III. Päläs, Jenna, and Mirva Salminen (2019) Alustan asiakkaan vastuusta ja vastuuttamisesta yksilöturvallisuuden tuottamisessa – sopimusoikeudellinen näkökulma kyberturvallisuuteen jakamistaloudessa. In: Päläs, Jenna, and Kalle Määttä (Eds.) *Jakamistalousjuridiikan käsikirja*. Helsinki: Alma Talent, 319–380.

Jenna Päläs ja Mirva Salminen[1]

ALUSTAN ASIAKKAAN VASTUUSTA JA VASTUUTTAMISESTA YKSILÖTURVALLISUUDEN TUOTTAMISESSA – SOPIMUSOIKEUDELLINEN NÄKÖKULMA KYBERTURVALLISUUTEEN JAKAMISTALOUDESSA

1 Johdanto

Modernille jakamistaloudelle tyypillinen piirre on taloudellisen yhteistoiminnan ja yhteistyömuotojen kytkeytyminen digitaaliseen toimintaympäristöön, erityisesti sähköisille verkkoalustoille, jotka fasilitoivat käyttäjiensä välistä vaihdantaa ja muita taloudellisen toiminnan muotoja.[2] Sähköisen toimintaympäristön turvallisuus ja luotettavuus ovat tietoverkkojen varaan rakennetussa arvonluonnissa keskeinen tekijä – kyberturvallisuudesta on tullut tärkeä osa toimivan yhteiskunnan rakenteita. Kyberturvallisuus voidaan nähdä erityisesti jakamistaloudessa taloudellisen toiminnan mahdollistajana ja ylläpitäjänä. Nimittäin alustoihin ja niillä tapahtuvaan vaihdantaan kohdis-

[1] Tämä kirjoitus on yhteiskuntatieteilijän ja oikeustieteilijän keskustelun ja ihmettelyn tulos. Kummatkin kirjoittajat ovat vastanneet johdantoluvun ja johtopäätöksien kirjoittamisesta. Mirva Salminen on taustoittanut kyberturvallisuuden, yksilöturvallisuuden ja vastuuttamisen yhteiskunnallisia kysymyksiä sekä kirjoittanut kokonaisuudessaan luvun 2. Jenna Päläs on vastannut kirjoituksen oikeustieteellisestä osuudesta ja analyysistä, ja hän on kirjoittanut luvut 3–6.

[2] Ks. Hamari ym. 2015. Verkkoalustoilla tarkoitetaan tyypillisesti sekä sähköistä infrastruktuuria että alustan tarjoavaa tai ylläpitävää organisaatiota tai muuta toimijaa. Verkkoalustoille rakentuvaa vaihdantaa voidaan lähestyä myös alustatalouden käsitteestä käsin. Alustataloudesta ja verkkoalustojen käsitteestä ks. COM(2016) 288 final sekä Srnicek 2017.

tuva luottamus edellyttää riittävää turvallisuuden tasoa etenkin, kun jakamistalouteen osallistuvilla on tietoverkkoihin kytköksissä olevaa varallisuutta tai tietoja, joilla on varallisuusoikeudellista arvoa.[3]

Yksilöiden merkityksen kyberturvallisuuden tuottamisessa on nähty kasvavan, sillä ihmisten heikkouksien hyväksikäyttö on noussut teknisten tietoturvauhkien rinnalle – tai niiden ohi.[4] Globaalisti verkottuneessa digitaalisessa toimintaympäristössä turvallisuuden tuottamisen katsotaan kuuluvan kaikille yksittäisistä ihmisistä organisaatioihin, valtioihin sekä yli-, poikki- ja monikansallisiin toimijoihin asti. Ihmisten, laitteiden, palveluiden, organisaatioiden tai muiden vastaavien kytkeytyminen toisiinsa aiheuttaa kompleksisessa ympäristössä tilanteen, jossa kokonaisuuden turvaamista ei mikään toimija pysty hoitamaan yksin, vaan tarvitaan jokaisen panosta ja hajautettua vastuun kantamista.[5] Myös mediakeskusteluissa on nostettu esiin yksilön rooli ja toiminta digitaalisessa toimintaympäristössä.[6] Kyberturvasta on puhuttu jopa kansalaistaitona. Teknisen

[3] Tällaisia tietoja tai varallisuutta ovat mm. sähköpostitiedot, kuluttajan päätelaite, verkossa olevat tilit ja käyttäjätiedot, identiteetti, maksuvälineet, rahavarat sekä virtuaalinen omaisuus. ks. Peltomäki – Norppa 2015, s. 59 ss.

[4] Ks. Kyberturvallisuuskeskus 2019, s. 43. Ihmisten käyttäytymisen ja osaamisen lisäksi kuluttajalaitteiden tietoturva korostuu turvallisuuden ja luottamuksen rakentamisessa. Myös konsultointi- ja ICT-alan yritykset ovat tuoneet esiin kyberkouluttamisen tarvetta, esim. Rosenthal 2018; ISMG n/d.

[5] Dunn Cavelty 2007, s. 23–24, Limnéll ym. 2014, s. 13–14 ja 45–62, Lewis 2015, s. 93–94 ja 111–113 sekä Mueller 2017, s. 6–8 ja 15. Suomen kyberturvallisuusstrategiassa (SKTS) (2013, s. 5) esitettyjen periaatteiden mukaan ”[k]yberturvallisuus perustuu koko yhteiskunnan tietoturvallisuuden järjestelyihin. Kyberturvallisuuden edellytys on jokaisen kybertoimintaympäristössä toimivan toteuttamat tarkoituksenmukaiset ja riittävät tietojärjestelmien ja tietoverkkojen turvallisuusratkaisut.” Ks. Kyberturvallisuuskeskus 2019, s. 3, jossa korostuu inhimillisen kyberturvan merkitys digitaalisen ympäristön luottamuksen rakentumisessa.

[6] Kyberturvallisuudesta käytävässä keskustelussa ihminen mainitaan usein erehtyväisyytensä vuoksi turvallisuuden heikoimmaksi lenkiksi, esim. *Chief Executive,* 3.3.2017, ”Almost 90% of Cyber Attacks are Caused by Human Error or Behavior”; *CNBC,* 21.6.2018, ”The biggest cybersecurity risk to US businesses is employee negligence, study says”; *The Conversation*, 10.8.2018, ”Hackers cause most data breaches, but accidents by normal people aren’t far behind”; *Computer Business Review*, 3.9.2018 ”Revealed: Human Error, Not Hackers, to Blame for Vast Majority of Data Breaches”. Toisaalta ihmisen syyllistämistä myös kritisoidaan, esim. *Slate*, 22.1.2016, ”Calling Humans the ‘Weakest Link’ in Computer Security Is Dangerous and Unhelpful”; *ZDNet*, 22.2.2017, ”IT security breaches: Why users shouldn't take all the blame anymore”.

osaamisen ohella tarvitaan tällöin ihmisten osaamista ja käyttäytymistä painottavia ratkaisuja.[7] Ajatus digitaalisen toimintaympäristön kansalaistaidoista pitää sisällään yksilöön kohdistuvan vaatimuksen tietystä osaamis- ja huolellisuustasosta – toisin sanoen yksilön vastuusta ja yksilön vastuuttamisesta turvallisuuden tuottamisen osalta. Vastavuoroisesti digitalisaation on ajateltu vahvistavan yksilön asemaa lisäämällä hänen tiedon saantiaan ja vahvistamalla hänen arviointikykyään tietokoneen laskentakyvyn tullessa jokaisen käyttöön.[8] Sosiaalisen median etenkin on katsottu voimaannuttavan ihmisiä ja mahdollistavan ilmiöiden, intressien ja ongelmien esiin tuomisen.[9]

Tämä artikkeli tarjoaa yhden näkökulman yksilön vastuuseen digitaalisen toimintaympäristön turvallisuuden tuottamisessa. Kyberturvallisuuskeskustelun valtavirrasta poiketen artikkelissa ei keskitytä teknisiin tai strategisiin turvallisuushaasteisiin,[10] vaan yksilöturvallisuuteen jakamistalouden alustojen käyttäjän näkökulmasta. Oikeudellisessa keskustelussa kyberturvallisuutta on käsitelty lähinnä kansainvälisen oikeuden näkökulmasta taikka rikosvastuuseen tai tieto-

7 Limnéll ym. 2014, s. 14. Ks. Kyberturvallisuuskeskus 2019, s. 40 ss., jossa kyberturvataidot nähdään kansalaistaitoina, ja kansalaiskampanjoita esitetään ratkaisuksi yksilöiden tietoturvaosaamisen lisäämiseen ja kyberuhkien torjumiseen.

8 Dunn Cavelty 2007, s. 30.

9 Ks. esim. Smith ym. 2015, Saariketo 2015, s. 132 ja Li 2016; vrt. van Dijck – Poell 2013.

10 Tekninen lähestymistapa keskittyy tiedon luottamuksellisuuden, eheyden ja saatavuuden turvaamiseen tietojärjestelmissä. Ratkaisukeinoja ovat tällöin tekniset, hallinnolliset ja koulutukselliset keinot, joilla pyritään vastaamaan tietoturvauhkiin kuten haittaohjelmat, tietomurrot tai digitaalinen vakoilu. Strateginen lähestymistapa katsoo kyberturvallisuutta yhteiskunnan ja/tai valtion tasolta pyrkien varmistamaan yhteiskunnan toimivuuden – elintärkeät toiminnot tai kriittisen infrastruktuurin – uhkia kuten kyberrikollisuus, kansallinen tai taloudellinen vakoilu, informaatiovaikuttaminen tai kyberoperaatiot yhteiskuntaa vastaan. Ks. esim. Salminen 2018. Tieto-, informaatio-, kyber- ja digitaalinen-etuliitteellisten käsitteiden jaottelu ei ole yksiselitteistä, vaan niitä käytetään paljon rinnakkain ja päällekkäin sekä määritellään erisisältöisesti, mikä olennaisesti lisää sekavuutta kyberturvallisuuden ympärillä käytävässä keskustelussa (Dunn Cavelty 2007, s. 20 ja 22).

suojasääntelyyn liittyvänä kysymyksenä.[11] Tämä kirjoitus pyrkii jäsentämään turvallisuuden tuottamista sopimusoikeudellisen vastuun- ja riskinjaon perusteiden näkökulmasta: keskiössä eivät tällöin ole esimerkiksi alustojen tai palveluntarjoajien vastuu oman suorituksensa virheettömyydestä, alustojen ylläpitäjien tietoturvallisuus tai tietosuojakysymyksistä huolehtiminen, vaan alustan käyttäjien oma toiminta sekä vaadittava huolellisuuden taso digitaalisessa toimintaympäristössä.[12]

Tässä artikkelissa esitetään, että voimassa oleva oikeus edellyttää alustoilla toimivilta yksilöiltä tiettyä huolellisuuden, osaamisen ja ymmärryksen tasoa, mikä ilmenee sopimusoikeudellisina velvollisuuksina toimia huolellisesti ja riskejä ennaltaehkäisevästi, sekä toiseksi vastuuna omasta toiminnastaan seuraavista riskeistä ja vahingoista. Sanottu näkyy erityisesti maksu-, viestintä- ja tunnistuspalveluiden oikeudetonta käyttöä koskevassa sääntelyssä. Erilaiset maksuvälineet, älypuhelinliittymät ja -sovellukset, näihin kytketyt rahoitusratkaisut ja tunnistamisen menetelmät ovat olennainen osa digitaalista vaihdantaa ja sopimista, ja siten myös modernia jakamistaloutta: Jakamistalouteen osallistuminen edellyttää tilanteesta riippuen osapuolten heikkoa tai vahvaa tunnistautumista. Alustojen välityksellä tarjottavien palveluiden tai tavaroiden maksaminen edellyttää digitaalista maksupalveluiden tai rahoituspalveluiden käyttöä. Kuitenkin digitaalisessa ympäristössä, kuten alustoilla, käyttäjät kohtaavat uudenmuotoisia uhkia ja riskejä. Yksi keskeinen uhka on edellä mai-

[11] Rikosoikeuden näkökulmasta ja identiteettivarkaudesta ks. Soininen 2017. Tietosuojasta ks. Korpisaari ym. 2018. Kansainvälisessä oikeudessa kyberturvallisuutta on käsitelty lähinnä ei-sitovissa käytänteissä kuten Tallinnan manuaalit (Tallinn Manual on the International Law Applicable to Cyber Warfare [2013] ja Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations [2017]). Ks. myös esim. Tsagourias – Buchan 2015 ja Svantesson 2016. Euroopan unionin tasolla Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus ETS No. 185 (Budapestin sopimus, 2001) ja yleinen tietosuoja-asetus 2016/679/EU (GDPR) ovat keskeisiä kyberturvallisuutta koskevia säädöksiä.

[12] Tässä artikkelissa tutkimusaihetta lähestytään etenkin ongelmakeskeisestä lainopista käsin. Ongelmakeskeisessä lainopissa systematisoidaan kokonaisuus jonkin peruskysymyksen suhteen, jotta saadaan kokonaiskuva niistä tekijöistä, jotka vaikuttavat säänneltävän kohteen vastuun sisällön muotoutumiseen. Lainopin suorittama perustutkimus muodostaa ikään kuin tutkimuksellisen perustan, jota ongelmakeskeinen lainoppi täydentää. Ks. esim. Kangas 1982, s. 386–387.

nittujen vaihdannassa käytettävien välineiden oikeudeton käyttö muun muassa petostarkoituksessa.[13]

Artikkelin tutkimuskysymyksenä on, millä edellytyksillä käyttäjälle syntyy vastuu maksuvälineiden, luoton käyttöön oikeuttavien tunnisteiden, viestintäpalveluiden ja tunnistusvälineiden oikeudettomasta käytöstä. Tässä yhteydessä on korostettava, että käytännössä oikeudettoman käytön kohdalla käyttäjä on joutunut rikoksen uhriksi. Tällä ei kuitenkaan ole merkitystä käyttäjän oman vastuun arviointiin,[14] vaan tästä huolimatta yksilöllä on sääntelyyn ja sopimukseen perustuvia toimintavelvoitteita oikeudettomalta käytöltä suojautumisessa ja oikeudettoman käytön riskin minimoisessa. Käyttäjien huolellisuuden ja riskien hallinnan tasoa on määritelty maksupalvelulaissa (290/2010, MPL), kuluttajansuojalain (38/1978, KSL) 7 luvun 40 §:ssä, laissa sähköisen viestinnän palveluista (917/2014, SVPL) sekä laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009, Tunnistuslaki). Toisin sanoen artikkelin tarkoituksena on selvittää, millaisia toimintavelvollisuuksia oikeudetonta käyttöä koskeva sääntely asettaa yksilöille, miten niitä on tulkittu oikeuskäytännössä ja miten nämä toimintavelvollisuudet konkretisoituvat digitaalisilla alustoilla. Artikkelin kokonaisvaltaisempana tavoitteena on tarkastella, onko kyberturvallisuuskeskustelussa tarkemmin pohdittu, millaista ”digitaalisten kansalaistaitojen” tasoa jakamistalouden alustojen käyttäjiltä voidaan odottaa ja kuinka hyvin heidän voidaan olettaa tunnistavan digitaalisen maailman uhkat ja riskit.

Oikeudettoman käytön tilanteita koskevaa sääntelyä lähestytään siten yksilöturvallisuuden ja alustojen käyttäjien vastuuttamisen näkökulmasta. Aluksi selvitetään, mitä kyberturvallisuus ja yksilöturvallisuus digitaalisessa toimintaympäristössä ovat sekä mitä yksilön

13 Ks. esim. Peltomäki – Norppa 2015, s. 34–35. Oikeudetonta käyttöä voi edeltää mm. luottokortin anastaminen tai sen käytön mahdollistavien tietojen urkkiminen älypuhelimesta.

14 Rikoksentekijän vastuu on kuitenkin erillistä suhteessa maksuvälineen haltijan vastuuseen, jolloin käyttäjä voikin sopimuksen tai lain perusteella joutua vastuuseen, vaikka oikeudeton käyttö täyttäisi rikoslaissa (39/1889, jäljempänä RL) rangaistavaksi säädetyn teon tunnusmerkistön. Koska tämän artikkelin tutkimuskohteena on tunnistusvälineiden haltijan vastuu yksilöturvallisuuden tuottamisesta, tunnistusvälineitä oikeudettomasti käyttävän henkilön vastuun tarkastelu jää artikkelin ulkopuolelle.

vastuuttamisella tässä ympäristössä tarkoitetaan. Tämä luo pohjan yksilön vastuuttamisen oikeudelliselle tarkastelulle. Oikeudettoman käytön tilanteita koskevan sääntelyn ja oikeuskäytännön tarkastelulla selvitellään, miten yksilön vastuuttaminen turvallisuuden tuottamisessa ilmenee sääntelyn tasolla. Tämän vuoksi tarkastellaan, millaisia toimintavelvollisuuksia, huolellisuusvelvoitteita ja varotoimenpiteitä MPL, SVPL, KSL 7 luvun 40 § ja Tunnistuslaki sisältävät käyttäjien näkökulmasta sekä arvioidaan näiden vastuujärjestelmien eroja. Tämä tarkastelu painottaa erityisesti kuluttaja-asiakkaiden ja palveluntarjoajan välisiä vastuun- ja riskinjakokysymyksiä.[15] Lopuksi pohditaan, millaisia johtopäätöksiä vallitsevasta oikeustilasta voidaan tehdä yksilön riittävän kyberturvallisuuden tietotaidon määrittämiseksi. Artikkelissa ei pyritä kokonaisvaltaisesti määrittelemään yksilöiltä vaadittavaa ”digitaalisten kansalaistaitojen” tasoa, eikä myöskään arvioida sitä, missä kohtaa kansalaisen ”liialliset” digitaaliset taidot muodostuvat uhkaksi tai sellaiseksi erityisosaamiseksi, jonka varaan yhteiskunnan tulevaisuutta rakennetaan.

2 Kyberturvallisuuden käsite ja yksilön vastuuttaminen

Jakamistalouden alustoilla käytävä vaihdanta korostaa yksilöiden toiminnan merkitystä. Jakamistalouden onkin katsottu nivoutuvan osaksi yksilökeskeistä yhteiskunnan hallintajärjestelmää, jossa hallinta

[15] Tärkeä jatkotutkimuksen aihe on kuluttaja- ja elinkeinoharjoittaja-asiakkaiden vastuuperusteiden eroavaisuuksien jäsentely. Monet säännökset ovat ns. vähimmäispakottavia kuluttajan hyväksi. Esimerkiksi pienyrittäjän asemassa olevan maksupalvelunkäyttäjän kohdalla voidaan sopia MPL:n sääntelystä poikkeavalla tavalla. Jakamistaloudessa resursseja tarjoavien kuluttajansuojaoikeudellinen asema voi olla haasteellista määrittää, sillä resurssientarjoajien toiminnassa voi olla elinkeinonharjoittamisen elementtejä, mutta sopimusasemaltaan heillä on samanlainen suojan tarve kuin kuluttajilla tai vaikkapa työntekijöillä. Toiseksi palvelusuorituksia ja alustakeikkaa tekevät yksilöt eivät välttämättä miellä toimivansa yrittäjinä tai elinkeinonharjoittajina. Tällä on myös vaikutuksensa kuluttajan asemaa turvaavan sääntelyn soveltumisen kannalta. Kuluttajalla viitataan tyypillisesti luonnolliseen henkilöön, joka hankkii erilaisia kulutushyödykkeitä, kuten palveluita, pääasiassa muuta tarkoitusta kuin elinkeinotoimintaa varten. Ks. esim. KSL 1 luvun 5 §.

tapahtuu yksilöiden vapauden kautta, mikä samalla kasvattaa heidän vastuutaan omasta elämästään[16]. Ajattelutavan mukaan yksilöturvallisuuden tuottaja jakamistalouden alustoilla on ensisijaisesti yksilö itse. Hänen oletetaan oman etunsa nimissä minimoivan riskit digitaalisessa ympäristössä toimiessaan. Julkinen hallinto sen sijaan tarjoaa palveluita ja neuvoja muun muassa siitä, miten itsestään tulee huolehtia, mutta yksilö päättää, seuraako hän annettuja neuvoja. Mikäli yksilö päättää jättää neuvot huomiotta ja joutuu esimerkiksi huijauksen uhriksi, hänelle lankeaa vastuu päätöksensä seurauksista. Kyse on yksilön vastuuttamisesta kyberturvallisuuden ylläpitämisessä – riippumatta siitä, onko yksilöllä tietotaitoa itsestään ja toimintaympäristöstään huolehtimiseen.[17] Suomessa ei ole erityistä ”kyberlainsäädäntöä”, mutta yksilön vastuuttamisen peruste turvallisuuden tuottamisessa digitaalisessa toimintaympäristössä on luettavissa niin kansallisesta kuin Euroopan unionin kyberturvallisuusstrategiasta sekä julkisen hallinnon tuottaman kyberturvallisuuden sanaston määritelmistä.

Suomen kyberturvallisuusstrategia (SKTS) määrittelee kyberturvallisuuden[18] tavoitetilaksi, ”jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan”[19]. Kyberturvallisuuden sanasto täydentää määritelmää huomauttamalla, että

[16] Tutkimuskirjallisuus (neo)liberaalista hallinnasta on varsin laaja, mutta jakamistalouteen liittyen ks. esim. Cockayne 2016 ja Renaud ym. 2018.

[17] Renaud ym. 2018, s. 198–199, 201 ja 207. Ks. myös Quickley – Roy 2012, s. 86–88.

[18] Luvussa käytetään kyberturvallisuus-käsitettä, joka on vakiintumassa koko digitaalisen toimintaympäristön turvallisuuteen viittaavaksi käsitteeksi, eli kaikkien globaalisti yhteen liitettyjen tietojärjestelmien muodostaman kokonaisuuden ja tämän kokonaisuuden toimivuudesta riippuvaisten yhteiskuntien turvallisuuden käsitteellistykseksi. Yksilöturvallisuuden tarkasteleminen jakamistaloudessa liittyy koko tähän toimintaympäristöön, minkä vuoksi esimerkiksi tietoturvallisuuteen (tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistaminen) tai tietosuojaan (yksilön oikeus omiin henkilötietoihinsa) keskittyminen olisi rajannut käsittelyä liikaa. Lisäksi halutaan korostaa, etteivät yksilön toiminnan seuraukset digitaalisessa toimintaympäristössä rajoitu em. ympäristöön vaan niillä voi olla yhtä lailla fyysisiä vaikutuksia.

[19] SKTS 2013, s. 1.

> [k]yberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia. Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä. Tietoturvan lisäksi kyberturvallisuuteen pyritään muun muassa toimenpiteillä, joiden tarkoituksena on turvata häiriytyneestä kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot. Siinä missä tietoturvalla tarkoitetaan tiedon saatavuutta, eheyttä ja luottamuksellisuutta, kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin.[20]

Kybertoimintaympäristö on strategian mukaan ”sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö”[21]. Tietojärjestelmä taas viittaa ”ihmisistä, tietojenkäsittelylaitteista, tiedonsiirtolaitteista ja ohjelmista koostuvaa[n] järjestelmää[n], jonka tarkoituksena on informaatiota käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi”[22]. Kyberuhka ”tarkoittaa mahdollisuutta sellaiseen kybertoimintaympäristöön vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa jonkin kybertoimintaympäristöstä riippuvaisen toiminnon”[23]. Kyberuhkasta kyberturvallisuuden sanasto mainitsee lisäksi, että

> [k]yberuhkat voivat aiheutua paitsi toteutuneista tietoturvauhkista myös digitaalisessa viestintäympäristössä toteutettavista, yhteiskunnan turvallisuutta vaarantavista teoista. Kyberuhkat voivat kohdistua yhteiskunnan elintärkeitä toimintoja, kansallista kriittistä infrastruktuuria tai kansalaisia vastaan joko suoraan tai välillisesti. Ne voivat olla peräisin maan rajojen sisältä tai niiden ulkopuolelta.[24]

[20] Kyberturvallisuuden sanasto 2018, s. 22.
[21] SKTS 2013, s. 12.
[22] Emt., s. 13.
[23] Ibid.
[24] Kyberturvallisuuden sanasto 2018, s. 25.

Euroopan unionin kyberturvallisuusstrategia (EUKTS) tarkoittaa kyberturvallisuudella

> yleisesti varokeinoja ja toimenpiteitä, joilla voidaan suojata verkkoympäristöä sekä siviili- että sotilaspuolella uhkilta, jotka liittyvät tai voivat haitallisesti vaikuttaa sen muodostaviin keskinäisriippuvaisiin verkkoihin ja tietoinfrastruktuureihin. Kyberturvatoimilla pyritään säilyttämään verkkojen ja infrastruktuurin käytettävyys ja eheys sekä niiden sisältämien tietojen luottamuksellisuus.[25]

Kyberturvallisuus on siis yhtä aikaa tavoitetila ja niiden keinojen ja toimenpiteiden kokonaisuus, joilla tavoitetilaan pyritään. Tietoturvan lisäksi se kattaa kybertoimintaympäristöstä riippuvaisten fyysisten toimintojen turvaamisen. Kybertoimintaympäristö koostuu tietojärjestelmistä, joiden yksi osatekijä on ihminen. Kansalaisena ihminen on myös kyberuhkien kohde – yhteiskunnan elintärkeiden toimintojen, kriittisen infrastruktuurin ja organisaatioiden ohella. Ihminen on yhtä lailla kyberuhkien lähde yhteiskunnan turvallisuuden vaarantavien tekojen tekijänä kuin inhimillisyytensä vuoksi mahdollinen haavoittuvuus järjestelmässä.[26] Ihminen on myös kyberturvallisuuden tuottaja, sillä toimiessaan digitaalisessa toimintaympäristössä taitavasti ja oletetun laisesti hän vahvistaa kokonaisuuden turvallisuutta ja luotettavuutta. Inhimillisellä toiminnalla ja valituilla teknisillä ratkaisuilla on myös keskeinen rooli tietosuojan ylläpitämisessä.[27] Tässä artikkelissa ihmistä lähestytään yksilönä, jonka turvallisuus digitaalisessa toimintaympäristössä on pohtimisen arvoinen kysymys. Tuotetaanko yksilöiden vastuuttamisella kyberturvallisuutta?

Yksilöturvallisuudella tässä artikkelissa tarkoitetaan asioiden etenemistä yksilön odottamalla tavalla tai tavalla, jonka hän tiedossaan ole-

25 EUKTS 2013, s. 3, alaviite 4.

26 Salminen 2018.

27 Yksilölle kuuluva perusoikeus on, että hänen henkilötietojaan käsitellään erilaisissa rekistereissä tavalla, jossa yksityisyyden suoja säilyy. Lisäksi yksilöllä on mahdollisuus tarkistaa hänestä kerätyt tiedot ja vaatia tarpeen mukaan niiden oikaisemista tai poistamista. Tietosuojasta laajemmin ks. Korpisaari ym. 2018. Tietosuoja kuuluu perusoikeuksiin lukeutuvan yksityiselämän suojan piiriin. Suomen perustuslain (731/1999) 10 §:n mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Luonnollisten henkilöiden henkilötietojen suojasta säädetään tietosuojalaissa (1050/2018).

van pohjalta voisi olettaa tapahtuvaksi. Ennakoimisen mahdollisuus on yksi turvallisuuden osatekijöistä. Tällöin muun muassa digitaaliset alustat ovat käytettävissä silloin, kun niitä tarvitaan; alustoja ylläpitävät ne tahot, jotka ylläpitäjiksi on merkitty; alustoilta ei vuoda tietoja kolmansille osapuolille eikä yksilöistä myydä tai muuten välitetä tietoja eteenpäin ilman heidän nimenomaista suostumustaan; alustoilla annettavat tiedot ovat oikeellisia eikä niiltä tartu haittaohjelmia. Alustoilla ei huijata, kiusata, loukata tai kiristetä. Kukaan ei esiinny jonkun toisen nimissä tai käytä alustoja kenenkään maineen pilaamiseen. Alustojen käyttämiseen ei siten liity ikäviä yllätyksiä, vaan yksilö voi luottaa niiden toimintaan. Pyydettäessä alustojen ylläpitäjät kykenevät myös osoittamaan ne turvatoimet, joihin on tartuttu alustojen turvallisuuden vahvistamiseksi. Moneen edellä kuvattuun tekijään yksilön on hankala vaikuttaa.

Digitaalisen ja fyysisen nivoutuessa yhteen kyberturvallisuuteen myös kuuluu, ettei yksilöille aiheudu fyysistä haittaa digitaalisten alustojen käyttämisestä. Tämä tarkoittaa esimerkiksi, että alustoilla sovitusta pidetään kiinni, jolloin vaihtokaupan, ystäväpalveluksen tai oston ja myynnin yhteydessä sovittu tapahtuu odotetun laisesti. Sosiaalisen median ja muiden alustojen kohdennetuilla vihakampanjoilla ei pystytä aiheuttamaan työn, tulojen tai henkisen hyvinvoinnin menetystä kampanjan kohteelle[28]. Monen alustapalvelun toimintaan oleellisesti liittyviä arviointi- ja arvostelujärjestelmiä ei manipuloida.[29] Alustojen käyttäjille muodostuu tällöin kokemus ja tunne siitä, että niiden käyttäminen on turvallista. Kokemuksen myötä rakentuu vähitellen luottamus niin alustoja ja niillä toimivia muita tahoja kuin koko digitaalista toimintaympäristöä kohtaan. Luottamuksen rakentaminen vie aikaa (ja siihen vaikuttavat myös muiden käyttäjien kokemukset, joita usein jaetaan samoilla alustoilla tai nettikeskusteluissa), mutta sen tuhoaminen on nopeaa ja uudelleen rakentaminen vaikeaa.[30]

[28] Vrt. Keats Citron 2016.
[29] Vrt. esim. Ivanova – Scholtz 2017.
[30] Connolly 2013; myös esim. Schneier 2012a, 2012b, 2013a, ja 2013b.

Edellä kerrotun mukaisesti yksilöturvallisuus alustataloudessa koostuu objektiivisesta, ulkopuolisesti havainnoitavasta turvallisuudesta, mikä tavanomaisen turvallisuusajattelun mukaan tarkoittaa todettua uhkan poissaoloa[31]. Digitaalisten alustojen käyttäjiä ei tällöin uhkaa tietojen vuotaminen ulkopuolisille, identiteettivarkaudet taikka petokset, kiristysyritykset tai muut väärinkäytökset. Yhtä olennainen osa turvallisuutta on subjektiivinen, yksilön kokemukseen liittyvä turvallisuus.[32] Mikäli yksilö tuntee voivansa turvallisesti käyttää digitaalisia alustoja, hän toiminee alustoilla aktiivisemmin. Kokemukseen vaikuttavat muun muassa arviot omasta digitaalisen osaamisen tasosta, alustojen ja niillä toimivien toimijoiden luotettavuudesta sekä lainsäädäntö-, viranomais- ja tuomioistuinjärjestelmän toimivuudesta digitaalisten alustojen väärinkäytösten yhteydessä. Mikäli yksilö ei luota esimerkiksi siihen, että kyberrikoksia koskeva lainsäädäntö on ajan tasalla, poliisilla on riittävät resurssit tutkia digitaalisia väärinkäytöksiä, alustojen ylläpitäjät ovat huolehtineet alustojen teknisestä turvallisuudesta tai että alustan käyttäjät ovat hyväntahtoisia, hän pysytellee pois alustoilta. Ongelmalliseksi luottamuksen puute tulee esimerkiksi tilanteissa, joissa yksilön tarvitsema tai haluama palvelu on saatavilla vain digitaalisessa muodossa ja alustalla, jonka käyttöä hän ei koe turvalliseksi.[33]

Koska odotetusta poikkeavalla tavalla toimiminen voi tuottaa alustojen ylläpitäjille tai niitä käyttäville toimijoille etua tai hyötyä, ei ole poissuljettua, että alustojen avaamia mahdollisuuksia hyväksikäytettäisiin.[34] Päinvastoin, kiusaaminen, loukkaaminen ja maineen mustaaminen ovat verrattain yleisiä toimintatapoja esimerkiksi sosiaalisen median alustoilla.[35] Huijaukset, kiristys- ja haittaohjelmat sekä tieto-

31 Wolfers 1952 Bournen 2014, s. 1 ja 3 mukaan. Myös Dunn Cavelty 2007, s. 36.
32 Ibid.
33 Esimerkiksi vuoden 2018 aikana uutisoitiin ongelmista Omakanta-palvelun käytössä liittyen mm. palvelun käytettävyyteen, henkilötietojen urkintaan ja väärin diagnoositietoihin tietokannassa. Helsingin Sanomat 7.1.2018, Iltalehti 20.2.2018, Turun Sanomat 29.6.2018 ja Kuntalehti 20.12.2018. Omakanta-palvelu on ”kansalaisten verkkopalvelu, joka näyttää terveydenhuollon kirjaamia tietoja potilaasta ja hänen lääkityksestään” (www.kanta.fi/omakanta, viitattu 11.3.2019).
34 Esim. Schneier 2012a, 2012b, 2013a ja 2013b.
35 Ks. esim. Keats Citron 2016.

vuodot ovat viikoittaisia uutisaiheita. Pyydettyjen tietojen saaminen alustojen ylläpitäjiltä on epävarmaa ja saattaa kestää pitkiä aikoja. Samoin hyvityksen hakeminen oikeudellisin keinoin. Kyberrikosten havaitseminen, tutkiminen, todistaminen ja niistä tuomitseminen kehittyvät, mutta käytännöt ovat kansallisissa lainsäädännöissä kirjavia.[36] Digitaalisessa ympäristössä tapahtuvat rikokset ja muut väärinkäytökset muodostavat yksittäisten internetin käyttäjien näkökulmasta merkittävän kyberuhkan.[37] Mahdollisia kyberrikollisuuden muotoja, joita alustojen käyttäjät voivat kohdata, ovat muun muassa erilaiset petosrikokset (RL 36 luku), vainoaminen ja laiton uhkaus (RL 25:7a ja 25:7) sekä yksityisyyden, rauhan ja kunnian loukkaaminen (RL 24 luku).[38] Teknisten haavoittuvuuksien ohella alustataloutta tällä hetkellä kiusaavatkin psykologiset, organisatoriset (myös organisaatiokulttuuriin liittyvät) ja sääntelyyn liittyvät haavoittuvuudet, joiden seurauksiin kiinnitetään lisääntyvästi huomiota[39].

[36] Kyberrikollisuudella viitataan rikolliseen toimintaan, jonka tekoympäristönä on tietojärjestelmä ja/tai jossa hyödynnetään sähköisiä viestintäverkkoja ja tietojärjestelmiä. Ks. HE 153/2006 vp, s. 4, jossa tietotekniikkarikoksella tarkoitetaan rikosta, joka kohdistuu tietojärjestelmään sekä rikosta, joka tehdään tietojärjestelmän avulla. Digitaalista toimintaympäristöä hyödyntävän rikollisuuden nimeäminen ja/tai määritteleminen ei ole vakiintunutta. Esimerkiksi Riekkinen (2019, s. 159–166) käyttää tietoverkkorikollisuuden käsitettä käyden samalla laajempaa keskustelua eri käsitteellistyksistä.

[37] Kyberuhkien jaottelua voidaan tehdä eri näkökulmista. SKTS:n taustamuistiossa ne jaetaan viiteen ryhmään: kyberaktivismi, kyberrikollisuus, kybervakoilu, kyberterrorismi ja kyberoperaatiot. Jaottelu voi olla myös varsin tekninen, esimerkiksi Euroopan unionin verkko- ja tietoturvaviraston (ENISA) vuoden 2018 Threat Landscape Reportin mukainen: haittaohjelmat, webin selainpohjaiset hyökkäykset, web-sovellushyökkäykset, tietojenkalastelu, palvelunestohyökkäykset, roskaposti, bottiverkot, tietomurrot jne. Ihmisten arkipäivän kokemusten näkökulmasta kyberuhkia taas ovat mm. puutteellinen informaatioinfrastruktuuri, turvattomat tai epävarmat tuotteet ja palvelut, riittämättömät digitaaliset taidot sekä sanallinen tai kuvallinen hyväksikäyttö verkkoalustoilla. Jaottelunäkökulmaeroista ks. Salminen 2018.

[38] Muita rangaistavaksi säädettyjä kyberrikoksia ovat mm. RL 38 luvussa säädetyt tieto- ja viestintärikokset, joita ovat esimerkiksi tietojärjestelmän häirintä (RL 38:7a), tietomurto (RL 38:8) ja tietosuojarikos (RL 38:9).

[39] Ks. esim. Quigley – Roy 2012, Aiken 2016 ja Gcaza ym. 2016.

Luottamuksen vahvistamista ja turvallisuuden tuottamista digitaalisilla alustoilla vaikeuttaa alustatalouden globaali luonne. Internet, jonka toiminnan varassa alustatalous pyörii, on määritelmällisesti yhteen liitettyjen tietoverkkojen muodostama globaali tiedonsiirtoverkko.[40] Internetin eri osien toimintavarmuus siten riippuu kunkin verkon fyysisen infrastruktuurin kunnosta, teknisestä tasosta, luodusta arkkitehtuurista (mukaan lukien turvallisuustekijät), tiedonvälityksen saumakohdista ja mahdollisista tukkeutumista, tietoverkon käyttäjien osaamisesta ja toiminnan motivaatioista. Samoin toimintavarmuuteen vaikuttavat infrastruktuurin ympäristö kuten maantiede, yhteiskuntien (epä)vakaus, toimijoiden taloudellinen tilanne ja heidän arvojärjestelmänsä. Lähes kaiken kytkeytyminen yhteen siirtää luottamuksen ja turvallisuuden rakentamisen, ylläpitämisen ja uudelleen rakentamisen osittain kunkin toimijan oman vaikutuskyvyn ulkopuolelle. Samalla se tarkoittaa osittain pakotettua luottamista siihen, että muut kokonaisuuden osatekijät toimivat odotetun laisesti.[41] Luottamusta ja turvallisuutta on pyritty vahvistamaan ja vahvistetaan muun muassa teknologiastandardeista sopimalla, kansainvälisin sopimuksin ja hyvin käytäntein, tiedonvaihdolla, säädännön viitekehyksiä uudistamalla, sekä yhteistyöllä ongelmaratkaisussa, teknologian kehittämisessä ja turvallisuusloukkausten selvittämisessä[42]. Yksiselitteistä viitekehystä internetin hallinnalle ei kuitenkaan ole luotu – eri kysymys on, kuinka toivottava tämän kaltainen viitekehys olisi – mistä johtuen tilanne on monitulkintainen, osittain epäselvä ja yksilöturvallisuuden kannalta haastava.[43]

Yksilölle sälytetään edellä kuvatun mukaisesti vastuuta koko globaalin digitaalisen toimintaympäristön turvallisuuden tuottamisesta. Yhtäältä tämä tehdään syyllistämällä ihmistä tieto-taidottomuudesta tai huolimattomuudesta, kuvaamalla häntä kyberturvallisuuden heikoimmaksi lenkiksi. Toisaalta vastuuttaminen tapahtuu erilaisten ”self

[40] Lewis 2015, s. 111–113, Singer – Friedman 2014, s. 13–14 ja Mueller 2016, s. 4 ja 15.
[41] Ks. esim. Schneier 2012a, 2012b, 2013a, 2013b ja Limnéll ym. 2014, s. 48.
[42] Esim. Mueller 2016, s. 9. Luottamuksen institutionaalisesta vahvistamisesta ks. esim. Connolly 2013.
[43] Ks. van Eeten – Mueller 2013, Mueller 2016, s. 11–12 ja Hofmann ym. 2017.

help" -oppaiden tuottamisen kautta[44] tai esimerkiksi julkaisemalla "top 5" tai "top 10" -kyberuhkalistauksia niihin vastaamisen keinoineen yksilöille ja yhteisöille[45]. Esimerkiksi Tietoturvan vuosi 2018 -julkaisussa Kyberturvallisuuskeskus neuvoo, ettei yksilön tulisi antaa mobiililaitteiden sovelluksille tarpeettomia oikeuksia. Hänen tulisi myös tarkistaa, onko vastaanotettu sähköpostiviesti, tekstiviesti, yksityisviesti some-palvelussa tai puhelu aito, hankkia tietoturvaohjelmistot (ja pitää ne ajan tasalla) sekä tarkistaa luottokortille kertyneiden veloitusten tilanne aika ajoin. Koska tarpeeksi pitkien ja monimutkaisten salasanojen muistaminen on vaikeaa (varsinkin, kun joka palveluun tulisi olla oma salasanansa, joka pitäisi myös vaihtaa riittävän usein), ohjeistetaan ottamaan kaksivaiheinen tunnistautuminen käyttöön aina kun se on mahdollista.[46]

Yksilön vastuuttaminen ja "kybertaidot kansalaistaitoina" -ajattelu kulkevat käsi kädessä, mihin palataan artikkelissa myöhemmin. Yksilön vastuuttaminen kytkeytyy sekä fyysiseen että digitaaliseen ympäristöön, toisin sanoen vastuu voi aktualisoitua niin digitaalisessa kuin fyysisessä toimintaympäristössä tehtyjen tai tekemättömiksi jätettyjen tekojen myötä, kuten artikkelin seuraavissa osioissa tuodaan esiin. Seuraavassa tarkastellaan yksilön vastuuttamista oikeudettoman käytön sääntelyn ja yksilön toimintavelvollisuuksien näkökulmasta.

44 Esim. Rousku 2014, Kodin kyberturvaopas – ohjeita digitaaliseen arkeen 2017 ja Turvallisesti netissä -oppaat lapsille ja aikuisille 2019.

45 Esim. Kyberturvallisuuskeskus julkaisee "Tietoturvan vuosi" -julkaisua, jossa listataan viisi tärkeintä tietoturvauhkaa yksilöille kunkin vuoden ajalta. Monet ICT-alan tai konsulttiyritykset listaavat samoin kunkin vuoden loppuun tai alkuun vuoden merkittävimmät kyberturvallisuusuhkat tai -trendit. Lisäksi eri lehtien tai muiden julkaisujen www-sivulta löytyy aika ajoin mainitun kaltaisia listauksia.

46 Kyberturvallisuuskeskus 2019, s. 5.

3 Maksupalvelun käyttäjän vastuu ja toimintavelvoitteet turvallisuuden tuottamisessa

3.1 Maksupalvelun käyttäjän vastuun lähtökohdat ja huolellisuus fyysisessä ympäristössä

Maksupalvelulailla (290/2010, jäljempänä MPL), säädetään maksupalvelun käyttäjän ja maksupalveluntarjoajan välisestä sopimussuhteesta ja vastuunjaon periaatteista.[47] Laki koskee erilaisia varojen siirtoon liittyviä maksupalveluita, kuten maksutapahtuman toteuttamista maksukortilla tai muulla maksuvälineellä, tilisiirtona tai varojen siirtona palveluntarjoajan maksutilille.[48] MPL ei sovellu maksun kohteena olevan hyödykkeen toimittamiseen, eikä se koske maksun perusteena olevaan oikeussuhteeseen liittyviä oikeuksia ja velvollisuuksia. Maksuvälineitä ovat muun muassa pankki- ja luottokorttien lisäksi verkkopankkitunnukset sekä matkapuhelinliittymä silloin, kun sitä käytetään maksamiseen.[49] Lähtökohtana on, että maksutapahtuman toteuttaminen edellyttää maksajan suostumusta (MPL 38 §): maksutapahtumaa pidetään oikeudettomana, jos maksaja ei ole antanut suostumustaan sovitulla tavalla.[50] Mikäli maksupalveluntarjoaja toteuttaa maksutapahtuman ilman maksajan suostumusta, syntyy palveluntarjoajalle velvollisuus MPL 63 §:n nojalla palauttaa rahamäärä tai saattaa maksajan maksutili sellaiseen tilaan, jossa se oli ennen maksutapahtumaa.

---

47 MPL:lla pantiin täytäntöön Euroopan parlamentin ja neuvoston direktiivi 2015/2366/EU maksupalveluista sisämarkkinoilla (eli ns. Payment Services Directive, PSD2). PSD2:n edellyttämät muutokset tulevat voimaan vaiheittain.

48 Soveltamisalasta tarkemmin ks. MPL 1 §, jossa laissa tarkoitettuja maksupalveluita ovat rahanvälitys, maksutoimeksiantopalvelut, käteisnostot ja -panot, tilitietopalvelut, maksuvälineen liikkeellelasku, maksunsaajan kanssa tehtyyn sopimukseen perustuva maksutapahtuman hyväksyminen ja käsitteleminen, joka johtaa varojen siirtämiseen maksunsaajalle.

49 HE 169/2009 vp, s. 14 ja 17.

50 Ilmaisu ”sovitulla tavalla” viittaa suostumuksen antamismenettelyyn sekä sen muotoon. Suostumus voidaan ilmaista mm. allekirjoittamalla maksutosite, näppäilemällä tunnusluku, soittamalla tai lähettämällä tekstiviesti. Ks. HE 169/2009 vp, s. 58.

MPL:n 53 §:n 1 momentissa sekä tyypillisesti myös maksuvälineestä tehdyssä sopimuksessa määritellään käyttäjältä vaadittava huolellisuuden ja tiedostamisen taso, joka tässä kirjoituksessa nähdään konkretisoituvan erilaisina oikeussuhdetta ja toimintaympäristöä koskevina toimintavelvoitteina, kuten *huolellisuusvelvoitteina ja varotoimenpidevaatimuksina.* MPL:n säännöksen mukaan maksuvälineen haltijan on käytettävä maksuvälinettä sopimusehtojen mukaisesti sekä haltijan on erityisesti kohtuullisin toimenpitein huolehdittava maksuvälineestä ja siihen liittyvistä turvatunnuksista, kuten PIN-koodeista ja muista tunnusluvuista sekä salasanoista.[51] *Kuluttajan* asemassa olevan käyttäjän osalta sellaiset sopimusehdot ovat mitättömiä, joilla poiketaan MPL:n säännöksistä maksupalvelun käyttäjän vahingoksi (MPL 7 §).[52] Maksuvälineen haltijan velvollisuus huolehtia maksuvälineestä ja siihen liittyvistä turvatunnuksista alkaa hänen vastaanottaessaan ne.[53] Maksuvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä maksuvälineen haltijan on tehtävä viipymättä katoamisilmoitus (MPL 54 §).

MPL:n 62 §:n 1 momentin säännöksessä luetellaan edellytykset, joiden täyttyessä maksupalvelun käyttäjä joutuu itse vastaamaan oikeudettomasta käytöstä johtuvista vahingoista.[54] Lainkohdan 1 kohdan mukaan maksupalvelun käyttäjä tai maksuvälineen hal-

---

51 Henkilökohtaisilla turvatunnuksilla tarkoitetaan maksupalveludirektiivin 2015/2366/EU 4 artiklan 31 alakohdassa henkilökohtaisia toimintoja, jotka maksupalvelun tarjoaja antaa maksupalvelun käyttäjälle tunnistamistarkoituksiin. Tyypillisesti kysymys on vahvaan tunnistamiseen käytettävästä tunnistusvälineestä, johon käsitteen ei kuitenkaan ole tarkoitettu rajoittuvan. Ks. HE 132/2017 vp, s. 33. Vrt. HE 169/2009 vp, s. 68, jossa todetaan, etteivät pankkitilin numero tai luottokortin numero ole lain tarkoittamia turvatunnuksia.

52 Säännökset ovat ns. vähimmäispakottavia kuluttajan hyväksi. Esimerkiksi pienyrittäjien kohdalla voidaan sopia MPL:n sääntelystä poikkeavasti mm. pienyrittäjän asemassa olevan maksupalvelunkäyttäjän kohdalla. Kuluttajan käsite on määritelty KSL 1 luvun 4 §:ssä. Määrittelyä koskevasta problematiikasta ks. Peltonen – Määttä 2015.

53 Maksupalveludirektiivin 69 artiklan 2 kohdassa sanamuodossa maksupalvelunkäyttäjän maksuvälineen saatuaan on ”erityisesti toteutettava kaikki kohtuulliset toimenpiteet huolehtiakseen henkilökohtaisten turvatunnuksensa suojaamisesta”.

54 Tämän lisäksi maksuvälineen myöntäjän korttiehdoissa voi olla määräyksiä mm. löytöpalkkion tai poisottopalkkion veloittamisesta kortinhaltijalta. Ks. KVL 02/39/2152, jossa katsottiin, ettei pankilla ollut oikeutta periä 150 euron poisottopalkkiota. Ratkaisu on annettu ennen MPL:n säätämistä.

tija[55] vastaa kadonneen tai oikeudettomasti toisen haltuun joutuneen maksuvälineen käytöstä tai muusta maksuvälineen käytöstä vain, jos hän on *luovuttanut* sen tietoisesti ja vapaaehtoisesti käyttöön oikeudettomalle.[56] Toiseksi vastuu voi lainkohdan 2 kohdan perusteella syntyä silloin, kun kyse on huolimattomuudesta tapahtuneesta 53 §:n 1 momentissa säädetyistä tai maksuvälinettä koskevassa sopimuksessa määritellyistä velvollisuuksien laiminlyönnistä. Kolmanneksi vastuu voi 3 kohdan mukaan syntyä, mikäli maksupalvelun käyttäjä tai muu maksuvälineen haltija laiminlyö 54 §:ssä säädetyn velvollisuuden tehdä *ilman aiheetonta viivytystä katoamisilmoitus* palveluntarjoajalle tai sen muulle nimeämälle taholle.[57]

3.1.1 Kuinka toimintavelvollisuuksien laiminlyönti ilmenee fyysisessä ympäristössä?

Käytännössä ratkaistaessa maksuvälineen käyttäjän ja esimerkiksi pankin välistä vastuunjakoa oikeudettomasta käytöstä kysymys on maksupalvelun käyttäjän menettelyn huolimattomuuden ja huolellisuuden arvioinnista.[58] Huolimattomuudessa on kysymys maksupalvelua koskevan sopimuksen sisältämien tai MPL:n 53 §:n 1 momentissa säädettyjen huolellisuusvelvollisuuksien rikkomisesta tai kohtuullisiin varotoimiin ryhtymättä jättämisestä, mitkä lisäävät oikeudettoman käytön riskiä ja vaaraa. Käyttäjän huolimattomuus voi ilmetä:

1) kortin tai muun maksuvälineen säilyttämisvelvollisuuden laiminlyöntinä
2) tunnusluvun tai muun turvatunnuksen säilyttämisen ja huolellisen käytön laiminlyöntinä

---

55 Lainkohta koskee sekä sitä maksupalvelun käyttäjää, joka on tehnyt maksuvälinettä koskevan sopimuksen, että maksuvälineen muuta haltijaa.

56 Ks. HE 169/2009 vp, s. 74–75. Tietoisen luovutuksen katsotaan ilmentävän tietoista riskinottoa.

57 Säännöksen taustalla oleva ajatus riskinjaosta perustuu siihen, että yleensä ainoastaan kortinhaltija voi havaita kortin katoamisen Vrt. KKO 2006:81, joka koski aikaisemmin voimassa ollutta KSL 7 luvun 19 §:n arviointia. Ks. KRIL 651/39/09, jossa aiheettomaksi viivästykseksi on katsottu se, että kortinhaltija ei kahteen tuntiin saanut katoamisilmoitusta tehtyä puhelimen akkuvirran loputtua.

58 Hildén – Sainio 2017, s. 4. Huomionarvoista on, että se maksupalvelun käyttäjä, joka on tehnyt maksuvälinettä koskevan sopimuksen, vastaa myös maksuvälineen haltijan huolimattomuudesta, ks. HE 169/2009 vp, s. 74.

3) kortin tai muun maksuvälineen tallella olon varmistamiseksi edellytettävän tarkistamisvelvollisuuden ja ilman aiheetonta viivästystä tehtävän katoamisilmoituksen laiminlyöntinä.

Maksuvälineen huolellinen säilyttäminen on haltijan perusvelvollisuus, johon kuuluu, että haltija ryhtyy kaikkiin kohtuullisiin toimenpiteisiin säilyttääkseen kortin turvallisesti. Kun arvioidaan, millaisia varotoimia voidaan kohtuudella vaatia, tulee huomio kiinnittää siihen, että maksuvälineet on tavanomaisesti tarkoitettu käytettäväksi päivittäisessä maksamisessa ja niitä on voitava kuljettaa mukana. Maksuvälineitä on säilytettävä kuitenkin vähintään yhtä huolellisesti kuin käteistä rahaa.[59] Kuluttajariitalautakunnan ja pankkilautakunnan ratkaisukäytännöstä löytyy linjauksia huolellisen säilyttämisen vaatimuksen täyttävistä toimintatavoista.[60]

Maksuvälineen haltijan kohtuullisiin varotoimiin kuuluu myös se, että maksuvälinettä ja siihen liittyvää tunnuslukua säilytetään erillään siten, ettei sivullinen voi yhdistää niitä toisiinsa. Tämänkään osalta ei voida edellyttää kohtuuttoman pitkälle meneviä turvallisuusjärjestelyjä.[61] Lisäksi pankkien yleiset korttiehdot tyypillisesti edellyttävät, että tunnusluvun näppäilyn yhteydessä näppäimistö suojataan siten, ettei sivullisella ole mahdollisuutta nähdä tunnuslukua.[62] Myös *pankkilautakunta* on ratkaisukäytännössään katsonut, että turvalliseen ja huolelliseen tunnuslukujen käyttämiseen kuuluu se, että maksuvälineen haltija ryhtyy kaikkiin kohtuullisiksi katsottaviin varotoi-

59 HE 169/2009 vp, s. 68–69.

60 Ratkaisussa KRIL 1948/39/11 katsottiin, että kortin säilyttäminen ulkomailla tapahtuneen ravintoillan aikana käsilaukun sisäpuolisessa, vetoketjullisessa taskussa on tavanomaista ja huolellista menettelyä, jota päivittäisessä maksamisessa käytettäväksi tarkoitetun kortin haltijalta voidaan edellyttää. Ks. myös PKL 9/12 ja PKL 17/12, joissa korttia säilytettiin laukussa. Tavanomaista ja lähtökohtaisesti huolellista menettelyä on myös maksuvälineen säilyttäminen takin povitaskussa (PKL 56/11).

61 Huolellista menettelyä on mm. kortin säilyttäminen lompakossa ja tunnusluvun säilyttäminen kotona lipaston laatikossa, ks. HE 169/2009 vp, s. 68. Ratkaisussa PKL 10/13 asiakkaan katsottiin huolimattomuudesta laiminlyöneen tunnusluvun huolellisen säilyttämisen erillään maksukorteista. Asiakas oli säilyttänyt Tallinnan risteilyllä korttejaan käsilaukussa ja korttien tunnusluvut sisältänyttä muistilappua kesäpuseronsa taskussa.

62 Hildén – Sainio 2017, s. 7.

miin, joilla estetään ulkopuolista saamasta tunnuslukua haltuunsa.[63] Kuitenkaan esimerkiksi se, että kortin tunnusluku on onnistuttu urkkimaan ruuhkaisella baaritiskillä, ei vielä indikoi, että kortinhaltija olisi toiminut huolimattomasti,[64] vaan maksutapahtumaa ympäröivät olosuhteet ratkaisevat, millaista huolellisuuden tasoa kortinhaltijalta voidaan edellyttää.

Kortinhaltijan huolellisuusvelvoitteen piiriin on katsottu kortin tallella olon seuraaminen olosuhteiden vaatimaa huolellisuutta noudattaen.[65] Tämä tarkistamisvelvollisuus määräytyy kulloisessakin tilanteessa vallitsevien olosuhteiden perusteella, riippuen muun muassa katoamis- ja anastusriskeistä, jolloin tarkistamisvelvollisuus voi olla korostunut.[66] Lisäksi merkitystä on tavalla, jolla maksuvälineen haltija on kyseisissä olosuhteissa korttiaan säilyttänyt sekä se, onko tapahtumainkulussa sattunut jotain poikkeavaa, jolloin tallella olo tulisi erityisesti tarkistaa. Tallella olon seuraamisen on katsottu kuuluvan olennaisesti huolellisen kortinhaltijan velvollisuuksiin, sillä tarkistamisvelvollisuus on kytköksissä MPL 54 §:n velvollisuuteen tehdä katoamisilmoitus viipymättä.[67] Suuressa ihmisjoukossa, metroasemalla[68] tai

63 Tilanteissa, joissa näköetäisyydellä on paljon ihmisiä, kuten vähittäiskaupan kassalla tai junalippuautomaalilla asioidessa, kohtuullisena vaatimuksena voidaan pitää näppäimistön suojaamista kädellä tai lompakolla. Näin mm. PKL 31/10, PKL 29/12 ja PKL 57/12.

64 Näin esim. KRIL 1948/39/11.

65 HE 169/2009 vp, s. 68. Kortinhaltijan tarkistamisvelvollisuus on yhteydessä kortinhaltijan kolmanteen vastuuperusteeseen, velvollisuuteen viipymättä ilmoittaa kortin katoamisesta tai oikeudettomasta käytöstä.

66 Näin esim. KKO 2006:81, jossa katsottiin, että tarkistamisvelvollisuus sisältyy silloisen kortinhaltijan vastuuta koskevaan KSL 7 luvun 19 §:n 1 momentin säännökseen, jonka 3 momentissa edellytettiin kortinhaltijan ilmoittavan viipymättä kortin katoamisesta. Säännös vastaa sisällöltään MPL 54 §:n ilmoitusvelvollisuutta.

67 Hildén – Sainio 2017, s. 14. Ks. myös PKL 51/12, jossa asiakkaan katsottiin huolimattomuudesta laiminlyöneen tarkistamisvelvollisuuden sekä korttiehtojen ja MPL 54 §:n ilmoitusvelvollisuuden, kun hän ei ollut tarkistanut kortin tallellaoloa heti ravintolasta kotiin tultuaan.

68 Ratkaisussa KRIL 3723/39/08 kortinhaltijan katsottiin laiminlyöneen tarkistamisvelvollisuuden. Korttia oli ehditty käyttää oikeudettomasti 14 tuntia ennen kuin luottokorttiyhtiö oli saanut ilmoituksen kortin katoamisesta. Kortinhaltija ei huolimattomuudestaan huolimatta ollut vastuussa oikeudettomasta käytöstä, sillä luottokorttiyhtiö ei antanut riittävää selvitystä siitä, että myyjäliikkeet olisivat silloin voimassa olleen KSL 7 luvun 19 §:n 2 momentin edellyttämällä tavalla varmistuneet huolellisesti korttia käyttäneen oikeudesta käyttää korttia.

ruuhkaisella baaritiskillä olosuhteet ovat sellaiset, että kortinhaltijan tulisi tarkistaa säännöllisesti kortin tallella olo, viimeistään kotiin saavuttaessa.[69] Tällöin havaittuaan maksuvälineen katoamisen, tai joutumisen oikeudettomasti toisen haltuun tai oikeudettoman käytön, haltijan tulee ilman aiheetonta viivytystä tehdä katoamisilmoitus.[70]

Maksupalvelun käyttäjän vastuu on euromääräisesti rajoitettu 50 euroon (MPL 62 §:n 2 mom.) tavallisen huolimattomuuden ja ilmoitusvelvollisuuden laiminlyöntitilanteissa. Lisäksi käyttäjän 62 §:n 2 momentin vastuuta on rajoitettu MPL 62 §:n 3 momentin edellytyksin. Maksukortin haltijan vastuu oikeudettomasta käytöstä katkeaa kortin sulkuilmoitukseen eli kun palveluntarjoajalle tai sen nimeämälle muulle taholle ilmoitetaan maksuvälineen katoamisesta, joutumisesta toisen haltuun tai oikeudettomasta käytöstä.[71] Käyttäjä ei vastaa lainkaan oikeudettomasta käytöstä, jos palveluntarjoaja ei ole huolehtinut siitä, että maksuvälineen haltijalla on milloin tahansa mahdollisuus tehdä katoamisilmoitus, maksunsaaja ei ole maksuvälinettä käyttäessä asianmukaisesti varmistunut maksajan oikeudesta käyttää maksuvälinettä tai palveluntarjoaja ei ole edellyttänyt vahvaa tunnistamista.

3.1.2 Törkeän huolimattomasti tai tahallisesti toimiva käyttäjä kantaa täyden vastuun

Tahallisissa tai törkeän huolimattomuuden tilanteissa haltija vastaa MPL 62 §:n 2 momentin nojalla oikeudettomasta käytöstä johtuvista vahingoista myös 50 euron ylittävältä osalta.[72] *Törkeällä huolimattomuudella* viitataan erittäin vakavaan varomattomuuteen, joka selvästi osoittaa haltijan suhtautuvan piittaamattomasti maksuvälineen hallintaan ja käyttöön liittyviin turvallisuusriskeihin. Maksuvälineen haltijan törkeää huolimattomuutta ovat lain esitöiden mukaan esimerkiksi

69 Ks. KRIL 1948/39/11, jossa kortinhaltija teki katoamisilmoituksen klo 11.02 vasta herättyään ja huomattuaan kortin kadonneen. Oikeudettomia ostoja oli tehty klo 2.41–11.00 välisenä aikana. Ks. myös PKL 51/12.

70 Se, onko ilmoitus tehty ilman aiheetonta viivytystä, arvioidaan tapauskohtaisesti, HE 169/2009 vp, s. 69. Ks. myös PKL 20/12.

71 Ks. KRIL 2403/39/10.

72 Vrt. PSD2-direktiivin 74 artikla. Maksuvälineen haltijan petollinen toiminta tai vähintään yhden 69 artiklassa säädetyn maksajan velvollisuuksien tahallinen tai törkeän huolimaton laiminlyönti johtaa siihen, että maksaja vastaa kaikista menetyksistä.

se, että haltija on säilyttänyt maksukorttia ja siihen liittyvää tunnuslukua samassa lompakossa, tai turvatunnuksien säilyttäminen muutoin maksuvälineen rinnalla avoimessa ja muille helposti havaittavassa muodossa.[73]

Myös viivyttely MPL 54 §:n tarkoittaman katoamisilmoituksen tekemisessä tai ilmoituksen tietoisella laiminlyönnillä voi yksittäistapauksessa osoittaa tahallisuutta tai törkeää huolimattomuutta.[74] Huolimattomuuden asteen arvioinnissa merkitystä on riskin todennäköisyydellä sekä sillä, onko käyttäjä menettelyllään lisännyt oikeudettoman käytön riskiä, joka olisi ollut kohtuullisin toimin torjuttavissa. Samalla huomiota on kiinnitetty siihen, onko käyttäjä tiedostanut tai olisiko käyttäjän tullut tiedostaa riskit. Rajanvetoa tavallisen ja törkeän huolimattomuuden välillä on käyty korkeimman oikeuden ratkaisussa KKO 2018:71 (ään. 3–2):

> A:n MasterCard Gold -yhdistelmäkortti ja siihen liittyvä tunnusluku oli anastettu A:n asianajotoimistosta työpöydältä, ja kortilla oli tehty käteisnostoja yhteensä 4 960 euroa. A oli säilyttänyt maksukorttiaan työpöydälleen jääneessä lompakossaan ja tunnuslukua pankilta tulleessa kirjeessä työpöydän laatikossa. Korkein oikeus katsoi, että A säilytti tunnuslukua alkuperäisessä pankin kirjekuoressa vastoin nimenomaista sopimusehtoa, mikä on lisännyt riskiä siitä, että ulkopuolinen voi löytää ja yhdistää tunnusluvun tiettyyn maksukorttiin. Yksistään pankin kirjeen säilyttäminen ei vielä merkinnyt huolimattomuutta. Oikeudettoman käytön riskiä oli olennaisesti lisännyt se, että A oli jättänyt toimis-

[73] HE 169/2009 vp, s. 75. Direktiivin johdanto-osion 72 kohdassa törkeä huolimattomuus määritellään käyttäytymiseksi, johon kuuluu merkittävä määrä piittaamattomuutta. Kuluttajariitalautakunta katsoi ratkaisussa KRIL 2403/39/10, että maksukortin oikeudeton käyttö oli seurausta kuluttajan törkeästä huolimattomuudesta tapahtuneesta maksupalvelulain 53 §:n 1 momentin velvoitteiden laiminlyönnistä. Tapauksessa K:n lompakko katosi Tallinnaan menevällä laivalla, ja K:n yhdistelmäkorttia käytettiin oikeudettomasti tunnuslukua käyttäen. Koska K ei esittänyt tunnusluvun säilyttämisestä mitään selvitystä, K:n katsottiin säilyttäneen korttia tunnusluvun kanssa samassa lompakossa.

[74] Pankkilautakunnan ratkaisussa PKL 20/12 Indonesiassa taskuvarkauden kohteeksi joutunut huomasi korttinsa kadonneen klo 15. Oikeudettomia ostoja oli tehty klo 04.46–17.54 välillä. Asiakas oli sulkenut korttinsa vasta klo 19.08. Lautakunta totesi, että asiakkaan olisi tullut ymmärtää riski korttinsa oikeudettomasta käytöstä ja huolellinen toiminta olisi edellyttänyt pankille viipymättä ja ilman aiheetonta viivästystä tehtävää ilmoitusta. Asiakas vastasi täysimääräisesti klo 15 jälkeen tapahtuneista nostoista.

> ton lukitsematta ja lompakon työpöydälle. Korkein oikeus totesi, että kodin tai työpaikan lukitsematta jättämisen merkitystä arvioitaessa tulee huomioida kodin tai työpaikan sijainti sekä siihen liittyvä vaara anastuksesta. A:n työhuone oli sijainnut toisessa kerroksessa, sisätiloihin ei ollut näköyhteyttä ulkoa, eikä kysymys ollut avoimesta julkisesta tilasta, kuten uimarannasta tai ravintolasta. Lompakon anastaminen ja kortin oikeudeton käyttö oli korkeimman oikeuden mielestä ollut sattumanvaraista. Lopuksi korkein oikeus totesi, että asianajaja A:n on jo ammattinsa puolesta tullut tiedostaa riskit. Koska A:n *huolimattomuus on ollut kertaluontoista, aiheutunut vaara on ollut lyhytaikainen eikä kovin todennäköinen* (kurs. tässä), korkein oikeus ei pitänyt A:n menettelyä törkeän huolimattomana.[75]

Samankaltaiseen arviointiin päädyttiin ratkaisussa KRIL 5651/39/2015, jossa työpaikkaa ei pidetty tilana, jossa käyttäjällä olisi korostunut velvollisuus varovaisuuteen. Huolimattomuutta ei pidetty törkeänä, koska ensinnäkään kysymys ei ollut rautatieasemaan tai anniskeluravintolaan rinnastettavasta julkisesta tilasta, joissa kortinhaltijalta edellytetään suurempaa huolellisuutta. Toiseksi pankin korttiehdoissa ei mainittu korttitietoihin liittyvistä riskeistä.

3.1.3 Kuluttajan ja luotonantajan vastuunjako luottokortin oikeudettomasta käytöstä

MPL:n sääntelyyn liittyy läheisesti kuluttajansuojalain (38/1978, jäljempänä KSL) 7 luvun 40 §:n säännös luotonantajan ja kuluttajan välisestä riskin- ja vastuunjaon periaatteista silloin, kun luottokorttia tai muuta luoton käyttämiseen oikeuttavaa tunnistetta käytetään oikeudettomasti. Säännös koskee sekä jatkuvia luottoja että kertaluottoja. Asiallisesti säännös vastaa niin vastuun perusteiltaan, euromääräiseltä ulottuvuudeltaan kuin myös vastuun rajoituksiltaan MPL 62 §:n säännöstä,[76] joten sen tulkinnassa ja toimintavelvoitteiden sisällön muo-

[75] Eri mieltä olleet oikeusneuvokset katsoivat, että A:n menettelyä olisi pidettävä törkeän huolimattomana siksi, että A oli osoittanut piittaamatonta suhtautumista maksuvälineen hallintaan ja käyttöön liittyviin turvallisuusriskeihin ja ohjeisiin, sillä A oli säilyttänyt tunnuslukua sopimusehtojen ja lain säännösten vastaisesti ja tietoisesti korottanut merkittävästi sen vaaraa, että ulkopuolinen voi yhdistää tunnusluvun korttiin. Tunnuslukua oli pitkään säilytetty työpaikalla, jota ei voida pitää yksityisenä tilana. Tällöin A:lla oli ollut korostunut huolellisuusvelvollisuus kortin ja tunnusluvun erillään säilyttämisen osalta.

dostamisessa voidaan tukeutua edellä esitettyyn MPL:n järjestelmään ja sitä koskevaan oikeuskäytäntöön.[77] Aikaisemmin luotonantajan ja kuluttajan vastuunjakoa koski KSL 7 luvun 19 §, jonka mukaan kuluttaja oli vastuussa vain *lievää suuremmasta* huolimattomuudesta johtuvista laiminlyönneistä, mutta sääntely yhdenmukaistettiin MPL:n säännöksen kanssa. Tältä osin MPL:n mukaisen vastuujärjestelmän voidaan katsoa olevan maksaja-kuluttajan kannalta ankarampi.[78]

KSL 7 luvun 1 §:n 4 momentin mukaan luoton käyttöön oikeuttavaan tunnisteeseen rinnastetaan myös tunniste, joka oikeuttaa tilin tai muun rahoituspalvelun tai rahoitusvälineen käyttöön.[79] Lisäksi 40 §:n säännöstä sovelletaan elinkeinonharjoittajaan, joka on tehnyt kuluttajan kanssa tunnistetta koskevan sopimuksen.

> Mielenkiintoinen kysymys onkin, mitä vastuunjakoa koskeva säännös merkitsee esimerkiksi alustavälitteisten vertaisluottojen kohdalla silloin, kun joku oikeudettomasti palveluun kirjautumalla ottaa käyttäjän nimissä luottoja.[80] Nimittäin 40 §:n sanamuoto edellyttää, että kuluttaja on tehnyt luottosopimuksen luotonantajan kanssa: ”Kuluttaja, joka on tehnyt luottosopimuksen luotonantajan kanssa, vastaa kadonneen tai oikeudettomasti toisen haltuun joutuneen [– –]”. Sanamuodon perusteella kuluttajan vastuu esimerkiksi tilanteessa, jossa tunnisteen oikeudeton käyttö on johtunut kuluttajan huolimattomuudesta edellyttää, että kuluttaja on tehnyt luotosta sopimuksen, eli vastuu alkaisi vasta luottosopimuksen tekemisen jälkeen. Tavallisesti vertaisluottoalustoilla luottosopimuksen katsotaan olevan luotonottajan ja toisen alustaa käyt-

76 Ks. HE 169/2009 vp, s. 93 ja HE 132/2017 vp, s. 57. Säännöstä ei sovelleta MPL:n soveltamisalaan kuuluviin luottosopimuksiin (KSL 7 luvun 4 §:n 1 mom.).

77 Näin esim. Peltonen – Määttä 2015, s. 533.

78 Ks. HE 169/2009 vp, s. 18, jossa todetaan, että MPL:n vastuujärjestelmällä pyrittiin yhdenmukaistamaan ja yksinkertaistamaan vastuukysymysten arviointia. Hallituksen esityksessä todetaan myös, että vastuun ei kuitenkaan arvioida muodostuvan kohtuuttoman ankaraksi, sillä vastuun euromääräinen yläraja törkeää lievemmissä huolimattomuustilanteissa rajoittaa maksupalvelun käyttäjän vastuuta.

79 Ks. HE 132/2017 vp, s. 57, jossa todetaan, että vaikka kertaluottoja ei käytetä luottokortilla tai muilla tunnisteilla, myös nämä luotot on syytä saada sääntelyn piiriin.

80 Vertaisluotoilla tarkoitetaan yksityishenkilöiden toisilleen myöntämiä luottoja, jotka tehdään alustan välityksellä. Vertaisluottojen käsitteestä, ks. Päläs 2017.

tävän sijoittaja-luotonantajan välinen[81], eikä kysymys ole näin alustan ja luotonottajan välisestä velkakirjasta. Palveluun kirjautuminen ei siten merkitse vielä luottosopimuksen syntymistä, vaan alustalla rahoitusta tarjoavat ja sitä tarvitsevat kohtaavat päättävät erillisessä prosessissa luottosopimuksen syntymisestä. Oikeudettomasti tunnistetta käyttäen tehty luottosopimus ei ole kuluttajan tekemä: tulisiko 40 §:n säännöstä tulkita siten, ettei kuluttaja ole tällöin vastuussa, vaikka tunnusten joutuminen johtuisi hänen huolimattomasta menettelystä?

3.2 Millainen on maksuvälineen käyttäjän vastuu digitaalisessa ympäristössä?

Edellä maksuvälineen käyttäjän huolimattomuus ja riskiä lisäävä menettely ovat ilmenneet *fyysisessä toimintaympäristössä* tapahtuvina toimintavelvollisuuksien laiminlyönteinä, joiden seurauksena oikeudeton käyttö on ollut mahdollista. Jakamistalouden alustoilla toimivien yksityishenkilöiden osalta olennaista on se, millä tavoilla maksupalvelun käyttäjän toimintavelvollisuudet, huolellisuusvelvoitteet ja kohtuulliset varotoimenpiteet konkretisoituvat päätelaitteita ja tietoverkkoja käytettäessä. Millaisia turvallisuutta edistäviä toimia käyttäjältä edellytetään silloin, kun kyse on maksuvälineen käytöstä verkkoalustoilla? Alkujaan vain fyysisesti esitettävät maksu- ja luottokortit[82] ovat yhä enemmän saaneet jalansijaa verkko-ostosten sekä muiden verkkopohjaisten maksutapahtumien välineenä. Fyysisen maksukortin digitaalista käyttöä voi olla esimerkiksi korttitietojen yhdistäminen alustan tarjoamaan sovellukseen tai asiakkuustilille, jolloin alustan välityksellä hankittujen tilauksien ja ostojen maksaminen veloitetaan suoraan maksukortilta.[83] Maksukorttien rinnalle on kehittynyt myös muita digitaalisia maksutapoja, kuten mobiilimaksaminen ja e-lompakot.

81 Ks. esim. Fellow Finance Oy:n käyttöehdot sekä Fixura Ab Oy:n yleiset ehdot.

82 Maksukortteja ovat mm. Visa Electron -kortit, aiemmat pankkikortit korvanneet debit-kortit, luottokortit sekä debit- ja credit-ominaisuudet sisältävät yhdistelmäkortit. Ks. Wuolijoki – Hemmo 2013, s. 631 ss.

83 Maksukorttia voi käyttää mm. Wolt-, Airbnb- ja Uber-palveluissa.

Maksuvälineiden, niitä koskevien tietojen ja verkkopankkitunnusten kalastelu (*phishing*)[84] sekä erilaiset huijaukset ovat keskeisimpiä yksityishenkilöiden kohtaamia kyberuhkia.[85] Tilausansahuijauksissa käyttäjää houkutellaan antamaan korttinsa tai muun maksuvälineiden tiedot luomalla hänelle mielikuva siitä, että hän on voittanut hienon tuotteen tai hänelle tarjotaan tuotteita ehdoilla, jotka ovat liian hyviä ollakseen totta. Tietojen kalastelua tapahtuu muun muassa sähköpostiviestillä lähetettävillä linkeillä, jotka ohjaavat käyttäjän maksupalveluntarjoajan verkkosivustoja muistuttavalle sivuille, joissa asiakasnumeroita, tunnuksia, salasanoja ja vahvistuskoodeja pyydetään antamaan esimerkiksi tilien sulkemisen tai muiden paikkaansa pitämättömien seurausten välttämiseksi. Kalasteltuja tietoja käytetään esimerkiksi oikeudettomien tilisiirtojen tekemiseen, tunnistautumiseen ja luottojen nostamiseen uhrien nimissä.[86]

Erityisesti tilausansojen kohdalla yksi tyyppiongelma liittyy siihen, onko maksupalvelunkäyttäjä antanut MPL 38 §:n edellyttämällä tavalla *maksusumman veloittajalle suostumuksensa maksutapahtuman* toteuttamiseen vai onko maksuvälinettä käytetty oikeudettomasti. Todistustaakkaa koskevan MPL 72 §:n 1 momentin mukaan maksupalvelun tarjoajan on osoitettava, että suostumus on annettu sovitulla tavalla. Tämä ei kuitenkaan yksin riitä vapauttamaan palveluntarjoajaa vastuusta, vaan palveluntarjoajan tulee tarvittaessa esittää muutakin näyttöä siitä, että haltija on antanut suostumuksensa maksu-

84 Tietojen kalastelulla viitataan toimintaan, jossa aidolta vaikuttavalla sähköpostilla, pikaviestillä tai huijaussivustolla pyritään huijaamaan ihmisiä paljastamaan luottamuksellisia tietoja. Kalastelussa voi olla kysymys myös sosiaalisesta manipuloinnista, jossa pyritään hyödyntämään ihmisten luontaisia ominaisuuksia luottamuksen rakentamiseksi, ks. Peltomäki – Norppa 2015, s. 171.

85 Tästä konkreettisena esimerkkinä voidaan mainita erityisesti vuonna 2018 laajamittaisesti eri organisaatioissa levinneet Office 365 -sähköpostihuijaukset, joissa kalasteltiin käyttäjätietoja Ks. kyberturvallisuuskeskus 2019, s. 3–7 ja 9. Muut vuoden 2018 listauksen uhkat ovat: huijaukset, huonosti suojatut laitteet, valesovellukset virallisissa sovelluskaupoissa sekä verkkopalveluiden tietovuodot. Tietojen kalastelulla voidaan pyrkiä toimintaan, joka täyttää RL 38:9a:ssä kriminalisoituun identiteettivarkauteen, ks. Soininen 2017, s. 86–87.

86 Lisäksi tietojen kalastelun ensikontakti voi tapahtua myös puhelinsoiton tai tekstiviestin muodossa, Hildén – Savikko 2017, s. 37.

tapahtumalle (MPL 72 §:n 3 mom.).[87] Kuten edellä ilmeni, suostumuksen tulee olla tietoinen, mikä edellyttää, että asiakkaan näytetään hyväksyneen tai saaneen tietoonsa palvelua koskevat sopimuksen ehdot:

> Ratkaisussa FINE-000699 asiakas oli verkko-ostosten yhteydessä hyväksynyt 1,15 euron veloitukset Visa Electron -kortilla, mutta hän kiisti hyväksyneensä neljän eri maksunsaajan 376,03 euron veloitukset. Pankki ei ollut MPL 72 §:n edellyttämällä tavalla osoittanut asiakkaan hyväksyneen tai saaneen tietoonsa eikä myöskään sitoutuneen korttitiedoilla tehtyihin riidanalaisille veloituksille. Asiakkaan toiminnassa ei ollut kysymys MPL 62 §:n 1 momentin 1 kohdassa tarkoitetusta maksuvälineen luovuttamisesta oikeudettomalle, kun asiakas oli luovuttanut korttitietonsa hyväksymiensä veloitusten tekemiseen. Kortin oikeudeton käyttö ei johtunut myöskään asiakkaan huolimattomuudesta, sillä lautakunta katsoi, että maksunsaaja oli käyttänyt korttitietoja sopimuksen vastaisesti oikeudettomiin veloituksiin.
>
> Pankkilautakunnan ratkaisussa PKL 24/16 A oli maksanut verkossa yhdistelmäkortillaan yhden euron televisiosta, koska oli luullut asioivansa Suomessa toimivan kodinelektroniikkaa myyvän ketjun kanssa. Yhden euron lisäksi A:lta veloitettiin 79 euroa. A katsoi tulleensa huijatuksi. Lautakunta katsoi, etteivät maksunsaajalla olleet oikeat kortti- ja yhteistiedot vielä yksistään osoita, että A olisi antanut suostumuksensa veloituksiin. Pankki ei osoittanut A:n saaneen lainkaan palvelua tai palveluntarjoajaa koskevia tietoja, joten lautakunta katsoi, ettei A ollut antanut suostumustansa, jolloin kyse on MPL 38 §:n tarkoittamasta oikeudettomasta käytöstä. A:n vastuu oli ratkaistava 62 §:n perusteella.[88]

---

87 Lainkohdan mukaan pelkästään se, että ”palveluntarjoaja voi näyttää, että suostumus maksutapahtuman toteuttamiseen on annettu maksuvälineellä, ei välttämättä yksin riitä osoittamaan, että maksuvälineen haltija on antanut suostumuksensa maksutapahtuman toteuttamiseen, toiminut petollisesti taikka laiminlyönyt tahallisesti tai törkeän huolimattomasti 53 ja 54 §:ssä säädettyjä velvollisuuksiaan”.

88 Ratkaisussa PKL 56/16 pankin katsottiin pankin näyttäneen, että asiakas itse oli tehnyt riidattomat ostot, eikä kyse ollut kortin oikeudettomasta käytöstä. Pankin mukaan asiakas oli itse tilannut deittisivustoilta palveluita hyväksyen maksut kortillaan. Palveluissa oli annettu kortin tiedot, kirjautuminen oli tehty asiakkaan sähköpostiosoitteella, toisessa palvelussa oli käytetty asiakkaan syntymävuotta ja toisessa sukunimeen viittaavaa käyttäjätunnusta. Lisäksi asiakkaan reklamaation jälkeen asiakkaan tililtä oli tehty uusi veloitus, jossa maksunsaajana oli sama yritys. Ks. myös FINE-000699, jossa asiakkaan tililtä oli tehty Visa Electron -kortin tiedoilla toistuvaisveloituksia.

Mikäli maksutapahtuma katsotaan oikeudettomaksi, aktualisoituu kysymys siitä, onko *haltija luovuttanut maksuvälineen käyttöön oikeudettomalle* 62 §:n 1 momentin 1 kohdan tarkoittamalla tavalla, mikä synnyttäisi haltijalle täysimääräisen vastuun. Kuten aikaisemmin on mainittu, luovuttamisen tulee tapahtua tietoisesti ja vapaaehtoisesti.[89] Toiseksi kyse on siitä, onko käyttäjä *huolimattomuudesta* laiminlyönyt MPL:n 53 §:n 1 momentin ja 54 §:n sekä sopimusehtojen velvoitteita. Maksupalvelun käyttäjältä voidaan edellyttää selvitystä tapahtumista, joissa maksuväline ja turvatunnukset ovat joutuneet sivullisen haltuun, kun maksuvälineen haltija kiistää hyväksyneensä maksutapahtuman ja vetoaa oikeudettomaan käyttöön.[90] Vastaavanlaista selvitystä edellytetään silloin, kun arvioidaan onko haltija noudattanut lain 53 §:n 1 momentin velvoitetta.[91] Toisaalta maksupalveludirektiivi PSD2:n johdanto-osion kappaleessa 72 todetaan, että varsinkin silloin, kun maksuvälinettä ei käytetä fyysisessä myyntipaikassa, vaan kysymys on esimerkiksi verkkomaksuista, maksupalveluntarjoajaa olisi aiheellista vaatia esittämään näyttö maksupalvelun käyttäjän huolimattomuudesta, sillä käyttäjän mahdollisuudet esittää näyttöä ovat tällaisessa tilanteessa rajatut.

> Koska A oli pankkilautakunnan ratkaisussa PKL 24/16 mieltänyt asioineensa kodinelektroniikkaa myyvän ketjun kanssa, lautakunta ei pitänyt korttitietojen luovuttamista tietoisena ja vapaaehtoisena, jotta kysymys olisi ollut MPL 62 §:n 1 momentin 1 kohdassa tarkoitetusta luovuttamisesta. Kun pankki ei myöskään osoittanut A:n toimineen huolimattomasti korttitietoja antaessaan, A ei lautakunnan mukaan ollut huolimattomuudesta laiminlyönyt korttiehtojen mukaisia velvoitteitaankaan. Lautakunta suositti A:lle syntyneen vahingon täysimääräistä hyvittämistä.

---

89 Ks. FINE-013245, jossa luovuttamisena ei pidetty verkkopankkitunnusten kertomista valepoliisille.

90 Ks. PKL 51/11 ja PKL 13/11, joissa katsottiin, että asiakas oli itse hyväksynyt maksutapahtumat, eikä selvitys osoittanut, että maksutapahtumissa olisi ollut kysymys kortin oikeudettomasta käytöstä.

91 Ks. mm. KRIL 2403/39/10, jossa kortinhaltija kiisti säilyttäneensä maksukorttia yhdessä tunnusluvun kanssa. Koska korttia oli käytetty nimenomaisesti tunnusluvun kanssa, eikä haltija antanut asiassa selvitystä, kuluttajariitalautakunta katsoi, ettei korttia ja tunnuslukua ollut säilytetty huolellisesti toisista erillään.

Ratkaisu PKL 24/16 antaa aihetta pohtia käyttäjän asemaa myös some- tai muilla verkkoalustoilla leviävien huijausten osalta:

> Viime aikoina käyttäjien kaapatuilta Facebook-tileiltä tai Facebookissa toimivan huijaussovelluksen välityksellä on levinnyt tilapäivityksiä, joissa kerrottiin – tosin huonolla suomen kielellä – mahdollisuudesta voittaa 500 euron lahjakortti vähittäiskauppa Prismaan. Viestissä kehotettiin googlaamaan merkkiyhdistelmä ”PRIS500WRT”, ja ensimmäinen hakutulos ohjasi Prisma-500.com-verkkosivulle, joka oli laadittu näyttämään Prisman virallisilta verkkosivuilta. Saadakseen lahjakortin käyttäjän oli tullut vastata kysymyksiin, antaa yhteystiedot ja luottokorttitiedot. Kysymyksessä oli kuitenkin Pointworld-yhtiön maksullinen jäsenyys, josta veloitettiin kuukausittainen tilausmaksu.[92] MPL 62 §:n 1 momentin 1 kohta ja pankkilautakunnan ratkaisukäytäntö huomioon ottaen Facebook-käyttäjä ei näyttäisi olevan vastuussa yllä olevassa tilanteessa, ellei hän ole antanut tietoista ja vapaaehtoista suostumusta maksutapahtumalle.[93] Eri asia on, tulisiko Facebook-käyttäjän yleisen tietämyksen ja päivityksen tökerön ulkoasun perusteella ymmärtää kyseenalaistaa, että kysymys on huijauksesta ja näin olla tietoinen vaarasta.

Myös kalastelutapausten osalta tyypillisesti kysymys siitä, onko maksuvälineen käyttäjä luovuttanut verkkopankkitunnuksensa käyttöön oikeudettomalle vai onko verkkopankkitunnusten siirtyminen oikeudettomasti toisen haltuun johtunut käyttäjän MPL:n 53 §:n 1 momentin ja sopimusehtojen velvollisuuksien huolimattomasta laiminlyönnistä.

> Ratkaisussa PKL 27/14 asiakkaan verkkopankkitunnuksia kalasteltiin tekstiviestillä, jossa kerrottiin asiakkaalla olevan avoin lasku ja uhattiin maksuhäiriömerkinnän tekemisellä heti seuraavana päivänä. Viestissä kehotettiin menemään maksumerkinta.net-sivulle tarkistamaan laskun tiedot, joka vaati verkkopankkitunnusten käyttämistä. Asiakas oli tämän jälkeen yrittänyt kirjautua verkkopankkiinsa, mutta pääsy palveluun oli estetty. Asiakkaan tilitä oli siirretty oikeudetta 3 800 euroa.

[92] Lisäksi on epäilty, että sivuilla vierailu saattoi asentaa haittaohjelman tietokoneelle. Ks. Ilta-Sanomat 9.2.2018.

[93] Vastuu voi todistustaakkaa koskevan sääntelyn valossa syntyä, mikäli maksupalvelun tarjoaja kykenee osoittamaan käyttäjän hyväksyneen tai olleen tietoinen palvelun ehdoista.

Pankkilautakunta katsoi, ettei asiakas ollut luovuttanut verkkopankkitunnuksiaan tietoisesti, sillä asiakas oli ollut siinä käsityksessä, että hän oli asioinut pankin kanssa. Kysymys ei ollut MPL 62 §:n 1 momentin 1 kohdan tarkoittamasta maksuvälineen luovuttamisesta.

Arvioidessaan, merkitsikö asiakkaan menettely MPL 62 §:n 2 momentin 2 kohdan huolimattomuudesta johtuvaa MPL:n 53 §:n ja verkkopankkitunnusten käyttöä koskevan sopimusehtojen velvoitteiden laiminlyöntiä, pankkilautakunta katsoi, että asiakkaan oli perusteltua ajatella jonkin maksamattoman laskun siirtyneen perintätoimiston perittäväksi. Lisäksi asiakkaan ei voitu olettaa tietävän, keiden tahojen kanssa pankilla oli sopimukset verkkopankkitunnusten käytöstä. Lautakunta piti poikkeuksellisena ainoastaan perintätoimistona esiintyneen ensiyhteydenottoa tekstiviestillä, mihin asiakkaan olisi tullut kiinnittää huomiota ja ymmärtää kyseenalaistaa yhteydenoton ja verkkosivujen asianmukaisuuden. Toisaalta pankki ei esittänyt, ettei vastaavaa yhteydenottotapaa voisi olla perintätoimistojen käytössä eikä pankki myöskään ollut turvallisuutta koskevissaan ohjeissaan antanut minkäänlaista varoitusta tai mainintaa tällaisista yhteydenotoista. Lautakunta suositti, että pankki vastaa vahingosta täysimääräisesti.

Niissä verkkopankkitunnusten kalastelutapauksissa, joissa tunnukset ovat päätyneet ulkopuolisen tietoon, ratkaisevaa on se, kuinka huolellisesti asiakkaan voidaan katsoa menetelleen tunnustensa suhteen. Asiakkaan huolellisuuden arviointi edellyttää kuitenkin selvitystä olosuhteista, kuten tunnusten säilyttämis- ja käyttötavasta, ja siitä, miten tunnukset ovat päätyneet ulkopuolisen haltuun.

Ratkaisussa FINE-006255 pankkilautakunta katsoi verkkopankkitunnusten oikeudettoman käytön johtuneen siitä, että asiakas oli laiminlyönyt MPL 53 §:n, 54 §:n ja pankkitunnusehtojen mukaisia velvollisuuksiaan säilyttämiseen, tallellaolon seuraamiseen ja sulkuilmoituksen tekemisen suhteen, ja piti asiakkaan menettelyä törkeän huolimattomana. Kirjautumiset asiakkaan tilille olivat tapahtuneet espanjalaisista IP-osoitteista, ja tililtä oli siirretty varoja yhteensä 13 400 euroa. Asiakas oli konttorikäynnillään maininnut saaneensa sähköpostiviestejä ja avanneensa niissä olleita linkkejä. Asiakas perusti valituksensa pankin järjestelmän tietoturva-aukkoon, mutta väitetystä haavoittuvuudesta ei ollut muuta selvitystä kuin asiakkaan epäilys. Lautakunta piti uskottavana, että tunnusluvun päätyminen ulkopuoliselle oli asiakkaan toiminnan seurausta.

Pankkilautakunta on käytännössään katsonut, että myös kalastelutapauksissa asiakkaalla on parhaat mahdollisuudet selvityksen antamiseen sen osalta, miten verkkopankkitunnukset ovat päätyneet niitä oikeudetta käyttäneen haltuun. Asiakkaan vaatiessa pankkia ottamaan vastuun voidaan asiakkaan aina edellyttää antavan selvityksen omasta menettelystään. Tapauksissa, joissa on jäänyt epäselväksi, kuinka tunnukset ovat siirtyneet ulkopuolisen haltuun ja joissa lautakunta ei voi luotettavasti arvioida tapahtumankulkua ja käyttäjän toimintaa, lautakunta on jättänyt ratkaisusuosituksen antamatta.[94]

Ratkaisussa PKL 27/14 pankkilautakunta kiinnitti vahvasti huomiota siihen, millaiseksi asiakas mielsi tapauksen kokonaistilanteen ja syntyikö asiakkaalle perusteltua aihetta olettaa, että yhteydenotossa oli todella kysymys asiallisesti toimivasta perintätoimistosta. Verkossa toimivan käyttäjän osalta olennaista onkin se, miten kussakin yksittäistapauksessa määritetään se vaadittava tietämyksen, ymmärtämisen ja osaamisen taso, jota huolellisesti toimivalta käyttäjältä edellytetään. Pankkilautakunnan ratkaisussa PKL 35/16 katsottiin, että asiakkaan olisi tullut *yleisen tietämyksen* ja hänelle lähetetyn *sähköpostin muotoilun* ja *sisällön* perusteella ymmärtää, ettei sähköposti ollut pankin lähettämä:

> Tapauksessa PKL 35/16 A oli saanut pankin ”turvallisuusosastolta” sähköpostin, jonka avattuaan B pankin turvallisuusjohtajaksi esittäytynyt pyysi päivitystä varten muutamia tunnuslukuja. Tämän seurauksena A:n tililtä oli ehditty oikeudettomasti siirtää 4 600 euroa. Lautakunta katsoi, että A:n olisi tullut ymmärtää sähköpostin muotoilun ja sisällön perusteella, ettei viesti ollut pankin lähettämä, ja hänen olisi tullut ymmärtää kyseenalaistaa yhteydenottojen asiallisuus. Lisäksi pankin verkkopalveluehdoissa nimenomaisesti kiellettiin kirjautuminen verkkopalveluun sähköpostilinkin kautta sekä tunnusten kertominen puhelimitse. Pankki oli myös vuoden 2016 keväällä tiedottanut verkkourkinnan vaarasta. Huolellisesti toimiessaan A:n olisi tullut jättää linkki avaamatta ja erityisesti jättää tunnusten antaminen. Mikäli A olisi kyseenalaista-

[94] Ks. FINE-013434 ja FINE-014299, joissa riidanalaiseksi jäi, kuinka ulkopuolinen on saanut tunnukset haltuunsa.

> nut yhteydenottojen asiallisuuden ja ottanut yhteyttä pankkiinsa, vahingoilta olisi voinut ainakin osittain välittyä. Lautakunta katsoi A:n menettelyn kokonaisuutena selvästi ja olennaisesti poikkeavan siitä, mitä huolelliselta verkkopankkitunnusten haltijalta vaaditaan. A:n huolimattomuus katsottiin törkeäksi.

Juuri turvallisuusriskien tiedostaminen sekä siitä huolimatta tapahtuva toimintavelvollisuuden laiminlyönti tai riskeistä piittaamaton varomattomuus olivat ratkaisujen KKO 2018:71 ja KRIL 5651/39/2015 huolimattomuuden astetta koskevan arvioinnin keskiössä: ratkaisuissa annettiin merkitystä sille, tiedostiko tai olisiko maksuvälineenhaltijan tullut tiedostaa olosuhteisiin liittyvät turvallisuusriskit.[95] Vastaavasti riskien tiedostaminen ja pyrkimys turvallisuusriskien pienentämiseen on ratkaisussa PKL 10/13 vaikuttanut vastuuarvioon lieventävänä tekijänä.[96] Maksupalvelun tarjoajien sopimusehtojen, turvaohjeiden ja tiedotteiden sisältämät maininnat turvallisuusriskeistä näyttävätkin myös pankkilautakunnan ratkaisuissa vaikuttavan olennaisesti siihen, mitä käyttäjä kussakin yksittäistapauksessa on voinut perustellusti olettaa tietoverkoissa toimiessaan.[97] Erityiset turvallisuutta koskevat ehdot näyttäisivät tekevän riskeistä tiedostettuja. Tiedostettujen riskien edellyttämien varotoimenpiteiden laiminlyönnin tai myötävaikuttamisen riskien toteutumi-

---

95 Kuluttajariitalautakunnan ratkaisun perusteella voidaankin kysyä, olisiko turvallisuusriskien sisällyttäminen pankin korttiehtoihin muuttanut ratkaisun lopputulosta, jolloin kortinhaltijan olisi katsottu menetelleen törkeän huolimattomasti. Ks. myös PKL 20/12, jossa asiakkaan olisi tullut ymmärtää riski korttinsa käytöstä sinä aikana, kun ilman aihetta viivytteli katoamisilmoituksen tekemisessä. Viivyttelyn osalta asiakkaan katsottiin menetelleen törkeän huolimattomasti, jolloin hän vastasi täysimääräisesti viivyttelyn aikana tehdyistä nostoista.

96 Ratkaisussa PKL 10/13 asiakkaan menettelyn katsottiin osoittavan *vakavaa varomattomuutta*, kun hän oli säilyttänyt kesäpuseronsa taskussa muistilappua, johon hän oli kirjannut korttiensa tunnusluvut helposti tunnistettavaan muotoon. Kokonaisuutena arvioituna asiakkaan ei katsottu laiminlyöneen velvoitteitaan törkeästä huolimattomuudesta, sillä hänen katsottiin tiedostaneen taskuvarkausriski ja pyrkineen pienentämään tätä riskiä.

97 Näin myös FINE-013245.

seen on katsottu ilmentävän sellaista piittaamattomuutta ja varomattomuutta, jotta huolimattomuuden on katsottu olevan törkeää:

> Ratkaisussa FINE-003435 asiakkaalle oli soitettu, ja pankin edustajaksi esittäytynyt oli pankin päivitystä varten pyytänyt verkkopankin tunnuslukuja. Asiakkaan tililtä oli verkkomaksuilla siirretty noin 2 500 euroa. Pankki oli tunnuslukukirjeen saatekirjeessä korostanut tunnusten henkilökohtaisuutta sekä todennut, ettei se koskaan tiedustele sähköpostilla tai puhelimella tunnuksia. Lisäksi pankki oli usein eri tavoin varoittanut kalastelusta. Lautakunta katsoi, että asiakkaan olisi tullut yleisen tietämyksen ja pankin antamien varoitusten perusteella ymmärtää, ettei ollut tosiasiassa asioinut pankin kanssa. Kokonaisuutena arvioiden asiakkaan menettely oli selvästi ja olennaisesti poikennut siitä, mitä huolelliselta verkkopankkitunnusten haltijalta edellytetään. Asiakas oli törkeästä huolimattomuudesta laiminlyönyt MPL 53 §:n 1 momentin velvoitteita ja verkkopalvelutunnusten yleisiä ehtoja.

Käyttäjän vastuun kannalta merkityksellistä on, lisääkö turvallisuusriskeistä mainitseminen sopimusehdoissa tai tiedotteissa käyttäjältä vaadittavia varotoimenpiteitä. Lain esitöiden valossa tämä näyttäisi olevan mahdollista.[98] Toiseksi olennaista on, nostaako riskien kuvaaminen käyttäjältä vaadittavaa huolellisuuden tasoa siten, että huolellisuusvelvoitteen katsotaan olevan aina korostunut. Tyypillisesti käyttäjän vastuun sisällöstä määrätään yksipuolisissa vakiosopimuksissa, eikä käyttäjä tosiasiallisesti ole vaikuttanut ehtojen laadintaan. Ongelma on se, että on hyvin tavallista – etenkin digitaalisessa muodossa verkossa olevien hyödykkeiden kohdalla – ettei käyttäjä ole tutustunut ehtojen sisältöön, ja sopimusehdot lähinnä vain nopeasti klikkaamalla kuitataan hyväksytyksi. Tällöin on mahdollista, että käyttäjä sopimuksen hyväksyessään tulee sidotuksi sellaisiin varotoimiin ja turvallisuusriskien välttämiseen, joista hän ei tosiasiallisesti ole tietoinen.[99] Tässä kohtaa on huomioitava, että MPL edellyttää ai-

98 Ks. HE 169/2009 vp, s. 68–69, jossa todetaan, että sopimukseen voidaan laatia tarkempia ehtoja siitä, millaisiin varotoimiin maksuvälineen haltijan on ryhdyttävä pitääkseen maksuvälineensä tallessa.

99 Tällaisessa tilanteessa käyttäjän vastuuta voi rajoittaa se, jos varotoimia ja turvallisuusriskien hallintaa koskevat ehdot katsotaan käyttäjän kannalta yllättäviksi ja ankariksi. Vakiosopimusehtojen sitovuutta ja liityntää sekä yllättäviä ja ankaria ehtoja koskevasta problematiikasta, ks. Wilhelmsson 2008, s. 66 ss.

noastaan kohtuullisiksi katsottavia varotoimenpiteitä kuluttaja-käyttäjältä (MPL 53 §:n 1 mom.). Toinen asia on, minkä tasoista ymmärtämistä, tietämystä ja teknistä osaamista kuluttajilta voidaan kohtuudella vaatia ja otetaanko arviossa huomioon käyttäjän subjektiiviset käsitykset ja odotukset asioiden kulusta sekä tietotaito verkon vaaroista esimerkiksi ikäihmisten kohdalla. Digitaaliset riskitekijät ovat kuitenkin paljon haastavampia havaita ja hallita kuin riskit fyysisissä kanssakäymisen muodoissa.

Säilyttämisvelvollisuudet, turvatunnusten suojaamisvelvoitteet ja *tarkistamisvelvollisuudet* ovat relevantteja myös digitaalisessa ympäristössä. Digitalisaation ja maksupalveluiden edetessä nämä toimintavelvoitteet voivat saada ihan eri muodon.[100] Edellä selostetuissa tapauksissa velvollisuuksien laiminlyönti on ilmennyt linkin klikkauksina, tunnusten puhelimitse kertomisena ja tietojen syöttämisenä sivustoille. Huomionarvioista on, että pankkilautakunnan ratkaisusuosituksissa merkitystä on annettu tietoverkoissa toimivan käyttäjän tietotaidolle: huolimattomuuden arviointi on perustunut siihen, ettei käyttäjän menettely ole yltänyt vaadittavalle tietämyksen ja ymmärtämisen tasolle tai on ollut tiedostetuiksi katsotuista turvallisuusriskeistä piittaamatonta.

4 Viestintäpalvelun käyttäjän vastuu oikeudettoman käytön tilanteissa

Edellä esitetty MPL:n oikeudetonta käyttöä koskeva vastuujärjestelmä koskee myös puhelinliittymällä toteutettavia maksuja, jotka veloitetaan teleyrityksen (mm. Telia, DNA ja Elisa) puhelinliittymää koske-

[100] Esimerkiksi ratkaisun KKO 2018:71 perustelukohdassa 27 korkein oikeus on linjannut, että myös maksukorttiin liittyvää tunnuslukua on voitava säilyttää kirjallisena paikassa, josta se on verrattain helposti saatavissa. Erilaisten tunnuslukujen ja muiden tunnisteiden yleistymisen vuoksi korkein oikeus katsoo, ettei voida edellyttää tunnisteiden säilyttämistä vain muistin varassa. Ratkaisun johdosta herääkin kysymys, missä eri tilanteissa esimerkiksi tunnuslukujen säilyttäminen käyttöjärjestelmän työpöydällä tai käyttäjätunnusten ja salasanojen hallintaa helpottavien sovellusten tai pilvipalveluiden käyttäminen voisi merkitä huolellisen säilyttämisen laiminlyöntiä?

van laskun yhteydessä. MPL:n säännökset eivät kuitenkaan MPL 3 §:n 1 momentin 6 kohdan mukaan sovellu teleyrityksen viestintäpalvelun käyttöön perustuvan laskutuksen yhteydessä käyttäjiltä perimiin maksutapahtumiin, joissa teleyritys toimii maksunvälittäjänä.[101] Näitä ovat enintään 50 euron määräiset maksutapahtumat, joiden yhteenlaskettu, käyttäjäkohtainen määrä on enintään 300 euroa kuukaudessa silloin, kun on kysymys digitaalisen sisällön tai ääniperusteisten palvelujen ostamisesta.[102] MPL:n soveltamisalan ulkopuolella olevien maksutapahtumien osalta teleyrityksen ja viestintäpalvelun käyttäjän eli tilaajan välisestä vastuun- ja riskienjaosta oikeudettoman käytön tilanteissa syntyneistä vahingoista on säädetty laissa sähköisen viestinnän palveluista (917/2014, jäljempänä SVPL) 125 §:ssä. Oikeudetonta käyttöä voi olla myös muu kuin viestintäpalvelussa käytettävän laitteen fyysinen hallinta.[103] Käytännössä kuluttajalla voi olla vaikeuksia esittää näyttöä oikeudettomasta käytöstä viestintäpalveluiden monimutkaisesta luonteesta johtuen. Lain esitöissä todetaankin, ettei riski saa jäädä kuluttajille kannettavaksi sen vuoksi, että näytön hankkiminen on mahdotonta.[104]

SVPL:ssa kuluttaja-tilaajan huolellisuusvelvoitteiden sisällöstä ei ole erikseen laissa säädetty. Kuluttajariitalautakunta on linjannut, että puhelinliittymän oikeudeton käyttö rinnastuu väärinkäytön riskeil-

---

101 Toiseksi MPL ei sovellu yllä mainitut euromääräiset vaatimukset täyttäviin sähköisestä laitteesta tai sen välityksellä toteutettaviin maksutapahtumiin, joissa on kysymys hyväntekeväisyystoiminnasta tai matka-, pysäköinti- tai pääsylippujen taikka muiden sen kaltaisen lippujen ostamisesta. Ks. HE 132/2017 vp, s. 58.

102 HE 132/2017 vp, s. 27. Digitaalista sisältöä ovat digitaalisessa muodossa olevat hyödykkeet, joiden käyttö on rajoitettu tekniseen laitteeseen. Komission direktiiviehdotuksessa digitaalisen sisällön toimittamista koskevista sopimuksista digitaalisen sisällön käsite on tarkoitettu laajaksi ja se kattaa niin ladattavat kuin suoratoistona lähetettävät elokuvat, pilvipalvelut ja sosiaalisen median sovellukset. Ehdotuksen mukaan direktiiviä sovellettaisiin myös sellaiseen digitaaliseen sisältöön, jonka vastikkeena kuluttaja luovuttaa dataa. Ks. COM(2015) 634 final, s. 12.

103 Sääntely on tarkoitettu teknologianeutraaliksi, joten SVPL:n säännös soveltuu myös muiden viestintäpalveluiden kuin kännykkäliittymän oikeudettoman käytön tilanteisiin. Ks. HE 231/2005 vp, s. 15 ja 31. Viestintäpalvelun oikeudettomasta käytöstä seuraavia vahinkoja ovat mm. puheluista tai palveluista johtuvat maksut, joita tilaaja ei ole itse soittanut tai tilannut. HE 231/2005 vp, s. 31. Omat erityiskysymyksensä liittyvät alaikäisen mm. pelisovellusten sisällä tehtyihin ostoihin. Näitä kysymyksiä ei tässä kirjoituksessa kuitenkaan tarkastella.

104 HE 231/2005 vp, s. 32.

tään ja suojautumismahdollisuuksiltaan pankki- ja luottokortin käyttöön, jolloin arvioinnissa on tukeuduttu luottokortin oikeudetonta käyttöä koskevaan, aiemmin voimassa olleeseen KSL 7 luvun 19 §:ään ja sitä koskevaan ratkaisukäytäntöön.[105] Tällöin liittymähaltijan velvoitteiksi on katsottu liittymän ja tunnisteiden huolellinen säilyttäminen[106] sekä tallellaolon tarkistaminen olosuhteiden vaatimalla tavalla, katoamis- ja anastusriskit huomioiden.[107] Lain esitöissä kuluttajan huolellisuusvelvoitteeseen on katsottu kuuluvan lisäksi *laitteiden riittävästä tietoturvasta huolehtiminen.*[108]

Lainkohdan 2 momentin mukaan tilaaja on vastuussa, jos laitteen katoaminen, joutuminen oikeudettomasti toisen haltuun tai oikeudeton käyttö on seurausta *lievää suuremmasta* huolimattomuudesta: tilaaja ei ole lainkaan vastuussa lievästä huolimattomuudesta. Huolimattomuuden astetta arvioidaan tapauskohtaisesti kaikki seikat huomioon ottaen. Puhelinliittymän luovuttaminen ulkopuoliselle on katsottu vastuun synnyttäväksi huolimattomuudeksi vastaavalla tavalla kuin MPL:n 62 §:n 1 momentin 1 kohdassa.[109] Lain esitöiden mukaan kuluttaja-tilaajan huolellisuutta arvioitaessa painoarvoa on sillä, mitä kuluttajan olisi pitänyt tietää ja tehdä. Lisäksi arviointiin vaikuttaa se, mitä normaalihuolelliselta ihmiseltä voidaan vastaavanlaisissa olosuhteissa edellyttää. Kuluttajan tietämys- ja toimintatason

[105] SVPL:n 125 §:n säännös muistuttaakin aikaisemmin voimassa ollutta KSL 7 luvun 19 §:n vastuuperusteita. Lain esitöissä on katsottu, että matkapuhelinliittymän ja luottokortin oikeudettoman käytön tilanteet ovat sääntelykohteena osittain samanlaiset ja eräissä suhteissa puhelinliittymä muistuttaa läheisesti luottokorttia. On huomattava, että KSL:n sääntely muutettiin vastaamaan MPL:n vastuusäännöstä, ks. HE 132/2017 vp, s. 57.

[106] Kuluttajariitalautakunta on katsonut, että matkapuhelinliittymää tulee voida säilyttää yhtä huolellisesti kuin luotto- ja pankkikorttia. Ks. KRIL 3923/38/07.

[107] Ks. KRIL 2563/39/2012, jossa kuluttaja ei tiennyt missä tai kenen hallussa liittymän SIM-kortti oli ollut, miten ulkopuolinen on voinut saada PIN-koodin tai onko PIN-koodin kysely ollut käytössä. Kuluttaja ei ollut seurannut liittymän SIM-kortin tallellaoloa, jolloin oikeudeton käyttö oli seurausta lievää suuremmasta huolimattomuudesta. Toisaalta ratkaisussa katsottiin, ettei teleyrityksen oma menettely mahdollistanut tarkistamisvelvollisuuden täyttämistä, jolloin teleyritys oli osittain vastuussa oikeudettomasta käytöstä.

[108] HE 231/2005 vp, s. 32.

[109] Ks. HE 231/2005 vp, s. 31–32. Säännös vastaa sisällöltään aiemmin voimassa olleen viestintämarkkinalain, VML:n 79a §:ä, jolloin SVPL 125 §:n tulkinnassa voidaan nojautua VML:n esitöihin.

määrittelyssä tulisi ottaa huomioon myös muun muassa teleyrityksen oma tiedotus ja muut toimet.[110] Tällöin teleyrityksen sopimusehdot ja tiedottaminen ovat olennaisessa asemassa vaadittavan huolellisuuden ja tietämyksen tason arvioinnissa.

> Esimerkiksi Telian yleisten käyttöehtojen kohdassa 4.2 todetaan, että ”asiakkaan tulee noudattaa liittymän säilyttämisessä, suojaamisessa ja käytössä korostettua huolellisuutta”, koska liittymää ja palveluita voidaan käyttää digitaalisen sisällön ja tavaroiden ostamiseen. Asiakkaan tulee huolehtia liittymän älykorttien ja laitteiden suojaamisesta tunnisteilla (PIN-koodi, suojakoodi, käyttäjätunnus, salasana), ja tunnisteita on säilytettävä erillään älykorteista ja laitteista siten, etteivät ne joudu ulkopuolisen haltuun tai tietoon. Lisäksi laitteiden ja älykortin oletusarvioiset tunnisteet tulee vaihtaa. Asiakkaan tulee myös huolehtia palvelun käytön, laitteiden ja ohjelmistojen riittävästä tietoturvasta ja suojaustoimenpiteistä, kuten virustorjunta- ja palomuuriohjelmistojen hankinnasta, käyttöjärjestelmien ja ohjelmistojen päivittämisestä ja muista vastaavista tarpeellisista toimista sekä muun muassa saldo- ja muiden rajoituspalvelujen hankinnasta. Ehdoissa todetaan erikseen, että asiakas käyttää palvelua omalla vastuullaan.

Ajallisesti tilaajan vastuuta on rajoitettu MPL:a vastaavalla tavalla: tilaaja ei ole vastuussa viestintäpalvelun oikeudettomasta käytöstä siltä osin, kun tilaaja on tehnyt teleyritykselle ilmoituksen laitteen katoamisesta, sen joutumisesta oikeudettomasti toisen haltuun tai sitä on oikeudettomasti käytetty, ja pyytää viestintäpalvelun sulkemista tai sen käytön estämistä (SVPL 125 §:n 1 ja 3 mom.). Vastuun synnyttävää lievää suurempaa huolimattomuutta voi olla kohtuullisessa ajassa tehtävän ilmoitusvelvollisuuden laiminlyönti.[111]

Liittymän haltija-käyttäjän vastuuttamisen näkökulmasta SVPL:n ja MPL:n vastuujärjestelmät ovat monimutkaiset. Puhelinliittymällä oikeudettoman käytön uhreiksi joutuneet käyttäjät ovat eri asemassa riippuen siitä, katsotaanko liittymän oikeudettomasta käytöstä olevan kysymys maksutapahtumasta (esim. pelisovellusostot) vai viestintäpalvelun velvoituksesta (puhelut, SMS-viestit, datapaketit). Toiseksi käyttäjät ovat eri asemassa riippuen siitä, onko liittymällä hankittu

[110] HE 231/2005 vp, s. 32.

[111] Vastuu on tältä osin yhteydessä siihen, että laiminlyönti poistaa mahdollisuuden vahingon rajoittamiseen. HE 231/2005 vp, s. 32.

digitaalisia ja ääniperusteisia tuotteita taikka muita tuotteita. SVPL:ssa kuluttaja ei vastaa lievästä huolimattomuudesta, mutta tilaajan vastuuta ei ole MPL:a vastaavalla tavalla euromääräisesti rajoitettu. Käyttäjän vastuun laajuus oikeudettomasti tilatun digitaalisen sisällön osalta on kirjaimellisesti eurosta kiinni: mikäli liittymällä on tehty oikeudettomasti ostoja 51 eurolla tai yhteensä 301 eurolla kuukauden aikana, tavallisen huolimattomuuden osalta käyttäjän vastuu rajoittuu MPL:n nojalla 50 euroon. Käyttäjä ei lievän huolimattomuuden tilanteessa ole vastuussa lainkaan, mikäli veloituksia on tehty enintään 50 eurolla tai yhteensä 300 eurolla kuukaudessa, mutta lievää suuremman huolimattomuuden kohdalla kuluttaja vastaa 300 euroon asti itse.

5 Sähköisten tunnistusvälineiden käyttäjän vastuuttamisesta

Erilaisilla alustoilla asiointi edellyttää yleensä käyttäjän tunnistamista. Tunnistaminen rakentuu henkilön sähköiseen identiteettiin kuuluville tiedoille ja ominaisuuksille.[112] Sähköisen identiteetin hyödyntäminen on peruselementti digitaalisessa sopimisessa ja muussa tietoverkkojen varassa tapahtuvassa asioinnissa, ja on siten myös oikeustoimikelpoisuuden käyttöväline digitaalisessa toimintaympäristössä kuten verkkoalustoilla.[113] Käyttäjän tunnistaminen on edellytys sille, että käyttäjä voi käyttää oikeudellista identiteettiään ja esimerkiksi velvoittautua erilaisiin sopimuksiin, kuten ostaa tuotteita verkkokaupasta, lainata rahaa vertaisluottoalustojen välityksellä tai tilata kuljetuspalvelu nouto-

[112] Sähköinen identiteetti koostuu sähköiseen muotoon tallennetuista luonnollisen henkilön ominaisuuksista ja tiedoista, jotka yksilöivät henkilön ja ovat siten ainutlaatuisia, jotta ne voidaan yhdistää vain tiettyyn henkilöön. Tällaisia ominaisuuksia ja tietoja voivat olla henkilötunnus tai muu tunnus ja henkilön perhettä tai tämän toimintaa ja asemaa kuvaavat tiedot. Sähköisestä identiteetistä etenkin julkisen hallinnon näkökulmasta ks. Voutilainen 2008, s. 4. Vrt. Pöysti 1999, s. 1112 ss. jossa hän viittaa sähköisellä identiteetillä oikeussubjektiin teknisesti tai oikeudellisesti luotettavalla tavalla yhdistyvää informaatioon, jonka perusteella henkilö voidaan tunnistaa sähköisessä ympäristössä.

[113] Pöysti 2000, s. 93 ja Voutilainen 2008.

ruoalle.[114] Sähköisellä tunnistamisella viitataan sähköisessä ympäristössä tapahtuvaan menettelyyn, jossa palvelun käyttäjä yksilöidään tietyksi väitetyksi tai oletetuksi henkilöksi siten, että siinä verrataan palvelun käyttäjän antamaa tietoa palveluntarjoajalla olevaan yksilöivään tunnistusinformaatioon.[115]

Sähköiset tunnistamismenetelmät jaetaan *heikkoihin* ja *vahvoihin* tunnistusmuotoihin. Heikkoa tunnistamista ovat sähköpostiosoitteen tai käyttäjätunnuksen ja salasanan yhdistelmät sekä ns. *Facebook-kirjautuminen*, jonka avulla kirjaudutaan Facebookin ulkopuolella tarjottaviin palveluihin.[116] Tunnistamisen tekee heikoksi se, että käyttäjän henkilöllisyydestä ei saada täyttä varmuutta.[117] Vahvasta sähköisestä tunnistamisesta säädetään laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009, jäljempänä Tunnistuslaki). Vahvalla sähköisellä tunnistamisella tarkoitetaan Tunnistuslain 2 §:n 1 momentin 1 kohdan mukaan ”henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden todentamista sähköistä menetelmää käyttäen, joka täyttää sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen[118] 8 artiklan

[114] Oikeudellinen identiteetti koostuu oikeuskelpoisuudesta, oikeustoimikelpoisuudesta sekä toimivallasta. Näin mm. Pöysti 1999, s. 1113. Suomessa sähköinen tunnistaminen käytännössä rinnastetaan sopimuksen tekemiseen ja sillä on samanlaiset oikeusvaikutukset kuin sähköisellä allekirjoituksella, ks. HE 36/2009 vp, s. 27. Vrt. kuitenkin Ponka 2013, joka katsoo, ettei tunnistamisen ja allekirjoittamisen käsitettä tule sekoittaa keskenään.

[115] Pöysti 1999, s. 1114. Tunnistuksen yhteydessä henkilö *todennetaan,* jolla viitataan toimenpiteeseen, jossa henkilön identiteetti varmistetaan jotakin olemassa olevaa tietoa vasten. Tunnistus tapahtuu henkilön hallussa olevan tunnisteen avulla ja todentaminen esimerkiksi käyttäjän hallussa olevan salasanan avulla. Ks. Voutilainen 2008, s. 5, jossa tunnisteena pidetään tietokokonaisuutta, jolla ”henkilön sähköinen identiteetti voidaan todentaa sähköisessä yhteydenpidossa”.

[116] Esimerkiksi Airbnb-palveluun voi kirjautua kolmannen tahon tarjoamalla sometilillä (Social Networking Services Account), kuten Facebookin tai Googlen välityksellä. Ks. Airbnb:n käyttöehdot kohta 4.2.

[117] Ks. mm. Airbnb:n käyttöehdot kohta 2.4, jossa korostetaan, ettei Airbnb sitoudu varmistumaan käyttäjänsä henkilöllisyydestä. Halutessaan Airbnb voi kuitenkin ryhtyä erilaisiin toimiin henkilöllisyyden varmentamiseksi.

[118] Laissa viitataan Euroopan parlamentin ja neuvoston asetukseen (EU) N:o 910/2014 sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta.

2 kohdan b alakohdassa tarkoitetun korotetun varmuustason tai mainitun kohdan c alakohdassa tarkoitetun korkean varmuustason vaatimukset". Lain 8a §:n mukaan tunnistusmenetelmässä on käytettävä vähintään kahta seuraavista todentamistekijöistä:

1) todentamistekijä, joka perustuu tiedossa oloon ja jonka henkilön on osoitettava olevan tiedossaan (jotain, mitä käyttäjä tietää)
2) todentamistekijä, joka perustuu hallussapitoon ja jonka henkilön on osoitettava olevan hallussaan (jotain, mitä käyttäjällä on hallussaan)
3) johonkin luonnollisen henkilön fyysiseen ominaisuuteen perustuvaa luontaista todentamistekijää (mm. käyttäjän sormenjälki).

Tällaisia todentamistekijöitä yhdistäviä tunnistusmenetelmiä ovat esimerkiksi käyttäjätunnus, jota käytetään tunnistamistapahtumassa yhdessä sirukortin tai muun välineen, kuten salasanalistan kanssa. Käytännössä kysymys voi olla verkkopankkitunnuksista, poliisin myöntämästä kansalaisvarmenteesta sekä teleyritysten tarjoamasta mobiilivarmenteesta. Vahvan sähköisen tunnistamisen perusajatuksena on se, että luotettava, luottamusverkostoon kuuluva toimija takaa palvelunkäyttäjän henkilöllisyyden, jolloin palveluntarjoaja tai muu osapuoli voi varmistua vastapuolen identiteetistä.[119]

Tunnistuslaki sisältää säännöksen vahvan tunnistusvälineen haltijan vastuusta oikeudettoman käytön tilanteesta, mutta heikoista tunnistusvälineistä ei ole erikseen säädetty.[120] Heikkoa tunnistamista on lähtökohtaisesti kaikki muut kuin vahvan tunnistamisen menetel-

[119] Ne vahvaa tunnistuspalvelua tarjoavat, jotka ovat tehneet Tunnistuslain ilmoituksen ja täyttävät lain vaatimukset, muodostavat sähköisen tunnistamisen luottamusverkoston. Tässä verkostossa on kaksi tunnustuspalvelun tarjoamisen muotoa: 1) välineen tarjoaja, joka tarjoaa tunnistusvälineitä loppukäyttäjälle sekä 2) tunnistusvälityspalvelun tarjoajat, jotka välittävät tunnistustapahtumia sähköisten palveluiden tarjoajille. Luottamusverkoston ideana on se, että sähköiset asiointipalvelut voivat hankkia sähköistä tunnistamista palveluunsa keskitetysti siten, että palveluntarjoajat voivat tehdä sopimuksen tunnistuspalvelun käytöstä vain yhden välityspalveluntarjoajan kanssa.

[120] Tunnistuslain mukainen vastuujako koskee lain 1 §:n 1 momentin nojalla vain vahvoja tunnistusvälineitä.

mät. Koska heikkojen tunnistusmenetelmien, kuten käyttäjätunnuksen ja salasanan, osalta erillissääntelyä ei ole, alustojen käyttäjien vastuu ja huolellisuusvelvoitteiden sisältö määräytyvät lähtökohtaisesti sopimusehtojen sekä yleisten sopimusoikeudellisten periaatteiden perusteella, kuten kauppalain (355/1987) vastuunjakoa ilmentävien periaatteiden nojalla.[121] Tällöin kuitenkin toimintavelvollisuuksien määrittelyssä sopimusehdoilla on keskeinen asema, ja alustojen käyttöehdoissa korostetaankin tyypillisesti käyttäjätilitunnusten luottamuksellisuutta ja henkilökohtaisuutta.[122]

> Kuvayhteisö- ja sisällönjakopalvelualusta *Instagramin* käyttäjiä on lähestytty tekijänoikeusrikkomusvaroitukseksi naamioiduilla huijausviesteillä (fake copyright infringement), joissa väitetään, että käyttäjä on syyllistynyt tekijänoikeuksien rikkomiseen. ”Copyright Centeriltä” tulleen viestin mukaan käyttäjällä on päivä aikaa selvittää rike, tai tili poistetaan. Viesti ohjaa klikkaamaan *Appeal*-linkkiä muun muassa tilin vahvistamiseksi, jolloin käyttäjää yritetään erehdyttää antamaan Instagram-käyttäjätunnukset, sähköpostiosoitteen sekä sähköpostin salasanan. Tilin kaappaamisen jälkeen huijarit voivat alkaa vaatia rahaa tai levittää roskasisältöä. Instagram on tänä päivänä yksi keskeisimmistä kanavista henkilöbrändin tuotteistamisessa sekä käyttäjien omien ja yhteistyötahojen tuotteiden markkinoimisessa ja mainonnassa, jolloin tilin kaappaus voi aiheuttaa merkittävääkin taloudellista vahinkoa esimerkiksi

[121] Myös alustojen digitaalisiin palveluihin sovelletaan KSL 2 luvun säännöksiä sopimattomista kaupallisista menettelyistä sekä KSL 3 luvun säännöksiä kohtuuttomista sopimusehdoista. Näiden lukujen yleissäännökset ovat hyödyke- ja teknologianeutraaleja. Digitaalisten palveluiden sääntelystä ks. Raijas ym. 2019.

[122] Ks. Airbnb:n käyttöehdot kohta 4.5, jossa kielletään tunnusten luovuttaminen kolmannelle sekä asetetaan käyttäjälle velvollisuus ilmoittaa tunnusten joutumisesta toisen haltuun tai mahdollisesta luvattomasta käytöstä: ”You are responsible for maintaining the confidentiality and security of your Airbnb Account credentials and may not disclose your credentials to any third party. You must immediately notify Airbnb if you know or have any reason to suspect that your credentials have been lost, stolen, misappropriated, or otherwise compromised or in case of any actual or suspected unauthorized use of your Airbnb Account. You are liable for any and all activities conducted through your Airbnb Account, unless such activities are not authorized by you and you are not otherwise negligent (such as failing to report the unauthorized use or loss of your credentials).”

saamatta jääneiden voittojen muodossa puhumattakaan siitä, mitä sähköpostitilin kaappaaminen saattaa aiheuttaa.[123]

5.1 Huolimaton toiminta vahvojen sähköisten tunnistusvälineiden haltijan vastuun perusteena

Tunnistamisvälineen oikeudettomassa käytössä on kysymys virheellisestä positiivisesta tunnistamisesta, jossa vilpillisen menettelyn tai tunnistuspalvelun häiriön seurauksena joku voi tunnistautua toisena henkilönä ja tehdä oikeustoimia toisena esiintyen.[124] Tunnistuslain lähtökohta on sama kuin MPL:ssa: tunnistusvälineen haltija ei vastaa oikeudettomasta käytöstä.[125] Toisena lähtökohtana kuitenkin on, että verkossa toimivien primääripalveluntarjoajien on voitava luottaa siihen, että palvelunkäyttäjä on todella se, joka hän väittää olevansa.[126] Tätä vaihdannan luottamusta laissa suojataan siten, että Tunnistuslain ja tunnistusvälinettä koskevan sopimuksen sisältämien velvoitteiden rikkomisella haltija on vastuussa oikeudettomasta käytöstä.

Kuten MPL:n kohdalla, myös Tunnistuslaki sisältää säännöksen tunnustenhaltijalta edellytettävästä huolellisuudesta, ja vastuunjakoperiaatteet ovat Tunnistuslain 3 §:n nojalla kuluttajan eduksi vähimmäispakottavaa sääntelyä.[127] Tunnistuslain 23 §:n 1 momentin mukaan tunnistusvälineen haltijan ”on käytettävä tunnistusvälinettä sopimuksen ehtojen mukaisesti” sekä säilytettävä tunnistusvälinettä tai tunnistamiseen tarvittavia yksilöintitietoja huolellisesti. Arvioitaessa millaisia varotoimia käyttäjä-haltijalta voidaan kohtuudella edellyttää, tulee huomioida, että tunnistusvälineet ovat tyypillisesti tarkoitettu käytettäväksi usein ja niitä tulee voida kuljettaa mukana. Tunnistuslain

123 Ks. Kaspersky Lab official blog, jossa todetaan, että huijaus on tehty erittäin vakuuttavalla ja taidokkaalla tavalla. Blogissa annetaan ohjeita, kuinka käyttäjä voi suojautua Instagram-tilin kaappaamiselta. Yksi neuvo on, ettei käyttäjätunnusta tai salasanaa saa koskaan luovuttaa autentikointia varten kolmannen osapuolen palveluille ja sovelluksille.

124 Muista oikeudettoman tunnistusvälineen käyttötilanteiden syntymisestä ks. Norros 2016, s. 29–30.

125 Ks. Norros 2016, s. 38, joka on katsonut, että pääsääntöisesti palveluntarjoaja ei voi rajoittaa vastuutaan vetoamalla siihen, että vahingon aiheuttamisen on vaikuttanut kolmannen rikos tai muu vilpillinen menettely.

126 Ks. HE 36/2009, s. 1 ja 36.

127 HE 36/2009 vp, s. 43.

esitöiden perusteella haltijan toimintavelvollisuudet vastaavat samanlaisia huolellisuus- ja varotoimia kuin mitä MPL:n vastuujärjestelmä sisältää.[128] Siten tunnistusvälineiden haltijalta edellytetään samanlaista huolellisuutta tunnistusvälineen ja yksilöivien tietojen säilyttämisessä ja käyttämisessä. Lisäksi varotoimiin kuuluu myös se, että haltija seuraa välineen tallella oloa olosuhteiden edellyttämällä tavalla (tarkistamisvelvollisuus).[129] Tunnistusväline on korostetun henkilökohtainen, ja lainkohdan 2 momentissa kielletään erikseen tunnistusvälineen luovuttaminen toisen käyttöön. Tunnistuslain 27 §:n 1 momentin mukaan vastuun synnyttää:

1) tunnistusvälineen luovuttaminen toiselle (1 kohta). Lain esitöissä tunnistusvälineen luovuttamisella tarkoitetaan tietoista ja vapaaehtoista hallinnan luovutusta: sinänsä luovutuksen tarkoituksella ei ole merkitystä, mutta lainkohdan soveltuminen edellyttää haltijan tietoista hallinnan luovutusta. On katsottu, että tunnistusvälineiden hallinnan luovutus ilmentää haltijan ottamaa riskiä väärinkäytöstilanteesta, minkä vuoksi haltija vastaa riskin toteutumisesta.[130]
2) haltijan lievää suurempi huolimattomuus, jonka seurauksena tunnistusväline katoaa, joutuu oikeudettomasti toisen haltuun tai sivullinen käyttää välinettä oikeudettomasti (2 kohta).
3) haltija laiminlyö ilmoittaa 25 §:n edellyttämällä tavalla tunnistuspalvelun tarjoajalle tai sen ilmoittamalle muulle taholle välineen katoamisesta, oikeudettomasti toisen haltuun joutumisesta taikka oikeudettomasta käytöstä (3 kohta).

[128] HE 36/2009 vp, s. 60. Yksilöintitietoja ovat asiakastunnukset, PIN-koodit ja muut tunnusluvut.

[129] HE 36/2009 vp, s. 60. Myös tunnistusvälineiden tarkistamisvelvollisuus on korostunut paikoissa, joissa on korkea anastusriski.

[130] HE 36/2009 vp, s. 64. Tietoinen luovutus synnyttää haltijalleen vastuun, tapahtuipa se missä tarkoituksessa tahansa. Tapauksessa KKO 2016:73 katsottiin, että Tunnistuslain 27 §:n 1 momentin 1 kohtaa, KSL 7 luvun 40 §:n 1 momentin 1 kohtaa ja maksupalvelulain 62 §:n 1 momentin 1 kohtaa välineen luovuttamisen osalta on tulkittava yhdenmukaisesti tilanteiden samankaltaisuuden vuoksi. Tietoista luovuttamista ovat myös välineen hallinnan siirron lisäksi sellaisen salasanan tai muun tunnuksen ilmaiseminen, joka on tarkoitettu ainoastaan haltijan tietoon.

Kuten SVPL:n 125 §:ssä, myös Tunnistuslaissa vastuu syntyy ainoastaan lievää suuremman huolimattomuuden osalta, joten tältä osin Tunnistuslaki eroaa MPL:stä. Merkittävin ero MPL:n järjestelmään on se, ettei haltijan vastuuta ole euromääräisesti rajoitettu, eikä vastuuta ole euromääräisesti jaoteltu huolimattomuuden asteen perusteella. Lain esitöiden mukaan syynä tähän on se, että ”vahvan sähköisen tunnistuspalvelun tarjoamisessa on kyse aivan toisenlaisesta toimintaympäristöstä” kuin mihin MPL:n säännös on tarkoitettu.[131] Esitöissä ei kuitenkaan millään tavalla selvennetä, miltä osin ympäristön erilaisuus ilmenee.

5.2 Vastuun sisällön arviointia ratkaisussa KKO 2016:73

Lievän huolimattomuuden ja haltijan vastuun rajoja on tarkasteltu korkeimman oikeuden ratkaisussa KKO 2016:73, jossa arvioitiin B:n huolellisuutta verkkopankin käyttäjätunnuksen ja avainlukulistan säilyttämisessä sekä sitä, onko B vastuussa tunnistusvälineidensä oikeudettomasta käytöstä luoton myöntänyttä yhtiötä kohtaan. Tapausta voidaan pitää merkittävänä, sillä siinä myös linjattiin Tunnistuslain 27 §:n vastuun sisältöä. Nimittäin lainkohdassa ei lainkaan määritellä, minkälaisesta vastuusta on kysymys ja kenelle haltija on vastuussa. Myöskään lain esityöt eivät määrittele vastuun sisältöä, eikä niin sanottu eIDAS-asetus[132] sisällä vastaavaa säännöstä.

> Tapauksessa B oli säilyttänyt käyttäjätunnuksia ja avainlukulistaa kotonaan samassa paikassa perheen ns. laskulaatikossa tavalla, joka mahdollisti sen, että hänen puolisonsa C oli tietoinen niiden säilytyspaikasta. B:n tietämättä ja suostumuksetta C oli käyttänyt B:n verkkopankkitunnuksia, ja ottanut B:n nimissä kuluttajaluoton jättäen luoton maksamatta ja salaten velkaan liittyvät perintäkirjeet. Luotonantajana ollut A Oy vaati, että B velvoitetaan maksamaan maksamatta jäänyt kuluttajaluotto liitännäissaatavineen, sillä B oli ainakin laiminlyönyt ilmoittaa tunnis-

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

[132] Euroopan parlamentin ja neuvoston asetus 910/2014/EU sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta.

tuspalvelun tarjoavalle pankilleen tunnusten joutumisesta puolisonsa haltuun. C oli käyttänyt B:n tunnistusvälinettä yli vuoden ajan, mistä voitiin päätellä, ettei B ollut säilyttänyt tunnuksia huolellisesti. C oli tuomittu kuvatunlaisesta toiminnasta rangaistuksiin useista petoksista.[133]

Korkein oikeus katsoi, että B oli käyttänyt luonteeltaan vahvaan sähköiseen tunnistamiseen käytettyjä välineitä huolimattomasti, mikä täytti Tunnistuslain 27 §:n 1 momentin 2 kohdan vastuun syntymisen edellytyksen. Vastuuarvioinnin lähtökohtana on, että koska tunnistusväline on juuri henkilöllisyyden luotettavan tunnistamisen vuoksi henkilökohtainen, haltijan tulee pitää hänelle henkilökohtaisesti myönnettyä tunnistusvälinettä vain omassa hallinnassaan ja ”pyrkiä kohtuullisin toimin estämään välineen väärinkäytön”. B oli rikkonut huolellisuusvelvoitteensa säilyttämällä tunnistetta huolimattomasti, sillä korkeimman oikeuden mukaan tunnisteen ”avoin säilytystapa” ei täytä edes perheenjäsenten kesken huolellisen säilyttämisen vaatimuksia.[134] Korkein oikeus katsoi edelleen, ettei B:n huolimattomuus ollut lievää, sillä B ei ollut ryhtynyt minkäänlaisiin toimiin pitääkseen tunnistusvälineen suojassa. Näin ollen B oli itse vastuussa tunnistusvälineiden oikeudettomasta käytöstä. Tästä johtuen B oli vastuussa myös hänen tunnistusvälineitään käyttäen otetusta luotosta ja siten velvollinen suorittamaan maksamatta jääneen luoton 100 euron pääoman korkolain 4 §:n 1 momentissa tarkoitettuine viivästyskorkoineen.[135]

Korkeimman oikeuden ratkaisun merkittävämpänä linjauksena voidaan pitää tunnistusvälineen haltijan sopimusvastuun syntymistä suhteessa kolmanteen osapuoleen. Argumentaatiossaan ja tulkinnassaan korkein oikeus nojautui vahvasti aikaisemmin voimassa olleeseen KSL

[133] Sekä käräjäoikeus että hovioikeus katsoivat, ettei B ollut vastuussa verkkopankkitunnusten oikeudettomasta käytöstä, sillä tunnistusvälineen oikeudeton käyttö ei johtunut B:n lievää suuremmasta huolimattomuudesta eikä B ollut tietoisesti luovuttanut tunnuksia C:lle. B:n vastuuta vastaan puhuvia seikkoja olivat se, ettei B ollut tietoinen C:n menettelystä, B ei ollut luovuttanut tunnistusvälinettä C:lle ja C oli suunnitelmallisesti salannut toimintansa ja perintäkirjeet B:ltä. Alemmat oikeusasteet myös katsoivat, ettei B:llä C:n toiminnasta johtuen ollut edellytyksiä ilmoittaa tunnistusvälineiden joutumisesta oikeudettomasti toisen haltuun.

[134] Korkein oikeus kuitenkin huomioi myös tyypillisesti vallitsevia perheolosuhteita sekä yhteisen talouden hoitamiseen liittyviä piirteitä. Korkein oikeus totesi, että kodin piirissä tapahtuvaa varomatonta tunnistusvälineen käsittelyä voidaan herkemmin pitää vain lievänä huolimattomuutena.

[135] Tapauksessa korkein oikeus kuitenkin katsoi, ettei luotonantajalla ollut oikeutta periä muita luottokustannuksia, sillä kuluttajaluottosopimusta ei ollut tehty KSL 7 luvun 15 §:n 1 momentin mukaisessa määrämuodossa eli kirjallisesti tai sähköisesti siten, että sopimus voidaan tallentaa ja toisintaa muuttumattomana.

7 luvun 19 §:n säännökseen ja sitä koskevaan tulkintaan.[136] Siten kumotulla KSL 7 luvun 19 §:n säännökselle ja sitä koskevalle tulkintakäytännölle annettiin ratkaisussa vahva merkitys. Korkein oikeus totesi ratkaisussaan, että lain esitöistä voidaan päätellä tunnistusvälineen haltijan vastuun olevan lopputulokseltaan samankaltainen kuin kuluttajan vastuu luotto- ja maksuvälineiden oikeudettomasta käytöstä, vaikkakin KKO toteaa, että Tunnistuslain ja KSL:n säännökset koskevat eri tilannetta. KKO katsoi, että vahvalla tunnistusmenetelmällä myönnetty luotto on verrattavissa luottokortin käyttöön. Korkein oikeus katsoi, että jos tunnistusvälineen oikeudeton käyttö johtuu haltijan tahallisesta tai tuottamuksellisesta menettelystä, vastaa haltija myös luotosta. Tämä haltijan sopimusvastuu luotonantajaa kohtaan on vastaava kuin hänen itse tekemässään luottosopimuksessa.

Siinä missä MPL:n vastuujärjestelmä koski ainoastaan maksupalveluntarjoajan ja käyttäjän välisen oikeussuhteen sisäistä vastuun- ja riskinjakoa, Tunnistuslaki luo oikeusvaikutuksia myös tunnistuspalvelun tarjoajan ja käyttäjän välisen sopimussuhteen ulkopuoliselle, kolmannelle palveluntarjoajalle. Vastuun syntyminen tunnistusvälineen haltijan näkökulmasta tarkoittaa, että oikeudettoman käytön seurauksena syntyneet oikeustoimet ovat haltijaa sitovia.[137] Tällaista tahdosta riippumatonta sopimussitovuutta voidaan pitää merkittävänä poikkeuksena sopimusvapauden periaatteeseen.[138]

6 Kokoavia näkökohtia vastuujärjestelmistä ja kuluttaja-käyttäjien vastuuttamisesta

MPL:n, KSL:n, SVPL:n ja Tunnistuslain säännöksillä on yhteneväinen lähtökohta: kuluttajan asemassa oleva käyttäjä ei lähtökohtaisesti vastaa oikeudettomasta käytöstä, ja käyttäjän vastuutilanteet on tyh-

136 Korkein oikeus viittasi esimerkiksi ratkaisun KKO 2006:81 oikeusohjeisiin.

137 Mahdollista on myös, että oikeudettomasti välinettä käyttävä voi luopua haltijan oikeudesta suhteessa kolmanteen. Ks. Norros 2016, s. 30.

138 Sopimusvapauden periaatteen yhtenä elementtinä on päätäntävapaus: lähtökohtaisesti jokaisella oikeussubjektilla on oikeus päättää, sitoutuuko hän sopimukseen vai jättääkö hän sopimuksen tekemättä.

jentävästi määritelty laissa vähimmäispakottavasti. Siten säännökset ovat merkittävä osa kuluttajan kyberturvallisuutta. Käyttäjän yksilövastuu on käytännössä tuottamusvastuuta,[139] eli sääntelyn ja sopimuksen sisältämien toimintavelvoitteiden huolimattomuudesta johtuvat laiminlyönnit perustavat vastuun. MPL:n ja KSL:n osalta toimintavelvoitteiden sisältöä ja vastuun laajuutta arvioidaan yhtenäisin perustein. Sen sijaan Tunnistuslain ja SVPL:n soveltamistilanteiden osalta käyttäjän huolimattomuutta ja toimintavelvollisuuksien sisältöä arvioidaan oikeuskäytännössä aiemmin voimassa olleen KSL 7 luvun 19 §:n säännöksen ja oikeuskäytännön perusteluihin tukeutuen: Kumotut oikeudetonta käyttöä koskevat normit raamittavat huolimattomuuden arviointia myös viestintäpalveluiden ja tunnistusmenetelmien osalta.

Tunnistuslaissa ja SVPL:ssa ei ole rajoitettu kuluttajan vastuuta kuten MPL:n ja KSL:n säännöksessä, joissa kuluttajan vastuu huolimattomuudesta rajautuu euromääräisesti. Toiseksi Tunnistuslaissa ja SVPL:ssa kuluttajan lievä huolimattomuus ei synnytä vastuuta. Kolmanneksi vastuujärjestelmät eroavat toisistaan sopimusulottuvuutensa osalta. MPL koskee maksupalvelun tarjoajan ja maksupalvelun käyttäjän välistä riskinjakoa ja vastuun kohdentumista, eikä lakia sovelleta primääripalvelun hankintaa koskevaan sopimussuhteeseen. KSL:n säännös koskee luotoantajan ja luottoon oikeuttavan tunnisteen haltijan suhdetta ja SVPL koskee teleyrityksen ja liittymän haltijan vastuunjakoa. Korkein oikeus on ratkaisussaan KKO 2016:73 tulkinnut Tunnistuslain puolestaan mahdollistavan sen, että huolimattomasti tunnistusvälineitään säilyttänyt kuluttaja on vastuussa sopimuksen täyttämisestä primääripalveluita tarjonneelle. Heikkojen tunnistusmenetelmien, kuten käyttäjätunnuksen ja salasanan, osalta erillissäätelyä ei

[139] HE 231/2005 vp, s. 17. Tuottamusvastuulla viitataan siihen, että osapuoli vastaa vahingosta vain, jos se on aiheutunut tahallisesta tai tuottamuksellisesta toiminnasta. Tunnistusvälineiden osalta ks. Ponka 2013, s. 403.

ole, vaan alustojen käyttäjien vastuu ja huolellisuusvelvoitteiden sisältö määräytyvät lähtökohtaisesti sopimusehtojen perusteella.[140]

Kilpailu- ja kuluttajavirasto onkin peräänkuuluttanut huomion kiinnittämistä siihen, voivatko vastuujärjestelmät sisältää sellaisia ristiriitoja ja tulkinnanvaraisuuksia, joiden seurauksena kuluttaja voi joutua kantamaan kohtuuttoman suuren vastuun tunnistusvälineiden oikeudettomasta käytöstä.[141] Alustatalouteen osallistuvan kuluttajan näkökulmasta voi olla vaikea hahmottaa, mitä vastuusääntelyä sovelletaan missäkin tilanteessa ja miten häneltä vaadittava huolellisuuden taso kulloinkin määräytyy: pidetäänkö oikeudellisessa arvioinnissa esimerkiksi verkkopankkitunnuksia maksuvälineenä vai tunnistamismenetelmänä? Verkkopankkitunnusten käytön ja sähköisten maksu- ja tunnistustapahtumien osalta on käyttäjille tulossa näkyviä muutoksia, sillä uusi MPL:n sääntely (85b §) edellyttää palveluntarjoajilta vahvan tunnistamisen käyttöä, jos maksaja käyttää maksutiliään tietoverkon välityksellä, käynnistää sähköisen maksutapahtuman tai toteuttaa etäkanavan kautta toimen, johon voi liittyä väärinkäytöksen riski. Tunnuslukulistojen osalta on katsottu, etteivät ne täytä hallussapitoa koskevan elementin vaatimuksia[142]. Tästä syystä paperisten avainlukulistojen lisäksi vaaditaan 14.9.2019 alkaen toinen tunnistamisen elementti, jotta sääntelyn edellyttämä kaksiosainen tunnistaminen toteutuu.[143] Osa pankeista on ilmoittanut luopuvansa avainlukulistojen käytöstä kokonaan[144]. Taustalla on PSD2:sta seuraava teknisiä standardeja koskeva sääntely, jonka tarkoituksena on muun muassa parantaa maksupalveluiden turvallisuutta, vähentää petosriskiä sekä esimerkiksi pienentää paperisten avainlukulistojen kopiointimahdollisuuk-

[140] Myös alustojen digitaalisiin palveluihin sovelletaan KSL 2 luvun säännöksiä sopimattomista kaupallisista menettelyistä sekä KSL 3 luvun säännöksiä kohtuuttomista sopimusehdoista. Näiden lukujen yleissäännökset ovat hyödyke- ja teknologianeutraaleja. Digitaalisten palveluiden sääntelystä ks. Raijas ym. 2019.

[141] Ks. mm. Hannula 2017, jossa todetaan, että Tunnistuslaki ja maksupalvelulainsäädäntö kytkeytyvät vahvasti toisiinsa siten, että näitä vastuujärjestelmiä tulisi arvioida kokonaisuutena.

[142] Ks. FIVA8/01.02/2019, jossa todetaan, ettei kannanotto tunnuslukulistojen käytön jatkamisesta koske tilanteita, joissa pankkitunnuksia käytetään vahvaan tunnistamiseen muihin kuin maksamiseen ja maksutilin käyttöön liittyviin palveluihin. Kannanotto ei myöskään koske Tunnistuslain tulkintaa.

[143] EBA-Op-2019-06 ja FIVA8/01.02/2019.

[144] YLE 29.3.2019.

sia.[145] Paperisten listojen tilalle pankit ovat tarjonneet muun muassa älypuhelimeen mobiiliavainta, tunnuslukusovellusta, tunnuslukulaitetta tai tekstiviestivahvistusta.[146] Sovelluspohjaisiin ratkaisuihin siirryttäessä onkin pohdittava, millaisia vaatimuksia laitteiden ja ohjelmien käytön osalta käyttäjään kohdistuu, ja johtaako älypuhelimen hallintaan kytkeytyvien eri palveluntarjoajien yhteen kietoutuminen myös vastuuperusteiden monimutkaistumiseen. Toisin sanoen, mikä vaikutus käyttäjän vastuun arvioinnin kannalta on silloin, kun älypuhelimen hallintaan ja käyttöön kytkeytyy useita eri sovelluksia ja sovelluksia kehittäviä palveluntarjoajia.

Kuluttaja-käyttäjän vastuu konkretisoituu alustoilla säilyttämisvelvollisuuksina, tunnuslukujen ja muiden turvatunnusten huolellisena säilyttämisenä, välineiden tallella olon seuraamisena ja tietoturvasta huolehtimisena. Näiden toimintavelvollisuuksien sisällöillä on kyberfyysiset ulottuvuutensa niiden tarkemman sisällön jäädessä teknologian kehityksen ja oikeuskäytännön varaan. Mielenkiintoista esimerkiksi on se, mitä on digitaalinen huolimaton säilyttäminen: onko esimerkiksi sovellusväärennöksen lataaminen älypuhelimeen tai virustorjunnan laiminlyönti maksupalvelun käyttäjän toimintavelvollisuuksien laiminlyöntiä? Digitaalisessa ympäristössä vastuuarvioinnissa näyttää korostuvan käyttäjän osaaminen, ymmärtäminen ja riskien tiedostaminen: eri asia on, millaista osaamisen ja tietämyksen tasoa voidaan odottaa.

Kohonneen riskin tilanteissa kuluttajien huolellisuusvelvoitteiden on katsottu korostuvan. Tällöin palveluntarjoajien ohjeistukset, tiedottaminen sekä turvallisuusriskeistä ja varotoimenpiteistä mainitseminen sopimusehdoissa ja tiedotteissa luovat pohjan sille, mitä kussakin tilanteessa pidetään huolellisena menettelynä. Vaikka lainsäätäjän

[145] Ks. komission delegoitu asetus 2018/289 Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/2366 täydentämisestä asiakkaan vahvaa tunnistamista sekä yhteisiä ja turvallisia avoimia viestintästandardeja koskevilla teknisillä sääntelystandardeilla, perusteluosiot 1–3 sekä asetuksen 7 artikla. Artiklan mukaan maksupalveluntarjoajien on toteutettava ”toimenpiteitä, joilla vähennetään sitä riskiä, että oikeudettomat tahot käyttävät ryhmään ’hallussapito’ kuuluvia asiakkaan vahvan tunnistamisen tekijöitä”. Toiseksi artikla edellyttää, että ns. maksajan hallussa pidettäviin tekijöihin sovelletaan toimenpiteitä, joiden tavoitteena on estää kyseisten tekijöiden kopioituminen.

[146] Ks. mm. OP.media 1.4.2019 ja Nordean lehdistötiedote 8.5.2018.

lähtökohtaisena ajatuksena on ollut rajoittaa kuluttaja-käyttäjän vastuuttamista turvallisuusvelvoitteita synnyttävillä sopimuslausekkeilla, oikeuskäytännössä lausekkeille on annettu tosiasiallisesti toimintavelvoitteita laajentava vaikutus. Näin ollen huolimattomuus vastuuperusteena mahdollistaa kuluttaja-käyttäjän vastuuttamisen siten, että hänelle sopimusvelvoitteissa siirretään vastuuta turvallisuuden tuottamisessa. Vastuuttamista rajoittaa toki KSL 3 luvun 1 §:n kohtuuttomien sopimusehtojen käyttämisen kieltävä säännös. Säännöksen yleislausekkeen heikkoutena on kuitenkin pidetty sitä, että se ei täsmällisesti määrittele sitä, millaisia huolellisuusvelvoitteita ja taloudellisen riskin jakamista koskevia ehtoja pidetään kohtuullisina.[147]

Digitaalisen ympäristön jatkuva kehittyminen edellyttää käyttäjiltään jatkuvaa sopeutumista. Esimerkiksi maksamisen ja maksupalveluiden markkinat ovat murroksessa ja palvelutarjoajien kenttä on edelleen pirstaloitumassa ja monipuolistumassa.[148] Maksutilejä pitävien pankkien lisäksi ns. kolmannet osapuolet voivat tarjota maksutoimeksiantojen käynnistyspalveluita ja tilitietopalveluita, joiden tarjoaminen ei enää edellytä kolmannen palveluntarjoajan ja pankin välistä sopimusta.[149] Kuluttajat kohtaavat verkossa yhä enemmän vaihtoehtoja maksamiselle sekä yhä enemmän välikäsiä ja maksupalveluiden

147 Ks. esim. HE 231/2005 vp, s. 14. Kuluttajaa suojaavana voidaan pitää myös KSL 4 luvun 3 §:n tulkintaperiaatetta, jonka mukaan yksipuolisesti laadittua epäselvää sopimusehtoa tulkitaan laatijansa vahingoksi. Yksipuolisesti laadittujen vastuunrajoitusten osalta epäselvyyssäännön merkitys korostuu entisestään, koska vastuunrajoitusten osalta suppeaa tulkintaa pidetään muutenkin yleisenä lähtökohtana. Ks. Hemmo I 2003, s. 654.

148 Tämä on seurausta uuden EU-sääntelyn tavoitteesta lisätä kilpailua ja kuluttajien toimintavaihtoehtoja sekä mahdollistaa uusien palvelutarjoajien tarjoamat palvelut. Ks. KKV tiedote 12.1.2018.

149 Maksutoimeksiantojen käynnistyspalveluilla tarkoitetaan kuluttajien pyynnöstä kolmannen maksupalveluntarjoajan käynnistämää maksutoimeksiantoa, joka koskee toisen palvelutarjoajan, kuten pankin tarjoamaa maksutiliä (Payment Initiation Service, PIS). Kuluttajien pyynnöstä käynnistyvä maksutoimeksianto voi olla esimerkiksi kuluttajan verkkokaupassa tai alustalla antama lupa ulkopuoliselle palveluntarjoajalle maksun tai tilisiirron tekemiseksi, joka annetaan maksutapavaihtoehtojen valinnassa. Tilitietopalveluilla (Account Information Service, AIS) viitataan lisäpalveluihin, joita ovat esimerkiksi sovelluspohjaiset henkilökohtaisen taloudenpitoon liittyvät palvelut, ja jotka perustuvat palveluntarjoajan verkon välityksellä koostamaan tietoon pankin pitämästä kuluttajien maksutileistä.

tarjoajia.[150] Myös alustatalouden toimijat (*Alibaba, Amazon, eBay*) ovat ottamassa yhä vahvempaa jalansijaa ja *Facebook* on kehittämässä *Whatsapp*-sovellukseen omaa kryptovaluuttaansa ja maksamisen muotoja[151]. Yhtenä kehitystrendinä näyttääkin olevan se, että erilaiset finanssipalvelut ovat siirtymässä primääripalveluita tarjoaville tai niitä välittäville alustoille, ja alustat ovatkin yhdistäneet perinteisiksi pankkipalveluiksi katsottavia palveluita oman ydintoimintaansa yhteyteen (*Alipay, Amazon Pay, PayPal*).[152]

Kuluttaja-käyttäjien näkökulmasta uudet rahoitusratkaisut, maksutavat ja uudet kolmannet palveluntarjoajat voivat johtaa siihen, että kuluttajien on yhä vaikeampaa hahmottaa digitaalisessa toimintaympäristössä toimivien eri tahojen oikeudellista asemaa ja tästä seuraavia osapuolten vastuita ja velvollisuuksia. Maksaminen ja maksupalvelut ovat sulautumassa osaksi eri palvelukokonaisuuksia ja -yhdistelmiä, joissa primääripalveluntarjoajan ja maksupalvelujen tarjoajan sekä tilinpitäjäpankin roolit ja vastuu-ulottuvuuksien rajat hämärtyvät. Samalla eri palveluntarjoajien välillä vastuuta pyritään tyypillisesti ketjuttamaan ja siirtämään toimijalta toiselle.[153] Huoli on herännyt siitä,

[150] Maksutoimeksiantoja voi tehdä esimerkiksi e-lompakkoa muistuttavan *Paytrail*-maksupalvelun kautta, joissa asiakas voi hallinnoida ja maksaa eri verkkokaupoissa tekemiään maksujaan. Kuluttaja voi rahoittaa ostoksensa *Klarna*-sovelluksella, joka tarjoaa verkkokauppojen yhteydessä mahdollisuuden maksaa ostokset laskulla ja luotolla. Maksuja välittävä *Trustly* tarjoaa mahdollisuuden tehdä maksuja (tilisiirtoja) suoraan pankkitililtä verkkopankkitunnuksia käyttäen ilman, että tilisiirto tehdään kuluttajan pankin välityksellä.

[151] Helsingin Sanomat 1.3.2019.

[152] Mattila – Seppälä – Lähteenmäki 2018, erityisesti s. 5. Alustojen tarjoamat palvelut ovat yleensä maksuttomia ja alhaisesti hinnoiteltuja ja palvelut on integroitu helppokäyttöiseksi ja saumattomaksi kokonaisuudeksi.

[153] Raijas ym. 2019, s. 30, jossa he huomauttavat, että palveluntarjoajat vastaavat omista palveluistaan kuluttajille yleisten kuluttaja- ja sopimusoikeudellisten oppien mukaisesti, eivätkä palveluntarjoajien vastuuta rajoittavat vastuuvapauslausekkeet saa olla kuluttajien kannalta kohtuuttomia. Digitaalisia palveluita koskevaa erityissääntelyä ei voimassa olevassa KSL:ssa ole, mutta EU:ssa on vireillä direktiiviehdotus sopimusoikeudellisesta sääntelystä, joka koskee digitaalisen sisällön virhevastuuta ja toimittamista sekä kuluttajien oikeussuojakeinoja. Ks. COM(2015) 634 final.

kuinka kuluttajat pystyvät tunnistamaan, ketkä ovat luotettavia ja valvonnan piirissä olevia maksutoimeksiantopalvelujen tarjoajia.[154]

Kysymys on relevantti esimerkiksi MPL 62 §:n 1 momentin mukaisessa maksuvälineen käyttäjän vastuuta koskevassa arvioinnissa: sekä MPL:ssä että tyypillisesti maksuvälinettä koskevassa sopimuksessa kielletään maksuvälineen luovuttaminen ulkopuolisen käyttöön. Kuitenkin uusien maksutoimeksiantopalvelun tarjoajien palvelut perustuvat siihen, että uudet palveluntarjoajat voivat hyödyntää pankkien kuluttajille myöntämiä tunnistamismenetelmiä tunnistautumisessa maksutapahtuman yhteydessä.[155] Maksutoimeksiantopalveluiden tarjoajien pääsy tilinpitäjäpankkien asiakkaiden tileille edellyttää asiakkaan suostumusta, mutta kokonaan toinen asia on, onko asiakkailla riittävästi osaamista ja tietoa käytössään, jotta he voisivat välttää asiointia epäluotettavien palveluntarjoajien sivustoilla ja näiden tarjoamien älypuhelinsovellusten lataamista. Toiseksi asiakkaan tulisi myös kyetä arvioimaan, mitä mahdollisia riskejä ja oikeusvaikutuksia hänen antamaansa suostumukseen liittyy. Oikeuskäytännön varaan jääkin, kuinka kuluttajien maksuvälineiden luovuttamista tulisi arvioida tilanteessa, jossa kuluttaja altistuu huijauksille ja väärinkäytöksille siitä syystä, ettei hän ole kyennyt havaitsemaan tai arvioimaan palveluntarjoajan luotettavuutta. Lisäksi mielenkiintoista on seurata, millaiseksi alustojen välityksellä asioivalta maksupalvelun käyttäjältä edellytettävän osaamisen, tiedostamisen ja ymmärtämisen taso muodostuu.

Oikeudettoman käytön uhriksi joutuneella käyttäjällä on oikeus saada korvausta vilpillisesti tai tuottamuksellisesti toimineelta oikeudettomalta käyttäjältä vahingonkorvauksena tai mahdollisesti perusteettoman edun palautuksena. Tosiasiallisesti vahingot jäävät kuitenkin käyttäjän vastattavaksi, mikäli oikeudetonta käyttäjää ei tavoiteta tai hän on maksukyvytön.[156] Haasteita lisää myös se, että erilaisissa tietojen kalasteluissa ja huijausten muodoissa on kysymys valtion

[154] Hannula 2017. Huolenaiheena ovat tulkintakysymykset tilinpitäjäpankin vastuusta kolmansien osapuolten toiminnasta johtuvista väärinkäytöstilanteista.

[155] Hannula 2017. Maksutoimeksiantopalveluiden tarjoajat voivat hyödyntää tilinpitäjäpankin tarjoamaa tunnistamismenettelyä, oli kysymys tilinpitäjäpankin itsensä tarjoamista tunnistuspalveluista tai pankin tunnistuspalveluntarjoajalta hankkimasta tunnistuspalvelusta.

[156] Tunnistusvälineen osalta ks. Norros 2016, s. 30–31.

rajat ylittävästä, jopa ammattimaisesta rikollisuudesta. Lisäksi velvollisuuksille rakentuvan järjestelmän ongelmana ovat vastuunjakotilanteet, joissa on hankalaa, ellei jopa mahdotonta aukottomasti selvittää, kuka osapuolista on rikkonut velvoitteitaan.[157] Tällöin vaarana on, että heikompi osapuoli kantaa vastuun, kuten pankkilautakunnan ratkaisuissa FINE-013434 ja FINE-014299 käsitellyissä tilanteissa näyttäisi käyneen.

7 Lopuksi: Kyberturvallisuuden heikoin lenkki on ihminen – vai onko?

Digitalisaatio, verkkoalustainfrastruktuurit ja kyberturvallisuus kulkevat käsi kädessä. Kyberturvallisuuskysymykset ovat arkipäiväisiä asioita kaikille tietoverkoissa ja verkkoalustoilla toimiville. Kyberturvallisuutta koskevassa keskustelussa on painotettu jokaisen vastuuta turvallisuuden tuottamisessa. Usein velvoittavuusargumentti esitetään listoina asioista, jotka yksilön pitää huomioida digitaalisessa toimintaympäristössä toimiessaan. Esimerkiksi Limnéll ym. mukaan yksilön tulee huolehtia:

- Tietojen varmuuskopioinnista siten, että tärkeät tiedot on tallennettu useampaan turvalliseen paikkaan. Tällöin esimerkiksi tietokoneen kovalevyn rikkoutuminen ei aiheuta tietojen menetystä.
- Riittävän pitkien salasanojen käytöstä samoin kuin siitä, ettei käytä samaa salasanaa useammassa palvelussa ja että vaihtaa ne aika ajoin.
- Ettei avaa epäilyttäviä sähköpostiliitteitä tai klikkaa odottamattomasti tulleiden sähköpostiviestien sisältämiä linkkejä.
- Ettei yhdistä omiin tietokoneisiin tai mobiililaitteisiin tuntemattomia laitteita tai tuntemattomia / muiden käytössä olleita muistitikkuja.
- Älylaitteiden tietoturvasta, jottei laitteilta vuoda tietoja ulkopuolisille tahoille.

[157] Tunnistusvälineiden osalta Ponka 2013, s. 410–411.

- Ettei jaa tietoja eteenpäin tahoille, joille ne eivät kuulu. Erityisesti on syytä huomioida sosiaalisen median keskustelut, jotka eivät ole niin yksityisiä kuin miltä vaikuttavat.
- Ohjelmistopäivitysten asentamisesta.
- Ettei joudu sähköposti- tai verkkoalustahuijausten uhriksi. Tällöin voi mm. soveltaa ajatusta siitä, ettei liian hyvältä kuulostava asia tai yllättävä voitto ole kuin huijaus.
- Terveen järjen ja kriittisyyden käytöstä tietoverkkoympäristössä.[158]

Yhtä lailla myös Suomen valtio tuottaa ohjeistusta (kuten alaviitteissä 44 ja 45 mainitut viranomaistahojen julkaisemat oppaat, VAHTI-ohjeet[159] ja kyberturvallisuusviikon[160] video- ym. materiaalit) siitä, miten ihmisen pitää digitaalisessa toimintaympäristössä toimia pitääkseen yllä itsensä ja muiden kyberturvallisuutta. Ohjeilla tuotetaan yhteiskunnallista normistoa ja määritetään, millainen on ”kyberosaava” kansalainen. Huolellisuusarviossa osaamista peilataan normaalihuolellisesti toimivaan keskivertokäyttäjään, jota ei kuitenkaan ole olemassakaan.[161]

Voimassa olevasta oikeudesta ei löydy yksiselitteistä vastausta sille, minkälaista digitaalisen tietämyksen ja tietotaidon tasoa yksilöiltä voidaan odottaa, vaan toimintavelvollisuuksien sisältö määräytyy olosuhdekohtaisesti ja käyttäjän huolellisuutta arvioidaan aina tapauskohtaisesti. Toisin sanoen yksilön vastuu on tilannesidonnainen, eli yksilöiltä voidaan edellyttää eri tilanteissa ja olosuhteissa erilaista tietotaidon tasoa.[162] Toisaalta juuri dynaamisuus turvallisuuden tuottamisessa ja siihen liittyvissä velvoitteissa tuo tarpeellista joustavuutta vastuunjakokysymyksiin, koska digitaalinen toimintaympäristö muuttuu koko ajan. Silti artikkelissa käsitellyt oikeustapaukset ilmentävät ajatusta nor-

158 Limnéll ym. 2014, s. 50–52.

159 ”Valtiovarainministeriön asettama Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) kehittää VAHTI-ohjeistusta, joka kattaa kaikki tietoturvallisuuden osa-alueet.” https://vm.fi/julkaisut/vahti (viitattu 15.3.2019).

160 Suomessa vuosittain lokakuussa pidettävä kyberturvallisuusviikko on osa Euroopan kyberturvallisuuskuukautta, ks. https://cybersecuritymonth.eu/ (viitattu 15.3.2019).

161 Ohjeistuksilla ei myöskään ole sääntelyyn nähden samanlaista oikeuslähteen asemaa tarvittavan digitaalisen toimintaympäristön tietotaidon määrittämisessä.

162 Voidaankin esittää, että kaikilla digitaalisen toimintaympäristön toimijoilla on tilannesidonnaista vastuuta kyberturvallisuuden tuottamisessa.

maalihuolellisen käyttäjän ”yleisen tietämyksen” tasosta, eli täysin osaamaton ja ymmärtämätön yksilö ei digitaalisessa toimintaympäristössä saa olla.

Onkin tarpeen käydä laajempaa keskustelua siitä, millaiseksi yksilön vastuu kyberturvallisuuden tuottamisessa muodostuu ja millaiseksi sitä tulisi kehittää. Lisäksi voidaan kysyä, haluammeko digitaalisesta ympäristöstä ihmislähtöisen, kaikille turvallisen mahdollisuuden osallistua yhteiskunnan jäsenenä verkossa ja alustoilla tapahtuviin toimintoihin, vai onko verkko tarkoitettu vain henkilöille, jotka osaavat toimia oikein, eli huolellisille ja rationaalisille, kansalaistaidoilla varustetuille toimijoille. Oikeudellisesti kysymys on järjestelmävastuun ja yksilövastuun välisestä rajanvedosta: Missä määrin järjestelmältä voidaan edellyttää toimivuutta ja luotettavuutta? Entä mikä on järjestelmän tarjoajan vastuu sellaisten edellytysten luomisesta, jotta yksilöt voivat toimia vastuullisesti? Tulisiko alustojen esimerkiksi aktiivisesti tiedottaa uhkista sekä kehittää omia järjestelmiään siten, että vieraalta laitteelta tehtävät ostot edellyttäisivät erillistä vahvistusta? Sen sijaan, että vastuuarvioinnissa painottuisi pelkästään vaadittavan normaalihuolellisen toimijan riskitietouden määrittely, oikeudellisessa harkinnassa tulisi huomioida myös esimerkiksi käyttäytymistieteellisiä näkökohtia.

Lainsäädäntö on yksi keskeisistä keinoista, joilla yhteiskunnan turvallisuutta – luotettavuutta ja ennakoitavuutta – rakennetaan. Digitalisaatio, ja jakamistalouden kehittyminen yhtenä sen ilmenemismuotona, on kuitenkin globaali kehityskulku, joka kunnioittaa kansallisia rajoja tai lainsäädäntöjä verrattain huonosti. Siksi on tarve myös jonkin asteiselle kansainväliselle yhteisymmärrykselle siitä, kuinka ymmärtämätön, tietämätön tai osaamaton ihminen voi vastuutta tai rajoitetulla vastuulla verkossa olla.[163] Ihminen ei ole kyberturvallisuuden heikoin lenkki, vaan lenkki muiden joukossa. Tietyn tietotaidon tasoa on kohtuullista odottaa, mutta kuinka pitkälle menevää yksilön vastuuttaminen voi olla ilman, että luottamus verkkoalustoja kohtaan heikentyy? Meneillään oleva lainsäädännön kehittäminen niin Euroopan unionin

[163] Tämän keskustelun käyminen esimerkiksi Yhdistyneiden kansakuntien alla samalla, kun keskustellaan pääsystä internetiin ihmisoikeutena, ei lienisi pahitteeksi. Ks. Yhdistyneiden kansakuntien yleiskokous (UNGA) 2011 ja 2016.

kuin kansallisella tasolla toivottavasti vastaa selkeästi vastuunjaon kysymyksiin yhteiskunnan turvallisuutta lisäten. Vahvan sähköisen tunnistamisen edellyttäminen verkossa tapahtuvien maksutapahtumien yhteydessä on ainakin askel yksilöturvallisuuden edistämisessä verkkoalustoilla.

LÄHTEET

Aiken, Mary, The Cyber Effect. John Murray Publishers 2016.

Airbnb:n käyttöehdot, Terms of Service for European Users. Saatavissa: https://www.airbnb.fi/terms [viitattu 22.2.2019]

Bourne, Mike, Understanding Security. Palgrave Macmillan 2014.

Chief Executive, 3.3.2017, "Almost 90% of Cyber Attacks are Caused by Human Error or Behavior". Ross Kelly. Saatavissa: https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/ [viitattu 1.3.2019]

CNBC, 21.6.2018 "The biggest cybersecurity risk to US businesses is employee negligence, study says". Carmen Reinicke. Saatavissa: https://www.cnbc.com/2018/06/21/the-biggest-cybersecurity-risk-to-us-businesses-is-employee-negligence-study-says.html [viitattu 1.3.2019]

Cockayne, Daniel G., "Sharing and neoliberal discourse: The economic function of sharing in the digital on-demand economy" Geoforum 77, 2016, pp. 73–82.

COM(2015) 634 final: Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi tietyistä digitaalisen sisällön toimittamista koskeviin sopimuksiin liittyvistä seikoista.

COM(2016) 288 final: Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle: Digitaalisten sisämarkkinoiden verkkoalustat. Euroopan mahdollisuudet ja haasteet.

Computer Business Review, 3.9.2018, "Revealed: Human Error, Not Hackers, to Blame for Vast Majority of Data Breaches". Ed Targett. Saatavissa: https://www.cbronline.com/news/kroll-foi-ico [viitattu 1.3.2019]

Connolly, Regina, "Trust in Commercial and Personal Transactions in the Digital Age". Teoksessa Dutton, William H. (toim.) The Oxford Handbook on Internet Studies. Oxford University Press 2013.

The Conversation, 10.8.2018, ”Hackers cause most data breaches, but accidents by normal people aren't far behind”. Nicholas Patterson. Saatavissa: http://theconversation.com/hackers-cause-most-data-breaches-but-accidents-by-normal-people-arent-far-behind-99684 [viitattu 1.3.2019]

van Dijck, José & Thomas Poell, ”Understanding Social Media Logic”. Media and Communication 1(1), 2013, pp. 2–14.

Dunn Cavelty, Myriam, ”Is Anything Ever New? – Exploring the Specificities of Security and Governance in the Information Age.” Teoksessa Dunn Cavelty, Myriam – Mauer, Victor – Krishna-Hensel, Sai Felicia (toim.) Power and Security in Information Age. Investigating the Role of the State in Cyberspace. Ashgate 2007.

van Eeten, Michel J. G. – Mueller, Milton, ”Where is the governance in Internet governance?” New Media & Society 15(5), 2013, pp. 720–736.

Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö (EUKTS). JOIN(2013) 1 final ja JOIN(2013) 1 final/2. Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A52013JC0001 [viitattu 10.3.2019]

Euroopan unionin verkko- ja tietoturvavirasto (ENISA), Threat Landscape Report 2018. Saatavissa: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 [viitattu 26.2.2019]

European Banking Authority (EBA), Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2, EBA-Op-2019-06, 21 June 2019. Saatavissa: https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf [viitattu 4.7.2019]

Fellow Finance Oyj:n Yleiset käyttöehdot. Saatavissa: https://www.fellowfinance.fi/Yleiset/kayttoehdot [viitattu: 14.3.2019]

Finanssivalvonnan kannanotto FIVA 8/01.02/2019, 24.6.2019, tunnuslukulistat osana asiakkaan vahvaa tunnistamista. Saatavissa: https://www.finanssivalvonta.fi/saantely/kannanotot-ja-tulkinnat/02_2019/ [viitattu 4.7.2019]

FINE:n (Vakuutus- ja rahoitusneuvonta) pankkilautakunnan, PKL ratkaisut:

- PKL 31/10
- PKL 13/11
- PKL 51/11
- PKL 9/12
- PKL 17/12
- PKL 20/12
- PKL 29/12
- PKL 56/12
- PKL 57/12
- PKL 10/13

– PKL 27/14
– PKL 24/16
– PKL 35/16
– PKL 56/16
– FINE-000699
– FINE-003435
– FINE-006255
– FINE-013434
– FINE-014299
– FINE-013245

Fixura Ab Oy:n yleiset ehdot. Voimassa 1.3.2019 alkaen. Saatavissa: https://www.fixura.fi/fi-fi/sijoittaminen/sijoitusehdot/ [viitattu 14.3.2019]

Gcaza, Noluxolo – von Solms, Rossouw – Grobler, Marthie M. – Jansen van Vuuren, "A general morphological analysis: delineating a cyber-security culture" Information & Computer Security 25(3), 2016, pp. 259–278.

Hannula, Paula, Asiantuntijakirjoitus: Isoja muutoksia maksamisen markkinoilla. Kuluttaja-asiamiehen uutiskirje 6/2017. Kilpailu- ja kuluttajavirasto. Saatavissa: http://www.anpdm.com/article/0/40/444350427643415847 71/4661305 [viitattu 2.3.2019]

HE 231/2005 vp: Hallituksen esitys Eduskunnalle viestintämarkkinalain ja eräiden markkinaoikeudellisten asioiden käsittelystä annetun lain muuttamisesta.

HE 153/2006 vp: Hallituksen esitys Eduskunnalle Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen hyväksymisestä, laiksi sen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta sekä laeiksi rikoslain, pakkokeinolain 4 luvun, esitutkintalain 27 ja 28 §:n ja kansainvälisestä oikeusavusta rikosasioissa annetun lain 15 ja 23 §:n muuttamisesta

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

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

HE 232/2014 vp: Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräiksi siihen liittyviksi laeiksi.

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

Helsingin Sanomat, 7.1.2018 "Kanta-palvelussa on tapahtunut rikoskäsittelyynkin johtanutta urkintaa, kun esimerkiksi naapurin terveystietoja on katsottu luvatta – "Tuomioitakin on tullut"". Saatavissa: https://www.hs.fi/kotimaa/art-2000005516158.html [viitattu 11.3.2018]

Helsingin Sanomat, 1.3.2019 ”New York Times: Facebook kehittää omaa kryptovaluuttaa WhatsAppiin. Saatavissa: https://www.hs.fi/talous/art-2000006020187.html [viitattu 14.3.2019]

Hildén, Tuomas – Sainio, Vesa, Vastuu maksukortin oikeudettomasta käytöstä – Ratkaisukäytäntöä pankin ja asiakkaan välisestä vastuunjaosta. FINE Vakuutus- ja rahoitusneuvonta 2017.

Hofmann, Jeanette – Katzenbach, Christian – Gollatz, Kirsten, ”Between coordination and regulation: Finding the governance in Internet governance” New Media & Society 19(9), 2017, pp. 1406–1423.

Iltalehti, 20.2.2018 ”Omakanta-palvelussa oleva tuntematon häiriö estää potilastietojen katselun – ei viitteitä tietomurrosta”. Saatavissa: https://www.iltalehti.fi/kotimaa/a/201802202200758083 [viitattu 11.3.2019]

Ilta-Sanomat, 9.2.2018 ”Prisman nimissä leviää taas Facebook-huijaus – älä edes vieraile sivustolla!”. Saatavissa: https://www.is.fi/digitoday/art-2000005560765.html [viitattu 10.3.2018]

Instagram-palvelun käyttöehdot, 19.4.2018. Saatavissa: https://www.facebook.com/help/instagram/478745558852511 [viitattu 21.3.2019]

ISGM, n/d. Making the Shift to Human-Centered Security. Saatavissa: https://www.ciosummits.com/Online_Assets_Forcepoint_Transcript_-Making_Shift_to_ Human_Centered_Security.pdf [viitattu 1.3.2019].

Ivanova, Olga – Scholtz, Michael, ”How can online marketplaces reduce rating manipulation? A new approach on dynamic aggregation of online ratings.” Decision Support Systems 104, 2017, pp. 64–78.

Kangas, Urpo, Lesken oikeudellinen asema. Oikeusdogmaattinen tutkimus lesken sosiaaliturvan laajuudesta. Suomalaisen Lakimiesyhdistyksen julkaisuja. A-sarja nro 156, Vammala 1982.

Kaspersky Lab official blog, 15.3.2019 ”Instagram accounts hijacked with fake copyright infringement notifications”. Saatavissa: https://www.kaspersky.com/blog/instagram-hijack-new-wave/25997/ [viitattu 21.3.2019]

Keats Citron, Danielle, Hate Crimes in Cyberspace. Harvard University Press 2016.

KKV:n tiedote 12.1.2018, Maksamiseen tulossa uusia vaihtoehtoja. Kilpailu- ja kuluttajavirasto. Saatavissa: https://www.kkv.fi/ajankohtaista/Tiedotteet/2018/12.1.2018-maksamiseen-tulossa-uusia-vaihtoehtoja/ [viitattu: 2.3.2019]

Kodin kyberopas – ohjeita digitaaliseen arkeen. Turvallisuuskomitea 2017. Saatavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2017/04/Kodin_kyberopas_TK_2017_verkkojulkaisu.pdf [viitattu 11.3.2019]

Korkeimman oikeuden ratkaisut:
- KKO 2006:81
- KKO 2016:73
- KKO 2018:71

Korpisaari, Päivi – Pitkänen, Olli – Warma-Lehtinen, Eija, Uusi tietosuojalainsäädäntö. Alma Talent 2018.

Kuluttajavalituslautakunnan ratkaisut:
– *KVL 02/39/2152* (9.9.2003)

Kuluttajariitalautakunnan ratkaisut:
– *KRIL 3923/38/07* (6.4.2009)
– *KRIL 3723/39/08* (14.12.2009)
– *KRIL 651/39/09* (17.12.2010)
– *KRIL 2403/39/10* (15.3.2011)
– *KRIL 1948/39/11* (19.3.2013)
– *KRIL 2563/39/2012* (14.3.2014)
– *KRIL 5651/39/2015* (9.10.2017)

Kuntalehti, 20.12.2019 ”Apulaisoikeuskanslerin päätös pakottaa STM:n pohtimaan Omakantaa – palvelun sulkeminen alle 10-vuotiaiden osalta mahdollinen ratkaisu.” Saatavissa: https://kuntalehti.fi/uutiset/sote/apulaisoikeuskanslerin-paatos-pakottaa-stmn-pohtimaan-omakantaa-palvelun-sulkeminen-alle-10-vuotiaiden-osalta-mahdollinen-ratkaisu/ [viitattu 11.3.2019]

Kyberturvallisuuden sanasto. Sanastokeskus TSK, Turvallisuuskomitean sihteeristö, Viestintäviraston Kyberturvallisuuskeskus, Huoltovarmuuskeskus. Saatavissa: https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/ [viitattu 10.3.2019]

Lewis, Ted G., Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. 2nd edition. John Wiley & Sons 2015.

Li, Zongchao, ”Psychological empowerment on social media: Who are the empowered users?” Public Relations Review 42, 2016, pp. 49-59.

Limnéll, Jarno – Majewski, Klaus – Salminen, Mirva, Kyberturvallisuus. Docendo 2014.

Mattila, Juri – Seppälä, Timo – Lähteenmäki, Ilkka, Kuka vie ja ketä? Pankit alustatalouden ristitulessa. ETLA raportti 84. 14.9.2018. Saatavissa: https://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-84.pdf [viitattu 1.3.2019]

Mueller, Milton, Will the Internet Fragment? Polity Press 2017.

Nordean lehdistötiedote 8.5.2018, Jo miljoona asiakasta käyttää Nordean uusia tunnistautumistapoja – paperinen tunnuslukukortti jää historiaan. Saatavissa: https://www.nordea.com/fi/media/uutiset-ja-lehdistotiedotteet/press-releases/2018/05-08-11h13-jo-miljoona-asiakasta-kayttaa-nordean-uusia-tunnistautumistapoja---paperinen-tunnuslukukortti-jaa-historiaan.html [viitattu: 18.5.2019]

Norros, Olli, Selvitys tunnistamiseen liittyvistä vahingonkorvauskysymyksistä. Viestintäviraston julkaisuja 004/2016 J. Saatavissa: https://

www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Selvitys_tunnistamiseen_liittyvista_vahingonkorvauskysymyksista_004_2016__J.pdf [viitattu: 13.3.2019]

OP.media 1.4.2019, Pelkkä avainlukulista ei pian enää riitä – Mobiiliavain kannattaa aktivoida viimeistään nyt. Saatavissa: https://op.media/talous/raha-ja-arki/pelkka-avainlukulista-ei-pian-enaa-riita-mobiili-avain-kannattaa-aktivoida-viimeistaan-nyt-ce182027022e41e090-fe531c2caaafb7 [viitattu 18.5.2019].

Quigley, Kevin – Jeffrey Roy, "Cyber-Security and Risk Management in an Interoperable World: An Examination of Governmental Action in North America" Social Science Computer Review 30(1), 2012, pp. 82–94.

Peltomäki, Juha – Norppa, Kati, Rikos meni verkkoon. Näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Talentum Media Oy 2015.

Peltonen Anja – Määttä, Kalle, Kuluttajansuojaoikeus. Talentum Media Oy 2015.

Ponka, Ilja, Sähköinen tunnistaminen ja allekirjoitus Suomen velvoiteoikeudessa. Unigrafia Oy 2013.

Päläs, Jenna, Vertaisluotot ja sääntelysokeus. Edilex 2017/21.

Pöysti, Tuomas, Sähköinen identiteetti. Teoksessa Encyclopaedia Iuridica Fennica 7, Oikeuden yleiset tieteet, s. 1112–1116. Suomalainen Lakimiesyhdistys, Helsinki 1999.

Pöysti, Tuomas, Julkisen vallan velvoite edistää sähköisen identiteetin ja verkkoyhteiskunnan infrastruktuurin turvallisuutta. Oikeus 1/2000.

Pöyhönen, Juha, Kohti uutta varallisuusoikeutta. Lakimies 4–5/1997, s. 525–560.

Raijas, Anu & al, Kilpailun ja kuluttajansuojan kysymyksiä datataloudessa. Kilpailu- ja kuluttajaviraston selvityksiä 1/2019.

Renaud, Karen – Flowerday, Stephen – Warkentin, Merrill – Cockshott, Paul – Craig Orgeron, "Is the responsibilization of the cyber security risk reasonable and judicious?" Computers & Security 78, 2018, pp. 198–211.

Riekkinen, Juhana, Sähköiset todisteet rikosprosessissa. Väitöskirja. Alma Talent 2019.

Rosenthal, Bill, 24.7.2018, How to Take a Human-Centered Approach to Cybersecurity. Saatavissa: https://logicaloperations.com/insights/blog/2018/07/24/573/how-to-take-a-human-centered-approach-to-cybersecurity/ [viitattu 1.3.2019].

Rousku, Kimmo, Kyberturvaopas. Tietoturvaa kotona ja työpaikalla. Alma Talent 2014.

Saariketo, Minna, "Neuvotteluja sosiaalisen median arkkitehtuurisesta vallasta. Käyttäjien ja ei-käyttäjien suhtautuminen Facebookiin teknologiavälitteisenä tilana." Media & Viestintä 38(3), 2015, pp. 128–146.

Salminen, Mirva, Refocusing and Redefining Cybersecurity: Individual Security in the Digitalising European High North. Referee-artikkeli. The Yearbook of Polar Law X. Koninklijke Brill Nv 2018.

Schneier, Bruce, 16.2.2012a, ”The Big Idea: Bruce Schneier”, Schneier on Security -blogi. Saatavissa: https://www.schneier.com/essays/archives/2012/02/the_big_idea_bruce_s.html [viitattu 10.3.2019]

Schneier, Bruce, 27.2.2012b, ”High-Tech Cheats in a World of Trust”, Schneier on Security -blogi. Saatavissa: https://www.schneier.com/essays/archives/2012/02/high-tech_cheats_in.html [viitattu 10.3.2019]

Schneier, Bruce, helmikuu 2013a, ”Trust and Society”, Schneier on Security -blogi. Saatavissa: https://www.schneier.com/essays/archives/2013/02/trust_and_society.html [viitattu 10.3.2019]

Schneier, Bruce, 31.7.2013b, ”NSA Secrets Kill Our Trust”, Schneier on Security -blogi. Saatavissa: https://www.schneier.com/essays/archives/2013/07/nsa_secrets_kill_our.html [viitattu 10.3.2019]

Singer, Peter W. – Friedman, Allan, Cybersecurity and Cyberwar. What Everyone Needs to Know. Oxford University Press, 2014.

Slate, 22.1.2016, ”Calling Humans the ”Weakest Link” in Computer Security Is Dangerous and Unhelpful”. Josephine Wolff. Saatavissa: https://slate.com/technology/2016/01/calling-humans-the-weakest-link-in-computer-security-is-dangerous.html [viitattu 1.3.2019]

Smith, Brian G. – Linjuan Men, Rita – Reham Al-Sinan, ”Tweeting Taksim communication power and social media advocacy in the Taksim square protests” Computers in Human Behavior 50, 2015, pp. 499–507.

Soininen, Heidi, Identiteettivarkaus kyberrikoksena – termit ja tunnusmerkistö. Referee-artikkeli. Defensor Legis N:o 1/2017.

Srnicek, Nick, Platform Capitalism. Polity Press 2017.

Suomen kyberturvallisuusstrategia (SKTS). Valtioneuvoston periaatepäätös 24.1.2013. Turvallisuuskomitean sihteeristö. Saatavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf [viitattu 16.1.2018]

Svantesson, Dan Jerker B., Private International Law and the Internet. 3rd edition. Wolters Kluwer 2016.

Telian palveluiden yleiset toimitusehdot kuluttaja-asiakkaille. Saatavissa: https://www.telia.fi/dam/jcr:0df8c8b8-966c-45b3-b7f2-e912f78b8309/YLEISET_TOIMEHDOT_KULUTTAJA.pdf [viitattu: 12.3.2019].

Traficom, Kyberturvallisuuskeskus, Tietoturvan vuosi 2018, julkaistu 5.2.2019. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Vuosikatsaus_2018_tulostettava_sivuttain.pdf [viitattu 7.2.2019]

Tsagourias, Nicholas – Buchan, Russell (toim.), Research Handbook on International Law and Cyberspace. Edward Elgar 2015.

Turun Sanomat, 29.6.2018 ”Jopa 1500 potilaan Omakanta-palveluun väärä diagnoosi Tyksin hoitojakson jälkeen.” Saatavissa: https://www.ts.fi/uutiset/paikalliset/4002194/Jopa+1500+potilaan+Omakantapalveluun+vaara+diagnoosi+Tyksin+hoitojakson+jalkeen [viitattu 11.3.2019]

Turvallisesti netissä, opas lapsille. Traficom, Kyberturvallisuuskeskus. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/turvallisesti-netissa-oppaat-lapsille-ja-vanhemmille [viitattu 11.3.2019]

Turvallisesti netissä, opas vanhemmille. Traficom, Kyberturvallisuuskeskus. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/turvallisesti-netissa-oppaat-lapsille-ja-vanhemmille [viitattu 11.3.2019]

Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI, Tunnistaminen julkishallinnon verkkopalveluissa 12/2006. Valtionvarainministeriö. Edita Prima Oy 2006.

Voutilainen, Tomi, Sähköisen identiteetin käytöstä julkisessa hallinnossa. Referee-artikkeli. Edilex 2008/8.

Wilhelmsson, Thomas, Vakiosopimus ja kohtuuttomat sopimusehdot. Talentum Media Oy 2008.

Wuolijoki, Sakari – Hemmo, Mika, Pankkioikeus. Talentum 2013.

Yhdistyneiden kansakuntien yleiskokous (UNGA). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. A/HRC/17/27. 2011. Saatavissa: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf [viitattu 1.3.2019]

Yhdistyneiden kansakuntien yleiskokous (UNGA). The promotion, protection and enjoyment of human rights on the Internet. A/HRC/32/L.20. 2016. Saatavissa: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf [viitattu 1.3.2019]

YLE, 29.3.2019, ”Kieltääkö EU avainlukulistat? Yle kysyi seitsemästä pankista mitä syyskuussa oikein tapahtuu – kukaan ei tiedä sitä varmasti”. Juha-Matti Mäntylä. Saatavissa: https://yle.fi/uutiset/3-10711540 [viitattu 4.7.2019].

ZDNet, 22.2.2017, ”IT security breaches: Why users shouldn't take all the blame anymore”. Danny Palmer. Saatavissa: https://www.zdnet.com/article/it-security-breaches-why-users-shouldnt-take-all-the-blame-anymore/ [viitattu 1.3.2019]