava: ”44.000 EUR tilille GB40 REVO xxxx xxxx xxxx 73. Vahvista maksu palvelussamme avainlukulistan järjestysnumeroa 188 vastaavalla avainluvulla. OP” Viestissä ilmoitettiin siirrettävä summa, vastaanottajan tilinumero sekä ohje maksun vahvistamiseen avainlukulistan avulla. Viestin kieliasu oli muodollisesti puutteellinen. Sen alkuosa jäi predikaatin puuttumisen vuoksi epäselväksi, eikä asiakas voinut päätellä, oliko kyse maksun suorittamisesta vai esimerkiksi tarkastamisesta tai peruuttamisesta.[133]

Hovioikeus arvioi, että viestin rakenne ja informatiivisuus eivät täyttäneet riittävän selkeän viestinnän vaatimusta, joka on olennainen asiakkaan tietoisen suostumuksen arvioinnissa. Viestin alkuosa “44.000 EUR tilille GB40 REVO…” ei sellaisenaan ilmaissut selvästi maksutoimeksiannon luonnetta. Hovioikeus totesi, että selkeämpi ja yksiselitteisempi muotoilu olisi auttanut asiakasta ymmärtämään viestin todellisen tarkoituksen.[134] Yksiselitteisempi ja selkeämpi muotoilu hovioikeuden perusteluiden perusteella voisi olla: “Olette siirtämässä 44.000 euroa tilille GB40 xxxx xxxx xxx 73 ja maksun saajaksi olette ilmoittanut Mikko Mallikas. Antakaa tunnusluku yyyy, jos haluatte suorittaa kyseisen maksun.”

Hovioikeuden mukaan asiakkaan olisi tullut kiinnittää huomiota vahvistusviestin loppuosaan, jossa pyydettiin nimenomaisesti ”vahvistamaan maksu”. Tältä osin hänen toimintansa oli huolimatonta. Kuitenkin, koska asiakas oli juuri ennen tätä saanut valesivustolta ohjeet, joiden mukaan hänen tuli peruuttaa maksu, hänen virheellinen käsityksensä viestin merkityksestä oli ymmärrettävä. Näin ollen kyse ei ollut sellaisesta vakavasta varomattomuudesta, joka osoittaisi piittaamatonta suhtautumista maksuvälineen turvallisuuteen.[135]

---

[133] Itä-Suomen HO 13.11.2024 t. 462 s. 16.
[134] Itä-Suomen HO 13.11.2024 t. 462 s. 16.
[135] Itä-Suomen HO 13.11.2024 t. 462 s. 16.

FINEn ratkaisussa FINE-049807 asiakas joutui verkkourkinnan kohteeksi hakeutuessaan hakukoneen kautta pankin verkkopalveluun, mutta päätyi pankin aidon kirjautumissivuston kaltaiselle valesivulle. Asiakas syötti valesivustolle verkkopankkitunnuksensa ja pankilta saamansa kertakäyttökoodin, joka oli tosiasiassa tarkoitettu pankin mobiilisovelluksen käyttöönottoon. Rikolliset aktivoivat pankin mobiilisovelluksen asiakkaan nimissä ja tekivät sen avulla useita oikeudettomia tilisiirtoja yhteensä 63 950 eurosta. Asiakkaan lopullinen vahinko oli 54 500 euroa. Asiakas vaati pankilta korvausta.[136]

Asiakas sai valesivustolla ollessaan yhteensä neljä viestiä, jotka ovat sisällöltään seuraavat:

> Klo 17:13 SMS:
> "Olet kirjautumassa [pankin] Verkkopankkiin. Ole hyvä ja syötä vahvistuskoodi 88268 verkkopankissa sille varattuun kenttään."
>
> klo 17:17 SMS:
> "Olet hakemassa tapahtumatietoja verkkopankissa. Ole hyvä ja syötä vahvistuskoodi 92791 verkkopankissa sille varattuun kenttään."
>
> klo 19:59 SMS:
> "Käytä kertakäyttökoodia A-076911 viimeistelläksesi [pankin mobiilisovelluksen] käyttöönotto. Koodi on voimassa 3 minuuttia."
>
> klo 20:00 SMS:
> *"[Pankin mobiilisovellus] on aktivoitu laitteessa iPhone 6s. Jos et ole itse aktivoinut laitetta, ole heti yhteydessä Sulkupalveluun +358 20 333."*[137]

FINE katsoi, että asiakkaan valesivulle päätyminen hakukoneen kautta ei sellaisenaan osoittanut huolimattomuutta. Keskeistä oli pankin lähettämän aktivointikoodiviestin suppea ja rutiiniviestiä muistuttava muoto, joka teki erehdyksen objektiivisesti

---

[136] FINE-049807.
[137] FINE-049807.

ymmärrettäväksi. Asiakas sekoitti aktivointikoodin tavanomaiseen kirjautumis- tai vahvistuskoodiin, joita pankki lähettää. Vaikka asiakkaan olisi tullut epäillä menettelyä ja pidättäytyä koodin syöttämisestä, menettely ei kokonaisuutena täyttänyt törkeän huolimattomuuden kynnystä. Pankin myöhempi aktivointihälytysviesti ei vaikuttanut arvion lopputulokseen, koska asiakkaalla ei ollut tosiasiallista mahdollisuutta reagoida siihen heti.[138]

Hovioikeuden tuomio ja FINEn ratkaisu korostavat pankin viestinnän merkitystä huolimattomuuden ja vastuun arvioinnissa. Viestin kielellinen epäselvyys ja vastaanottajaa koskevien tietojen puuttuminen loivat tilanteen, jossa asiakkaan erehtyminen oli inhimillisesti ymmärrettävää. Ratkaisut osoittavat, että viestinnän selkeys ei ole vain tekninen kysymys, vaan olennainen osa asiakkaan mahdollisuutta ymmärtää, mihin toimenpiteeseen hän antaa suostumuksensa. Hovioikeuden tuomio ja sen perustelut osoittavat myös, että vastuun arviointi ei koske yksinomaan asiakkaan toimintaa, vaan ulottuu pankin viestintäkäytäntöihin.

Mitä selkeämpi ja varoittavampi pankin viesti on, sitä enemmän vastuuta voidaan asettaa asiakkaalle. Vastaavasti epäselvä ja monitulkintainen viestintä siirtää vastuuta takaisin pankille. Ratkaisuissa korostuu, että viestinnän tulee olla aidosti kaksisuuntaista. Pankin velvollisuutena on antaa asiakkaalle ymmärrettäviä ja huomiota herättäviä varoituksia sekä varmistaa, että asiakas kykenee hahmottamaan viestin sisällön oikein. Arvioinnissa huomioidaan siten realistinen ja inhimillinen näkökulma siihen, miten asiakkaat tosiasiallisesti toimivat petostilanteissa ja miten hyvin pankin viestintä tukee heidän kykyään tunnistaa riski.

Nykykäytännössä törkeän huolimattomuuden raja on siirtynyt lähemmäs lievän huolimattomuuden astetta erityisesti tilanteissa, joissa pankin viestintä muistuttaa asiakkaan arjessa esiintyviä tavanomaisia pankilta saatuja viestejä.

---

[138] FINE-049807.

Edellä esitetyn perusteella voidaan todeta, että törkeän huolimattomuuden arviointi on kokonaisvaltainen prosessi, jossa punnitaan asiakkaan toimintaa suhteessa pankin viestinnän selkeyteen, olosuhteisiin ja asiakkaan yksilöllisiin ominaisuuksiin. Keskeisiksi arviointitekijöiksi ovat oikeuskäytännössä nousseet pankin lähettämien vahvistusviestien informatiivisuus, asiakkaan tosiasiallinen mahdollisuus ymmärtää toimenpiteen merkitys sekä tilanteen poikkeuksellisuus. Vastuu jakautuu sen mukaan, kumpi osapuoli olisi voinut tehokkaammin estää vahingon syntymisen. Mikäli pankki ei ole riittävän selkeästi varoittanut asiakasta riskeistä, törkeän huolimattomuuden kynnys ei ylity, vaikka asiakas olisikin toiminut huolimattomasti.

6 Johtopäätökset ja toimintasuositukset

6.1 Johtopäätökset

Tässä luvussa esitetään tutkielman keskeiset johtopäätökset ja vastataan johdannossa asetettuihin tutkimuskysymyksiin.

Tutkielman tavoitteena oli selvittää, miten vastuu jakautuu pankin ja asiakkaan välillä tilanteissa, joissa rikollinen on onnistunut aktivoimaan pankin mobiilisovelluksen asiakkaan nimissä ja vahvistamaan sillä maksuja. Tarkastelu perustui maksupalvelulain ja vahvaa sähköistä tunnistamista koskevan sääntelyn soveltamiseen sekä FINEn ja tuomioistuinten ratkaisukäytännössä omaksuttuihin tulkintalinjoihin. Keskeisenä havaintona on, että vastuunjaon arviointi perustuu tapauskohtaiseen kokonaisharkintaan, jossa painottuvat sekä asiakkaan menettely että pankin viestinnän ja suojausmekanismien selkeys.

Ensimmäinen alakysymys koski pankin ja asiakkaan välisten velvollisuuksien jakautumista sopimussuhteessa ja sitä, miten nämä velvollisuudet luovat perustan vastuunjaon arvioinnille. Tältä osin voidaan todeta, että vaikka sääntelykehikko tarjoaa periaatteessa selkeät säännöt vastuun jakautumiselle, sen soveltaminen verkkohuijaustilanteissa on osoittautunut haasteelliseksi. Maksupalvelulain suostumusperiaatteen mukaisesti maksutapahtuma katsotaan hyväksytyksi, jos asiakas on vahvistanut sen omassa laitteessaan. Tällöin pankilla on vahva peruste pitää maksua asiakkaan hyväksymänä ja arviointi kohdistuu siihen, onko asiakas toiminut huolellisesti. Käytännössä monissa huijaustapauksissa asiakkaat kuitenkin noudattavat rikollisten ohjeita ymmärtämättä, että he vahvistavat maksun itse. Viimeaikaisessa oikeuskäytännössä, kuten hovioikeuden ratkaisuissa [139] on korostettu, että maksutapahtuman hyväksyminen edellyttää tietoista suostumusta juuri kyseiseen maksuun. Maksajan tahdonilmaisun ja vahvistamisen on muodostettava kokonaisuus,

[139] Itä-Suomen HO 13.11.2024 t. 462 s. 11.

joka kuvastaa ymmärrystä siitä, että kyse on maksamisesta tietylle taholle tietty rahamäärä. Jos asiakas ei ymmärrä teon oikeudellista merkitystä eikä tiedosta hyväksyvänsä maksua, suostumusta maksupalvelulain tarkoittamassa mielessä ei ole syntynyt. Tällöin tapahtumaa on pidettävä oikeudettomana, ja arviointi siirtyy siihen, onko asiakas omalla huolimattomuudellaan myötävaikuttanut vahingon syntymiseen. Ensimmäisen alakysymyksen osalta voidaan siten todeta, että sopimussuhde luo osapuolille toisiaan täydentävät velvollisuudet, jotka muodostavat oikeudellisen perustan vastuunjaon arvioinnille väärinkäytöstilanteissa.

Toinen alakysymys koski vastuun edellytyksiä oikeudettomissa maksutapahtumissa. Tämän osalta tutkimus osoittaa, että myös tilanteissa, joissa asiakas ei ole antanut lainkaan suostumustaan maksulle, esimerkiksi silloin, kun rikolliset ovat aktivoineet tunnistusvälineen omaan laitteeseensa, on tarpeen tarkastella, onko asiakas toiminut huolellisesti tunnistusvälineen haltijana. Maksupalvelulain vastuunrajoitukset eivät vapauta tästä velvollisuudesta. Vastuun määrä ei siten riipu yksinomaan suostumuksen olemassaolosta, vaan siitä, kuinka huolellisesti asiakas on toiminut tilanteessa kokonaisuutena arvioiden. Tämä korostaa sitä, että vastuu ei perustu pelkkään yksittäiseen tekoon, kuten vahvistuskoodin syöttämiseen valesivustolle, vaan asiakkaan koko toiminnan loogisuuteen ja ennakoitavuuteen suhteessa tilanteen olosuhteisiin.

Pankin tiedonantovelvollisuus ja viestinnän selkeys ovat keskeisiä tekijöitä sen arvioimisessa, voidaanko vastuu siirtää asiakkaalle. Mikäli pankin lähettämä aktivointiviesti, maksun vahvistuspyyntö tai käyttöliittymä on epäselvä eikä asiakas voi kohtuudella ymmärtää toimenpiteen merkitystä, ei vastuun siirtäminen ole perusteltua. FINEn ratkaisuissa on painotettu, että asiakkaan on voitava tunnistaa riskit ja toimia niiden mukaisesti. Jos palvelun rakenne tai viestintätapa mahdollistaa erehdyksen, pankki on laiminlyönyt velvollisuutensa varmistaa turvallinen asiointi. Vastuun arviointi ei siten voi perustua yksinomaan asiakkaan käyttäytymiseen, vaan huomioon on otettava myös pankin luoma toimintaympäristö ja sen riskit. Tämä korostaa tarvetta entistä selkeämmille viesteille, yksiselitteiselle terminologialle sekä käyttöliittymille, jotka

minimoivat virhetulkinnan mahdollisuuden myös kiireisessä tai stressaavassa tilanteessa. Toisen alakysymyksen osalta voidaan siten päätellä, että vastuun siirtyminen asiakkaalle edellyttää paitsi asiakkaan huolimattomuutta, myös sitä, että pankki on täyttänyt omat velvollisuutensa turvallisen ja selkeän asiointiympäristön luomisessa.

Kolmas alakysymys koski huolimattomuuden ja törkeän huolimattomuuden välistä rajanvetoa verkkohuijaustapauksissa. Tämän osalta keskeisenä havaintona on, että kyseinen rajanveto on edelleen vaikeasti määriteltävissä. FINEn linjauksissa törkeän huolimattomuuden kynnys ylittyy yleensä silloin, kun asiakas on sivuuttanut selkeät varoitukset tai luovuttanut tunnuksensa tietoisesti sivulliselle. Sen sijaan tilanteissa, joissa huijaus on ollut poikkeuksellisen uskottava tai pankin viestit vaikeasti erotettavissa oikeista, asiakkaan toiminta on katsottu vain huolimattomaksi. Rajanvetoon vaikuttavat useat tekijät, jotka voidaan jakaa olosuhteisiin, pankin toimintaan ja asiakkaan henkilökohtaisiin ominaisuuksiin liittyviin seikkoihin.

Ensimmäisenä tekijänä on huomioitava olosuhteet, joissa väärinkäytös tapahtuu. Huijausten nopea kehitys ja tekninen monimutkaistuminen ovat muuttaneet merkittävästi sitä kontekstia, jossa huolellisuutta arvioidaan. Rikollisten viestit ja verkkosivut voivat olla niin uskottavia, että jopa huolellinen käyttäjä voi erehtyä pitämään niitä aitoina. Tämä kehitys korostaa pankkien vastuuta palveluidensa turvallisuuden, käyttöliittymien ja asiakasviestinnän kehittämisessä.

Pankin toiminta muodostaa toisen keskeisen arviointikriteerin. Pankkien tekniset ja organisatoriset menettelyt vaikuttavat merkittävästi vastuun jakautumiseen. Kun asiakas on tehnyt ilmoituksen tunnusten väärinkäytöstä, pankin vastuu alkaa välittömästi, ja sen on estettävä välineen käyttö ilman aiheetonta viivytystä. Jos pankin järjestelmät eivät tunnista poikkeavaa maksukäyttäytymistä tai reagoi siihen riittävän nopeasti, ei vastuun siirtäminen asiakkaalle ole oikeudenmukaista. Pankkien riskienhallintavelvoitteet ja rahanpesulain mukainen selonottovelvollisuus tukevat näkemystä, että pankeilla on velvollisuus ehkäistä ja tunnistaa epäilyttävät tapahtumat tehokkaasti. Näin pankin

sisäisten prosessien laatu ja reagointikyky muodostuvat olennaiseksi osaksi vastuuharkintaa. Vaikka maksupalvelulainsäädäntö ei edellytä erikseen reaaliaikaista petostapahtumien monitorointia, pankin on pystyttävä reagoimaan asiakkaan ilmoitukseen sekä muuhun väärinkäyttöä osoittavaan tietoon nopeasti ja tehokkaasti.

Kolmantena tekijänä asiakkaan huolellisuutta arvioitaessa merkitystä voidaan antaa myös hänen henkilökohtaisille ominaisuuksilleen, kuten iälle, digitaaliselle osaamiselle ja kokemukselle maksupalveluiden käyttämisestä. Vaikka maksupalvelulaki ei nimenomaisesti edellytä subjektiivisten tekijöiden huomioon ottamista, vastuunarvioinnissa sovellettava kokonaisarviointi mahdollistaa sen, että arvio huolellisuudesta suhteutetaan siihen, mitä voidaan kohtuudella odottaa kyseiseltä asiakasryhmältä. Esimerkiksi iäkkäiden henkilöiden tai harvoin sähköisiä palveluja käyttävien asiakkaiden ei voida olettaa tunnistavan verkossa tapahtuvia huijausmenetelmiä samalla tarkkuudella kuin säännöllisesti digitaalisia palveluita käyttävien. Tämä ei kuitenkaan tarkoita, että pankin vastuu vähenisi asiakkaan kokemattomuuden perusteella. Päinvastoin asiakkaiden erilaiset valmiudet korostavat pankin velvollisuutta varmistaa, että sen tarjoamat palvelut, viestintä ja turvallisuusohjeet ovat ymmärrettäviä ja saavutettavia kaikille asiakasryhmille. Näin ikä ja digitaalinen kokemus toimivat täydentävinä arviointiperusteina, jotka voivat vaikuttaa siihen, katsotaanko asiakkaan menettelyä huolimattomaksi vai törkeän huolimattomaksi. Kolmannen alakysymyksen osalta voidaan siten todeta, että huolimattomuusarviointi määräytyy tapauskohtaisen kokonaisarvion perusteella, jossa huomioon otetaan huijauksen uskottavuus ja olosuhteet, pankin viestinnän selkeys ja reagointikyky sekä asiakkaan menettely ja henkilökohtaiset ominaisuudet.

Edellä esitetyn perusteella voidaan vastata tutkielman päätutkimuskysymykseen, joka koski vastuun jakautumista tilanteissa, joissa asiakas on verkkohuijauksen uhrina luovuttanut verkkopankkitunnuksensa ja mahdollistanut pankin mobiilisovelluksen käyttämisen maksujen vahvistamiseen rikollisen laitteella.

Voimassa olevan oikeuden näkökulmasta vastuu jakautuu nykyisen sääntelyn ja oikeuskäytännön mukaan kolmen keskeisen arviointikriteerin perusteella. Ensimmäinen kriteeri on se, onko asiakas antanut maksulle tietoisen suostumuksen. Toinen kriteeri koskee sitä, onko asiakas toiminut huolellisesti tunnistusvälineen haltijana. Kolmas kriteeri puolestaan liittyy siihen, onko pankki täyttänyt omat velvollisuutensa turvallisen asiointiympäristön ja selkeän viestinnän osalta.

Tutkimus osoittaa kuitenkin, että vaikka nykyinen sääntely ja oikeuskäytäntö muodostavat perustan vastuunjaolle, ne eivät yksin takaa oikeudenmukaisia ja ennakoitavia lopputuloksia. Tapauskohtainen harkinta aiheuttaa epävarmuutta sekä pankeille että asiakkaille, ja samankaltaisissa tilanteissa voidaan päätyä eri johtopäätöksiin. Jotta oikeusturva ja järjestelmän luotettavuus säilyvät, tarvitaan yhtenäisempiä tulkintalinjoja ja mahdollisesti myös sääntelyn täsmennyksiä, jotka ottavat huomioon digitaalisen asioinnin erityispiirteet.

Tutkielman johtopäätöksenä voidaan esittää, että vastuunjaon tulisi perustua osapuolten todellisiin vaikutusmahdollisuuksiin väärinkäytöksen estämiseksi. Käytännössä tämä merkitsee sen arvioimista, kumpi osapuoli on kulloinkin paremmassa asemassa tunnistamaan riskin ja ehkäisemään vahingon syntymisen. Maksupalvelulain lähtökohtana on asiakkaan vahva suoja, jonka mukaan pankki kantaa pääsääntöisesti riskin oikeudettomista maksutapahtumista. Pankin mahdollisuudet vaikuttaa turvallisuusviestinnän selkeyteen, teknisiin suojamekanismeihin ja poikkeavan maksukäyttäytymisen tunnistamiseen ovat lähtökohtaisesti asiakasta paremmat, mikä puoltaa pankin korostunutta vastuuta palvelun turvallisesta toteuttamisesta. Toisaalta asiakkaan oma toiminta voi ratkaisevasti vaikuttaa vahingon syntymiseen, minkä vuoksi vastuunjaon on kannustettava myös asiakasta huolelliseen menettelyyn tunnistusvälineen säilyttämisessä ja käytössä.

Oikeudellisen vastuun ohella kyse on luottamuksesta. Digitaalisen pankkiasioinnin uskottavuus edellyttää, että asiakkaat voivat asioida turvallisesti ilman kohtuutonta riskiä

joutua petoksen uhriksi. Näin voidaan vahvistaa sekä kuluttajansuojaa että rahoitusjärjestelmän uskottavuutta nopeasti muuttuvassa digitaalisessa ympäristössä.

6.2 Toimintasuositukset

Tutkielman perusteella pankkien ja asiakkaiden välinen vastuunjako oikeudettomien maksutapahtumien yhteydessä ei ole yksiselitteinen. Ratkaisujen hajanaisuus ja huolimattomuuden arvioinnin tulkinnanvaraisuus korostavat tarvetta yhtenäisille toimintamalleille sekä teknisille että oikeudellisille tasoille. Käytännön kehitystoimilla voidaan vähentää väärinkäytösten määrää, lisätä oikeusvarmuutta ja vahvistaa asiakkaiden luottamusta sähköiseen asiointiin. Suositusten tavoitteena on siten tukea sekä pankkien että asiakkaiden toimintaa tavalla, joka pienentää väärinkäytösriskejä ja tehostaa vastuunjaon ennakoitavuutta. Seuraavat suositukset perustuvat tutkielmassa tehtyihin havaintoihin.

Kuten tutkielmassa on osoitettu, pankin viestinnän epäselvyys on ollut keskeinen tekijä vastuunjaon arvioinnissa. Pankkien tulisi kiinnittää erityistä huomiota viestinnän ja käyttöliittymien selkeyteen. Vahvan tunnistamisen ja maksujen vahvistamisen yhteydessä käytettävien viestien on oltava sellaisia, että asiakas voi yksiselitteisesti ymmärtää, mitä toimenpidettä hän on vahvistamassa. Viestien ja vahvistuspyyntöjen tulee erottaa selkeästi maksun hyväksyminen muista toimenpiteistä, kuten tunnistautumisesta tai sovelluksen aktivoinnista. Käyttöliittymissä tulisi korostaa näkyvillä varoituksilla tilanteita, joissa riski huijaukseen on suurentunut, ja erityisesti aktivointikoodien yhteydessä olisi käytettävä selkeitä varoitustekstejä, jotka estävät asiakkaan erehtymisen rikollisen ohjeistuksesta. Ohjeistuksen tulisi olla monikanavaista, visuaalisesti selkeää ja kielellisesti saavutettavaa, jotta se tavoittaa myös ne asiakkaat, jotka eivät seuraa aktiivisesti digitaalisia tiedotteita.

Teknisen riskienhallinnan kehittäminen on olennainen osa pankkien vastuuta. Pankkien tulisi hyödyntää reaaliaikaista maksuliikenteen seurantaa ja riskipohjaisia

tunnistusjärjestelmiä, jotka voivat estää tai viivästyttää epätyypillisiä maksutapahtumia. Poikkeavat siirrot, kuten suuret summat uuteen kohteeseen tai epätavalliseen aikaan, tulisi automaattisesti merkitä tarkastettaviksi ennen maksun toteutumista. Erityistä valvontaa tulisi kohdistaa tilanteisiin, joissa tunnistusväline otetaan käyttöön uudessa laitteessa tai mobiilisovellus rekisteröidään uudelleen, sillä tällaiset tapahtumat ovat tyypillinen väärinkäytösten riskikohta, joka käy ilmi useista FINEn ratkaisusuosituksista.

Pankkien olisi myös panostettava asiakkaiden ohjeistukseen ja tiedon lisäämiseen. Tietoturvaohjeiden tulee olla helposti saatavilla ja ymmärrettäviä, ja niissä olisi korostettava käytännön esimerkkien kautta sitä, että maksun vahvistaminen on aina oikeustoimi, jonka oikeusvaikutukset syntyvät asiakkaan tietoisesta suostumuksesta. Säännölliset viestintäkampanjat ja koulutukset lisäisivät asiakkaiden valmiuksia tunnistaa huijausyrityksiä. Pankkien viestinnän ja palveluiden tulisi olla selkeitä ja saavutettavia kaikille käyttäjäryhmille. Erityistä huomiota tulisi kiinnittää niihin asiakasryhmiin, joilla on vähemmän kokemusta sähköisestä asioinnista, kuten iäkkäisiin henkilöihin tai harvoin digitaalisia palveluja käyttäviin asiakkaisiin, ja jotka ovat siksi alttiimpia rikollisten vaikutukselle. Pankkien tulisi tarjota näille ryhmille mahdollisuus henkilökohtaiseen neuvontaan ja harkita vaihtoehtoisia tunnistautumismenetelmiä.

Myös asiakkailla on keskeinen rooli väärinkäytösten ehkäisemisessä. Pankkitunnuksia ja mobiilisovelluksia on käytettävä huolellisesti ja vain pankin virallisten kanavien kautta. Asiakkaan on tiedostettava, että pankkitunnuksilla tehty vahvistus merkitsee oikeudellisesti sitovaa tahdonilmaisua. Tunnuksia ei tule syöttää verkkosivuille, joiden aitoudesta ei ole varmuutta, eikä linkkien kautta tulleita pyyntöjä pidä noudattaa. Jos asiakas saa pankilta yllättäen viestin tai aktivointikoodin, hänen tulee varmistaa sen oikeellisuus ottamalla välittömästi yhteyttä pankkiin virallisten kanavien kautta eikä vastaamalla viestiin.

Asiakkaiden tulee lisäksi muistaa ilmoitusvelvollisuutensa. Jos tunnusten väärinkäyttöä epäillään, ilmoitus on tehtävä viipymättä. Ilmoituksen nopeus on ratkaiseva tekijä

vastuun siirtymisessä pankille, joten yhteystiedot pankin asiakas- tai sulkupalveluun on syytä pitää helposti saatavilla myös tilanteissa, joissa omat laitteet eivät ole käytettävissä. Samalla asiakkaiden kannattaa hyödyntää pankkien tarjoamia turvatoimia, kuten siirtorajoja, ilmoituksia uusista maksunsaajista sekä muita ilmoitus- ja seurantapalveluja, jotka auttavat havaitsemaan poikkeavia maksutapahtumia. On myös suositeltavaa ottaa käyttöön mahdolliset ilmoitukset uusista maksuista ja maksurajojen muutoksista, mikäli pankki tarjoaa tällaisia palveluja. Myös laitteiden ohjelmistojen päivittäminen ja vahvojen pääsykoodien käyttö ovat olennaisia osia turvallista asiointia. Asiakkaiden vastuulla on lisäksi seurata pankkien tiedotteita ja lukea huolellisesti viestit, joissa varoitetaan ajankohtaisista huijausmenetelmistä tai annetaan ohjeita turvalliseen asiointiin, sillä tietoisuuden ylläpitäminen on olennainen osa huolellista toimintaa.

Tutkielmassa havaittu tulkintojen hajanaisuus huolimattomuuden ja törkeän huolimattomuuden arvioinnissa osoittaa tarpeen sääntelyn täsmentämiselle. Lainsäätäjän ja valvontaviranomaisten tehtävänä on varmistaa, että pankkien ja asiakkaiden välinen vastuunjako pysyy johdonmukaisena ja oikeudenmukaisena. Maksupalvelulain säännöksiä huolimattomuuden ja törkeän huolimattomuuden arvioinnista olisi syytä tarkentaa esimerkiksi hallituksen esityksen tai viranomaisohjeistuksen tasolla. Tällä hetkellä tulkinnanvaraisuus johtaa epäyhtenäisiin ratkaisuihin, mikä heikentää oikeusvarmuutta. Yhtenäinen indikaatioluettelo huolimattomuuden arvioinnissa huomioon otettavista seikoista lisäisi ennustettavuutta ja tukisi sekä pankkien että asiakkaiden asemaa.

Lisäksi viranomaiset voisivat määrittää vähimmäistason pankkien turvallisuusviestinnälle. Finanssivalvonnan ja Liikenne- ja viestintäviraston yhteistyössä laatimat ohjeet yhtenäistäisivät pankkien toimintaa ja varmistaisivat sen, että asiakkaat saavat olennaiset varoitukset samassa muodossa riippumatta palveluntarjoajasta. Pankeille voitaisiin myös asettaa velvollisuus raportoida viranomaisille ja toisilleen havaituista huijausmenetelmistä ja niiden torjuntakeinoista, jotta parhaat käytännöt ja

tehokkaimmat ratkaisut leviäisivät koko toimialalle. Tulee kuitenkin ottaa huomioon, että osa tiedoista voidaan katsoa pankki- tai yrityssalaisuuden piiriin.

Pankkien välinen tiedonvaihto edellyttää huomion kiinnittämistä pankki- ja liikesalaisuuden suojaan sekä henkilötietojen käsittelyä koskeviin rajoituksiin. Pankkien on löydettävä ratkaisuja, joilla petosuhkiin liittyvää tietoa voidaan jakaa viranomaisten ja toimialan sisällä tavalla, joka ei paljasta yksittäisiä asiakkaita koskevaa luottamuksellista tietoa eikä vaaranna pankkien liikesalaisuuksia. Tiedonvaihto tulee siten toteuttaa ensisijaisesti anonymisoidussa tai muuten suojatussa muodossa. Toisaalta se, että lainsäädäntö turvaa pankki- ja liikesalaisuuden, ei voi muodostua esteeksi turvallisuusviestinnän kehittämiselle, vaan näiden intressien tasapainoinen yhteensovittaminen on osa pankin huolellisuus- ja riskienhallintavelvoitteita. Tiedonvaihdon kehittämistä voidaan näin pitää yhtenä tulevaisuuden keskeisimmistä keinoista vahvistaa koko rahoitusjärjestelmän kykyä torjua petoksia ja lisätä asiakkaiden luottamusta sähköisiin palveluihin.

Yhteenvetona voidaan todeta, että pankkien ja asiakkaiden velvollisuudet täydentävät toisiaan. Pankkien on luotava turvallinen ja ymmärrettävä asiointiympäristö, jossa virheiden ja erehdysten mahdollisuus on minimoitu, kun taas asiakkaiden on toimittava huolellisesti ja noudatettava pankin antamia ohjeita. Lainsäätäjän ja viranomaisten roolina on huolehtia siitä, että näitä velvollisuuksia tulkitaan yhdenmukaisesti ja että vastuunjaon perusteet säilyvät selkeinä myös muuttuvassa digitaalisessa toimintaympäristössä. Näiden toimenpiteiden avulla voidaan vahvistaa asiakkaansuojaa, parantaa riskienhallintaa ja lisätä luottamusta sähköiseen pankkijärjestelmään.

Lähteet

Alasoini, T. (2015). Digitalisaatio muuttaa työtä – millaista työelämää uudistavaa innovaatiopolitiikkaa tarvitaan? *Työpoliittinen aikakauskirja 02/2015*. Noudettu 23.1.2025 osoitteesta https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/e9a23c74-3195-490d-bcd9-04718b39c11e/content

Digihuijaukset jo huumerikollisuutta kannattavampia – pankeilta vaaditaan estotoimia sekunneissa, mutta torjuntaan on valjastettava muitakin. Finanssiala ry. Noudettu 10.12.2025 osoitteesta https://www.finanssiala.fi/uutiset/digihuijaukset-jo-huumerikollisuutta-kannattavampia/

Electronic identification. (2024). European Commission. Noudettu 25.2.2025 osoitteesta https://digital-strategy.ec.europa.eu/en/policies/electronic-identification

Euroopan talousalue. (2022). Patentti- ja rekisterihallitus. Noudettu 29.1.2025 osoitteesta https://www.prh.fi/fi/kaupparekisteri/useinkysytyt/euroopan_talousalue_eta.html

FINE, mitä teemme, missä ja miten voimme auttaa? (n.d.). Vakuutus- ja rahoitusneuvonta. Noudettu 26.1.2025 osoitteesta https://www.fine.fi/oppaat/julkaisu/fine-mita-teemme-missa-ja-miten-voimme-auttaa

FINE Vuosikertomus 2023. (2024). Vakuutus- ja rahoitusneuvonta. Noudettu 26.1.2025 osoitteesta https://www.fine.fi/tietoa-finesta/vuosikertomukset/fine-vuosikertomus-2023.html

Hemmo, M., & Hoppu, K. (2006). *Sopimusoikeus*. WSOYpro.

Hirvonen, A. (2011). *Mitkä metodit?: Opas oikeustieteen metodologiaan. [Ari Hirvonen].*

Huijareilla oli aktiivinen vuosi 2023 – Pankit saivat estettyä digihuijauksia lähes 33 miljoonan euron edestä. (2024). Finanssiala ry. Noudettu 3.3.2025 osoitteesta https://www.finanssiala.fi/uutiset/huijareilla-oli-aktiivinen-vuosi-2023-pankit-saivat-estettya-digihuijauksia-lahes-33-miljoonan-euron-edesta/

Huijaukset rajussa kasvussa vuonna 2024 – pankit saivat pysäytettyä huijattuja maksuja yli 44 miljoonan euron arvosta. (2025). Finanssiala ry. Noudettu 3.3.2025 osoitteesta https://www.finanssiala.fi/uutiset/huijaukset-rajussa-kasvussa-vuonna-2024-pankit-saivat-pysaytettya-huijattuja-maksuja-yli-44-miljoonan-euron-arvosta/

Huijausten selvittäminen ja ratkaisukäytännöt FINEssä. (2024). Vakuutus- ja rahoitusneuvonta. Noudettu 26.1.2025 osoitteesta https://www.fine.fi/oppaat/julkaisu/huijausten-selvittaminen-ja-ratkaisukaytannot-finessa.html

Husa, J., Mutanen, A., & Pohjolainen, T. (2008). *Kirjoitetaan juridiikkaa: Ohjeita oikeustieteellisten kirjallisten töiden laatijoille* (2. uud.p.). Talentum.

Hyvä pankkitapa. (2025). Finanssiala ry. Noudettu 19.9.2025 osoitteesta https://www.finanssiala.fi/aiheet/hyva-pankkitapa/

Hämäläinen, V-P. (2022). *Pankki syytti uhreja, kun pariskunta menetti huijarille 45 000 euroa – ”Ei voi sanoin kuvata, miltä se tuntuu”.* Yle. Noudettu 26.1.2025 osoitteesta https://yle.fi/a/74-20000848

Hämäläinen, V-P. (2023). *Huijari vei pariskunnalta kymmeniä tuhansia euroja, pankki syytti uhreja – nyt oikeus määräsi pankin maksajaksi.* Yle. Noudettu 26.1.2025 osoitteesta https://yle.fi/a/74-20048842

Kyberrikollisuus ylittää rajat tietoverkossa. (n.d.). Sisäministeriö. Noudettu 24.1.2025 osoitteesta https://intermin.fi/poliisiasiat/kyberrikollisuus

Lappi, M., Tykkä, M., Hidén, T. Heino, S., Sainio, V. ja Antila, E. (2024). *Huijausten selvittäminen ja ratkaisukäytännöt FINEssä.* Noudettu 21.10.2025 osoitteesta https://www.fine.fi/oppaat/julkaisu/huijausten-selvittaminen-ja-ratkaisukaytannot-finessa.html

Maksaminen ja tilit. (n.d.). Vakuutus- ja rahoitusneuvonta. Noudettu 14.1.2025 osoitteesta https://www.fine.fi/naissa-asioissa-autamme/maksaminen-ja-tilit.html

Mikä on Nordea ID -sovellus? (n.d.). Nordea. Noudettu 25.2.2025 osoitteesta https://www.nordea.fi/henkiloasiakkaat/palvelumme/verkko-mobiilipalvelut/tunnuslukusovellus.html

Mitä on tietojenkalastelu eli phishing? Näin verkkourkinta toimii. (2022). F-Secure. Noudettu 24.1.2025 osoitteesta https://www.f-secure.com/fi/articles/what-is-phishing

Mobiiliavain. (n.d.). Osuuspankki. Noudettu 25.2.2025 osoitteesta https://www.op.fi/henkiloasiakkaat/digitaaliset-palvelut/mobiiliavain

Määräykset ja ohjeet 20/2023. Rahanpesun ja terrorismin rahoittamisen estäminen. Finanssivalvonta. FIVA/2023/1289. Noudettu 12.2.2025 osoitteesta https://www.finanssivalvonta.fi/globalassets/fi/saantely/maarayskokoelma/2023/02_2023/02_2023.M2.pdf

Nikkanen, V. (2024). *Anteron, 84, tililtä vietiin 64 000 euron eläkesäästöt – näin huijaus eteni*. MTV Uutiset. Noudettu 29.1.2025 osoitteesta https://www.mtvuutiset.fi/artikkeli/anteron-84-tililta-vietiin-64-000-euron-elakesaastot-nain-huijaus-eteni/8866986

Nordea Bank Oyj. (2024). *Nordean vuosiraportointi 2023*. Noudettu 23.1.2025 osoitteesta https://www.nordea.com/fi/media/2024-02-26/nordean-vuosiraportointi-2023

Näin pankkien markkinaosuudet asuntolainoissa muuttuivat – Yhden pankin siivu kasvoi peräti 48 %. (2025) Kauppalehti. Noudettu 4.5.2025 osoitteesta https://www.kauppalehti.fi/uutiset/nain-pankkien-markkinaosuudet-asuntolainoissa-muuttuivat-yhden-pankin-siivu-kasvoi-perati-48/811ef416-1a2f-49be-87ea-1e7890cf8773.

Ojanen, T. (2016*). EU-oikeuden perusteita (3., uudistettu laitos.*). Edita Publishing Oy.

OP-Mobiili. (n.d.). Osuuspankki. Noudettu 9.3.2025 osoitteesta https://www.op.fi/henkiloasiakkaat/digitaaliset-palvelut/op-mobiili

OP:n tunnus- ja digisopimuksen ehdot. (2025) Osuuspankki. Noudettu 1.8.2025 osoitteesta

https://www.op.fi/tac?did=Hesah0000002701&cs=a5f016c17abe17349b418063eb32ad004f41c0e595ec5edc4b00b67b241fad91

Pankkitunnuksilla käytettävien palvelujen yleiset sopimusehdot. MMST96DL 03.25. (2025) Nordea. Noudettu 4.8.2025 osoitteesta https://www.nordea.fi/Images/146-480869/MMST960DL.pdf

Saarnilehto, A., & Annola, V. (2018). *Sopimusoikeuden perusteet* (8., uudistettu painos.). Alma Talent.

Selvitys peruspankkipalveluiden saatavuudesta ja hinnoittelusta vuonna 2023. (2024). Finanssivalvonta. Noudettu 23.1.2025 osoitteesta selvitys-peruspankkipalveluiden-saatavuudesta-ja-hinnoittelusta-vuonna-2023-netti.pdf

Suomessa toimivien luottolaitosten markkinaosuudet. (2024). Suomen Pankki. Noudettu 29.1.2024 osoitteesta https://www.suomenpankki.fi/fi/tilastot/taulukot-ja-kuviot/rahalaitosten-tase-lainat-ja-talletukset-ja-korot/taulukot/rati-taulukot-fi/markkinaosuudet_luottolaitokset_fi/

Sähköiset maksutavat. Suomen Pankki. Noudettu 14.2.2025 osoitteesta https://www.suomenpankki.fi/fi/raha-ja-maksaminen/maksaminen/sahkoiset-maksutavat/

Sähköinen tunnistaminen. (2025). Kyberturvallisuuskeskus. Noudettu 25.2.2025 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen

Säästöpankki tunnistus. (n.d.). Säästöpankki. Noudettu 25.2.2025 osoitteesta https://www.saastopankki.fi/fi-fi/asiakaspalvelu/yhteydenottokanavat/saastopankki-tunnistus

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

Palmgren, J. (2020). *Korona-aika lisäsi sähköisten pankkipalvelujen käyttöä jopa kymmenillä prosenteilla*. Noudettu 23.1.2025 osoitteesta https://www.finanssiala.fi/uutiset/korona-aika-lisasi-sahkoisten-pankkipalvelujen-kayttoa-jopa-kymmenilla-prosenteilla/

PSD2. (2023). Finanssivalvonta. Noudettu 14.2.2025 osoitteesta https://www.finanssivalvonta.fi/saantely/saantelykokonaisuudet/psd2/

Varo, varmista, varoita -kampanja: Digihuijausten määrä kasvoi selvästi vuoden 2022 jälkipuoliskolla. (2023). Finanssiala ry. Noudettu 3.3.2025 osoitteesta https://www.finanssiala.fi/uutiset/varo-varmista-varoita-kampanja-digihuijausten-maara-kasvoi-selvasti-vuoden-2022-jalkipuoliskolla/

Viljanen, J. (2004). *Oikeudellisten tutkimusten kirjoittamisopas*. Oikeustieteiden laitos.

Voutilainen, T. (2020). *Digitaalisten palvelujen sääntely*. Alma Talent.

Wuolijoki, S. (2022). *Pankkioikeus: I* (3., uudistettu painos.). Alma Talent.

Wuolijoki, S. (2023). *Pankkioikeus: II* (3., uudistettu painos.). Alma Talent.

Wuolijoki, S. (2009). *Pankin neuvontavastuu: Varallisuusoikeudellinen tutkimus pankin neuvonta- ja tiedonantovelvollisuuksista*. CC Lakimiesliiton kustannus.

Tilin yleiset ehdot. (2024). Nordea. Noudettu 28.2.2025 osoitteesta https://www.nordea.fi/Images/146-260862/henkiloasiakkaan-tilien-yleiset-ehdot-fi.pdf

Virallislähteet

Euroopan parlamentin ja neuvoston direktiivi 2007/64/EY, annettu 13 päivänä marraskuuta 2007, maksupalveluista sisämarkkinoilla, direktiivien 97/7/EY, 2002/65/EY, 2005/60/EY ja 2006/48/EY muuttamisesta ja direktiivin 97/5/EY kumoamisesta

Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/2366 maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/1001/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta.

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

HE 52/2021 vp. Hallituksen esitys eduskunnalle laiksi rikoslain 37 luvun muuttamisesta.

HE 132/2017 vp. Hallituksen esitys eduskunnalle laiksi maksupalvelulain muuttamisesta ja eräiksi siihen liittyviksi laeiksi.

HE 169/2009 vp. Hallituksen esitys Eduskunnalle maksupalvelulaiksi ja eräiksi siihen liittyviksi laeiksi.

Oikeustapausluettelo

Itä-Suomen HO 13.11.2024 t. 462

Vaasan HO 19.9.2024 t. 342

Satakunnan käräjäoikeus 6.9.2023 L 747/2022/1499

Pankkilautakunnan ratkaisusuositukset

FINE-043423

FINE-049807

FINE-058023

FINE-65394-H0X4X