TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Tsiviilõiguse õppetool

Katri Kitsing

INTERNETIPANGA IDENTIFITSEERIMISVAHENDITE KASUTAMISEL REALISEERUNUD TURVARISKIDEST TEKKIVA VASTUTUSE OLEMUS JA ULATUS

Magistritöö

Juhendaja
dr. iur. Martin Käerdi

TARTU
2015

Sisukord

Sissejuhatus

22. jaanuaril 2010. aastal jõustus muudetud kujul võlaõigusseaduse[1] (VÕS) 40. peatükk, millega muudeti oluliselt seaduse sisemist struktuuri ning täiendati normide sisu. Tõuke selleks andis eelkõige makseasutuste ja e-raha asutuste seaduse (MERAS)[2] vastuvõtmine Riigikogu poolt 2009. aastal, millise peamiseks eesmärgiks oli harmoniseerida Euroopa Parlamendi ja nõukogu direktiiv 2007/64/EÜ makseteenuste osutamise kohta[3] (edaspidi direktiiv 2007/64/EÜ) ning teha teatud muudatusi ka kehtivas e-raha asutuste regulatsioonis. Direktiivi 2007/64/EÜ vastuvõtmise vajaduse tingis asjaolu, et selle eesmärki – ühtse makseteenuse turu loomine – ei oleks liikmesriigid suutnud ise vajalikul tasemel saavutada, kuna see nõudnuks paljude erinevate liikmesriikide õigussüsteemides kehtivate eeskirjade ühtlustamist, mis oli paremini saavutatav ühenduse tasandil.[4] Olulist tööd Euroopa Liidu (EL) tasandil ühenduse õiguse strateegilises korrastamises teeb ka *Acquis Group*[5], kes on välja andnud eraldi kogumiku EL lepinguõiguses kehtivatest üldprintsiipidest.[6]

Nimetatud VÕS-i muudatustega asendati ka makseteenuse lepingu osapoolte vahelist suhet reguleerivaid norme. Asendamise peamiseks eesmärgiks oli ammendavalt reguleerida makseteenuse pakkuja ja makseteenuse kasutaja vastutus. Ehkki peamised vastutust puudutavad põhimõtted jäid võrreldes eelmise regulatsiooniga muutmata, otsustas seadusandja siiski regulatsiooni selguse ja arusaadavuse huvides asendada nimetatud regulatsioon tervikuna, arvestades seejuures ka asjaoluga, et selline regulatsioon saab samaväärselt kehtestatud ka kõigis teistes Euroopa Majanduspiirkonna liikmesriikides.[7] Normide sisulised muudatused seisnevad peamiselt regulatsiooni laiendamises normide pikemalt lahtikirjutamise kujul ning mõisteaparaadi uuendamises. Kui eelmises VÕS-i regulatsioonis reguleeris vastutust peaasjalikult § 745, sätestades maksevahendi väljaja vastutuse, siis alates 22.01.2010.a kehtima hakanud redaktsioonis on kasutusele võetud mõiste makseteenuse pakkuja, kelle vastutus on mitme paragrahvi peale jaotatud – tulenevalt

[1] Võlaõigusseadus. Vastu võetud 26.09.2001. Jõustunud 01.07.2002. RT I 2001, 81, 487.
[2] Makseasutuste ja e-raha asutuste seadus. Vastu võetud 17.12.2009. Jõustunud 22.01.2010. RT I 2010, 2, 3.
[3] Euroopa Parlamendi ja nõukogu direktiiv 2007/64/EÜ, 13. november 2007, makseteenuste kohta siseturul ning direktiivide 97/7/EÜ, 2002/65/EÜ, 2005/60/EÜ ja 2006/48/EÜ muutmise ning direktiivi 97/5/EÜ kehtetuks tunnistamise kohta– ELT L 319, 5/12/2007. Edaspidi allmärkustes: Direktiiv 2007/64/EÜ.
[4] *Ibid*, preambula p 60, lk 9.
[5] Acquis Group. European Research Group on Existing EC Private Law Arvutivõrgus. Kättesaadav: http://www.acquis-group.jura.uni-osnabrueck.de. 13.04.2015.
[6] Nimetatud kogumis on välja toodud ka makseteenuste regulatsiooni puudutavad sätted, mis suuremas osas vastavad makseteenuste direktiivi 2007/64/EÜ sätetele. Vt "Principles of the Existing EC Contract Law (Acquis Principles) – Contract II: General Provisions, Delivery of Goods, Package Travel and Payment Services", edited by the Research Group on the Existing EC Private Law (Acquis Group), Munich 2009: Sellier.
[7] Seletuskiri makseasutuste ja e-raha asutuste seaduse eelnõu juurde. Arvutivõrgus. Kättesaadav: http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=2f4e7aa2-6a42-2e32-4295-c1ca7778230f&. 13.04.2015. Edaspidi allmärkustes: Seletuskiri.

sellest, kas tegemist on kordumatu tunnuse alusel tehtava maksetehinguga (§ 733^1), autoriseerimata maksega (§ 733^2) või täitmata ja valesti täidetud maksega (§ 733^3). Samuti on §-s 733^8 toodud uuendusena ka maksja vastutus seoses autoriseerimata maksetega.

Käesoleva magistritöö eesmärgiks on anda võrdlev-õiguslik hinnang makseteenuse lepingutes tekkivat vastutust reguleeriva regulatsiooni uuendustele, regulatsiooni võimalikule preventiivsele toimele ning poolte huvide kaitsele või selle puudumisele kehtivas regulatsioonis. Samuti on töö suunatud parandusettepanekute tegemisele seal, kus kehtiv regulatsioon on ilmselt puudulik või ebaselge ning eesmärgiks on koondada ühte töösse antud valdkonda puudutav olulisem materjal ja kirjandus. Töö uurimiseesmärgiks on analüüsida, kas 2010. aastal võlaõigusseadusesse sisse viidud muudatused parandasid regulatsiooni ka sisuliselt, ehk kas tegemist polnud mitte üksnes vormiliste muudatustega, aidates seda täiustada ning samuti analüüsida seda, kas uute normide alusel on osapoolte vahel jagunenud vastutuse ulatus õiglane ja poolte huvid piisavalt kaitstud. Analüüsi käigus tahab autor vastata muuhulgas küsimustele, kas makseteenuse lepingute kontekstis saab makseteenuse kasutajat vaadelda lepingusuhte nõrgema osapoolena ning kui saab, siis kas seadusandja arvestanud tema kui nõrgema lepingupoole huvidega vastutuse regulatsiooni sätestamisel.

Käesoleva töö kirjutamise esmaseks hüpoteesiks võtab autor selle, et 22. jaanuaril 2010. aastal jõustunud VÕS-i muudatused olid regulatsiooni kaasajastamise huvides vajalikud ning need tagavad regulatsiooni selguse. Teiseks hüpoteesiks on võetud see, et VÕS-i muudatused on küll kooskõlas direktiivis 2007/64/EÜ sätestatuga, ent sellele vaatamata ei ole siseriikliku õiguse aspektist vaadatuna makseteenuse lepingu poolte huvid kaitstud parimal võimalikul viisil.

Töö eesmärkide täitmiseks on vajalik leida vastus järgmistele probleemküsimustele: 1) milles seisnes VÕS-i muudatustega kaasnev seaduses kasutatava mõisteaparaadi uuendus ning kas nimetatud uuendused aitasid kaasa regulatsiooni kaasajastamisele; 2) millistest asjaoludest sõltub riisiko kandmine osapoolte vahel ning milliselt on reguleeritud maksevahendi kasutaja omavastutuse kohaldamise alused; 3) kas on õigustatud maksevahendi kasutaja omavastutuse piirmäära seadmine summale 150 eurot ning 4) kuidas tuleks makseteenuse osutamise temaatikas sisustada raske hooletuse mõistet kui omavastutuse kohaldamata jätmise alusena. Analüüsi käigus soovib autor muu hulgas vastata küsimusele, kust jookseb kehtivas õiguses piir makseteenuse pakkuja ja maksja vastutuse vahel, kui internetipanga identifitseerimisvahendite kasutamisel on nimetatud turvariskid realiseerunud ning kas see on õigustatud. Eelnimetatud küsimustele vastuseid otsides peatub autor peamiselt riisiko, üldise vastutuse ning omavastutuse teemadel. Sellest tulenevalt tõstatab autor töö vältel iga peatüki

raames ka alaküsimusi, millele vastuseid otsides on võimalik kujundada selge arusaam makseteenuse pakkuja ning maksja omavahelises suhtes kehtivast vastutuse regulatsioonist.

Tänast maailmamajanduse arengut iseloomustab mittesularahaliste maksevahendite, sh internetimaksete märkimisväärne levik.[8] Nii riigisiseste kui ka piiriüleste elektrooniliste maksetega tehtud tehingute arv suureneb nii mahu kui ka väärtuse poolest ning see trend peaks tulevikus veelgi suurenema, arvestades turgude ja elektrooniliste maksete süsteemi tehnoloogilise arenguga.[9] Nimetatud tehingute arvu suurenemise üheks põhjuseks on kindlasti ka pankade-poolne surve, millega soovitakse sularahas majandamise protsent viia võimalikult madalale, tõstmaks seeläbi nende poolt pakutavate teenuste kasutamise sagedust. Kindlasti ei saa aga jätta märkimata, et internetipanganduse kasutamise suur tõus on osaliselt tingitud ka selle mugavusest – inimesed saavad makseid sooritada sõltumata ajast ja nende asukohast.[10] Kuna sularahas arveldamine ning pangakontoris sularahatehingute tegemine muutub järjest kallimaks[11], sooritavad inimesed raha kokkuhoidmiseks üha enam vajalikke toiminguid internetipanga vahendusel. Kuivõrd inimesed pannakse juba täna, tulevikus aga tõenäolise sularahatehingute hinnatõusu tõttu juba märgatavalt enamgi sundolukorda, kus igapäevaste tehingute tegemiseks peavad nad kasutama internetipangandust, on vajalik, et makseteenuse pakkuja ning maksja vaheline lepinguline suhe oleks ka tavatarbijast kasutajale arusaadav. Nimetatud tingimuste täitmise esmaseks eelduseks on aga suhet reguleeriva seaduse selgus, arusaadavus ning vastuolude puudumine.

Käesoleva töö aktuaalsus tuleneb eelnevalt mainitud nõudest, et makseteenuse pakkuja ning maksja vaheline suhe, sh poolte vastutus oleks seaduse tasandil üheselt ning arusaadavalt reguleeritud. Nimetatu oli ka peamiseks põhjuseks, miks 2010. aastal VÕS-i direktiivi 2007/64/EÜ kohaldamiseks muudeti. Kuna internetipanganduse kujul on tegemist kiirelt areneva valdkonnaga, millega puutub kokku enamik inimesi[12], on oluline uurida, kas hetkel kehtiv VÕS-i regulatsioon on efektiivne ning arvestab võrdselt osapoolte huvidega. Kuna

[8] Euroopa Majandus- ja Sotsiaalkomitee arvamus 2009/C 100/04 teemal „Mittesularahaliste maksevahenditega seotud pettuste ja võltsimiste vastane võitlus", lk 1. Arvutivõrgus. Kättesaadav: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:100:0022:0027:ET:PDF. 13.04.2015.
[9] *Ibid,* lk 1.
[10] The Payment System: Payments, Securities and Derivatives, and the Role of the Eurosystem. European Central Bank, p 33. Edaspidi allmärkustes: The Payment System.
[11] Näiteks avaldas Swedbank alates 31.03.2014.a kehtiva hinnakirja, millise kohaselt sularahatehingute hinnatõus pangakontorites on märgatav. Arvutivõrgus. Kättesaadav: https://www.swedbank.ee/static/pdf/private/home/useful/pricelist_changes_est.pdf. 13.04.2015.
[12] Statistikaamet on koostanud 2012. aasta I kvartalis interneti kasutamise kohta aruande, millise kohaselt oli sel perioodil Eestis 16-74 aastaste seas internetikasutajaid 78%, kellest omakorda kasutab internetipangandust 87%. Ka teistes vanuserühmades esines nii interneti kui internetipanganduse kasutajaid, ent seal oli kasutamisaktiivsus madalam. Arvutivõrgus. Kättesaadav: www.stat.ee/dokumendid/68622. 13.04.2015.

tegemist on paljusid inimesi igapäevaselt puudutava küsimusega, on asjakohane kirjutada võrdlevõiguslik töö, milles oleks analüüsitud kehtiva regulatsiooni efektiivsust.

Võib küsida, et miks on internetipanga kasutamise puhul üldse oluline just selle kasutamisele eelnev identifitseerimisprotsess? See on oluline, kuna prognoosi kohaselt kasvas interneti kaudu ostjate arv 141 miljonilt 2009. aastal 190 miljonile 2014. aastal.[13] EL-i e-kaubanduse turg peaks kuni 2016. aastani kasvama aastas eeldatavasti umbes 10 % ning keskmised kulutused inimese kohta kasvasid EL-i tasandil prognoosi kohaselt 483 eurolt 2009. aastal 601 eurole 2014. aastal.[14] See tähendab aga seda, et interneti vahendusel sooritatud ostud tehakse reeglina internetipanga vahendusel, mis omakorda eeldab aga identifitseerimisvahendite kasutamist. Kuna internet võimaldab oma pakutavaid hüvesid tarbida ajast ning kohast sõltumata, on oluline hinnata, milline on riskide kandmise riisiko makseteenuse pakkuja ja kasutaja omavahelises lepingulises suhtes, milles seisneb kasutaja omavastutuse piirmäär ning millistel juhtudel on tegemist raske hooletusega, millise korral omavastutuse piirmäär kohaldamisele ei kuulu.

Töö teema aktuaalsus tuleneb ka asjaolust, et nimetatud teemal ei ole Eesti õiguskirjanduses väga palju kirjutatud. Osaliselt on VÕS-s jõustunud muudatusi oma 2012. aasta magistritöös kajastanud Raido Rink, kirjutades töö teemal "Autoriseerimata maksetehing elektroonilise maksevahendiga". Nimetatud tööd võib pidada eelkõige 2005. aastal Juridicas ilmunud Tõnu Runneli artikli "Elektroonilise maksevahendi abil omaja tahteta tehtud tehing" [15] edasiarenduseks. Ent nagu pealkirjast ka tuleneb, on R. Rink keskendunud peamiselt autoriseerimata maksetehingute kajastamisele, mis erineb käesoleva töö eesmärgist peatuda internetipangandusel ja selle kasutamisega seonduval vastutusel. Samuti on käesoleva töö lisaväärtusteks teised allikmaterjalid – Raido Rink'i töö põhineb peamiselt saksakeelsel võõrkirjandusel, kuid käesoleva töö autor on teemale lähenenud direktiivi põhiselt ning ingliskeelset kirjandust kasutades, avades seejuures ka elektroonilise maksevahendi mõiste ja olemuse, mis eelnimetatud töös puudub.

Töö kirjutamisel on kasutatud andmekogumis-, interpreteerimise, ajaloolist, analüütilist ning võrdlevaid meetodeid. Teema paikapanemisel ning vajaliku materjali kogumisel lähtus autor andmekogumis- ning ajaloolisest meetodist, koondades kokku asjakohased materjalid ning

[13] Roheline raamat: Euroopa integreerituma kaardi-, interneti- ja mobiilimaksete turu saavutamine. Brüssel, 11.1.2012. KOM (2011) 941 lõplik, lk 4. Arvutivõrgus. Kättesaadav: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0941:FIN:ET:PDF. 13.04.2015. Edaspidi allmärkustes: Roheline raamat.
[14] *Ibid.*
[15] T. Runnel. Elektroonilise maksevahendi abil omaja tahteta tehtud tehing. Juridica VI, 2005. Edaspidi allmärkustes: T. Runnel.

valides neist olulisemad, arvestades seejuures elektrooniliste maksevahenditega seotud vastutuse kui õigusliku institutsiooni arenguid erinevatel perioodidel. Kirjutamisel olid kesksel kohal VÕS-i redaktsioonid ning võlaõigusseaduse kommenteeritud väljaanded, samuti direktiivi 2007/64/EÜ kohta käivad materjalid, sealhulgas ka seletuskiri makseasutuste ja e-raha asutuste seaduse eelnõu juurde, mis käsitles direktiivi harmoneerimist Eesti õigusesse. Kahetsusväärselt leidub töö teema kohta väga minimaalselt kirjastatud kujul materjali, mistõttu on peamiste allikatena töötatud läbi erinevatest andmebaasidest pärit ning õigusteadlaste poolt kirjutatud teemakohased artiklid ja veebilehed. Kuivõrd magistritöö teema ei ole Eesti kohtupraktikas suures mahus käsitlemist leidnud, toob autor käesolevas töös välja kõik Eesti kohtute olulisemad seisukohad. Interpreteerimise meetodit kasutades mõtestas autor enda jaoks lahti asjakohaste materjalide läbitöötamisel saadud tulemused, kujundades seeläbi magistritöös käsitlemist leidvate küsimuste osas enda seisukoha. Analüütiline meetod leidis kasutust sedavõrd, et magistritöös on teemasid käsitletud stiilis üldiselt üksikule. Võrdleva meetodi aspektist on töös võrreldud Eesti ning Ühendkuningriikide regulatsioone, hinnates viimase poolt direktiivi 2007/64/EÜ rakendamist vastutuse osas ning selle eeskujuks olemise võimalust Eesti seadusandlusele.

Magistritöö on jaotatud kolmeks peatükiks. Esimeses peatükis käsitleb autor elektroonilise maksevahendi mõistet, tuues töö ülevaatlikkuse huvides välja maksevahendi mõiste ja olemuse ning kasutamisvõimalused. Teema kompaktsuse huvides on lühidalt analüüsitud ka teisi maksevahendeid, ent peatükk on siiski üles ehitatud selliselt, et oleks mõistetav internetipanga identifitseerimisvahendi kui maksevahendi erinevus teistest elektroonilistest maksevahenditest. Samal eesmärgil on ka alapeatükis 1.2 toodud välja maksekaardi tüüpi maksevahendid ja nende olemus, mida õiguslikult küll maksevahenditena ei kvalifitseerita, ent mis olemuselt maksevahenditele siiski korrespondeeruvad.

Töö teine peatükk keskendub riskide analüüsimisele, mis tõusetuvad identifitseerimisvahendite kasutamisest. Autor toob välja peamised riskid, mis on identifitseerimisvahendite kasutamisele iseloomulikud, ning hindab nendega seotud vastutuse jagunemist osapoolte vahel. Samuti on analüüsitud makseteenuse kasutajal tekkivat omavastutuse olemust, milline on seaduse tasandil maksimaalse summalise piirmääraga paika pandud. Omavastutuse kohaldamata jätmise alustele keskendub autor töö kolmandas peatükis.

Kolmandas peatükis tõstatab autor küsimuse sellest, millistel juhtudel ning tingimustel on õigustatud jätta makseteenuse kasutaja omavastutus kohaldamata ning panna ta vastutama kogu tekkinud kahju ulatuses. Kuivõrd makseteenuse osutamise temaatikas on teenuse kasutaja peamisteks kohustusteks teatamis- ja hoolsuskohustus, analüüsib autor nende

kohustuste täitmata jätmise õiguslikke tagajärgi ning hindab, millised on tagajärjed siis, kui makseteenuse kasutaja rikub raskelt mõnda muud endal lasuvat kohustust, näiteks ei hoia hoolikalt internetipanga identifitseerimisvahendeid. Samuti võtab autor seisukoha küsimuses, millal saab makseteenuse kasutaja poolt rikutud kohustust kvalifitseerida raske hooletuse alla ning millal on tegemist kerge hooletuse tõttu tekkinud tagajärjega.

1. Internetipangas kasutatav identifitseerimisvahend kui elektrooniline maksevahend

1.1 Elektroonilise maksevahendi mõiste ja olemus

2009. aastal võeti uue seadusena vastu MERAS, mille peamiseks eesmärgiks oli harmoniseerida direktiiv 2007/64/EÜ makseteenuste osutamise kohta. Nimetatud direktiivi kujul ei ole küll tegemist täiesti uue regulatsiooniga EL tasandil, kuivõrd see tugineb suuremas osas Euroopa Komisjoni soovituses nr 97/489/EÜ[16] toodud põhimõtetele, ent kuni direktiivi vastuvõtmiseni puudus EL tasandil ühtne siduv õigusakt, mis makseteenuste temaatikat reguleeriks. Kuivõrd makseteenuse regulatsioon, eelkõige makseteenuste sisu tarbijakaitseline aspekt oli osaliselt reguleeritud VÕS-s, tuli samal ajal ka VÕS-i viia sisse mitmeid muudatusi, et siseriiklik õiguskord vastaks EL normidele. Nimetatud muudatustega, mis jõustusid VÕS-s 2010. aastal, korraldati suures ulatuses ringi ka elektroonilist maksevahendit puudutavad sätted.

Maksevahendi definitsioon oli ja on ka jätkuvalt defineeritud VÕS-s. Erinevus seisneb aga selles, et kui enne 20. jaanuari 2010. aasta kehtinud VÕS-i redaktsioonis tehti elektroonilise maksevahendi puhul vahet selle alaliikidel, milleks olid kaugjuurdepääsuga maksevahend ning e-raha, siis kehtiva seaduse redaktsioonis on nimetatud erisused kaotatud. Nimelt sätestab kehtiv VÕS § 709 lg 8 maksevahendi legaaldefinitsiooni[17] – maksevahend on makseteenuse pakkuja ja tema kliendi vahel kokkulepitud isikustatud seade või ka toimingute kogum, mida makseteenuse pakkuja klient kasutab maksejuhise algatamiseks. Nimetatud mõistet on sarnaselt käsitlenud ka Euroopa Keskpank, defineerides maksevahendi identifitseerimise ning makse teostamise vahendina.[18] VÕS-i muudatustega kaasnenud maksevahendi mõiste korrigeerimine on eelkõige põhjendatud seetõttu, et elektrooniliste maksevõimaluste kiiret arengut ning kasvutendentsi silmas pidades ei saa legaaldefinitsioon koosneda jäigast sõnastusest, mis ajale peagi jalgu jääks ning pidevat muutmist vajaks. Ehkki VÕS-i kommenteeritud väljaande kohaselt[19] kuulusid ka varasema seaduse regulatsiooni kohaldamisalasse nii füüsilist vormi omavad elektroonilised maksevahendid kui ka füüsilise

[16] Euroopa Komisjoni soovitus nr 97/489/EÜ. Arvutivõrgus. Kättesaadav: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1396256154001&uri=CELEX:31997H0489. 13.04.2015. Edaspidi allmärkustes: Komisjoni soovitus.

[17] Seadus on ühtse legaaldefinitsiooni alla koondanud nii maksevahendi, makseinstrumendi kui makseviisi.

[18] *The Payment System*, *opt.cit.,* p 25. Samuti on Euroopa Keskpank täpsustanud antud mõistet ka oma kodulehel, defineerides maksevahendit kui seadet või toimingute kogumit, mis võimaldab kanda rahalisi vahendeid maksjalt makse saajale. Kättesaadav: European Central Bank, *Payments and Markets Glossary*. Available at http://www.ecb.eu/home/glossary/html/glossp.en.html. 13.04.2015.

[19] A. Hinrikus. VÕS § 734/p 3.1. – P. Varul jt (koost). Võlaõigusseadus III. 8. ja 10. osa (§§ 619-916 ja 1005-1067). Komm vlj. Tallinn: Juura 2009, lk 238. Edaspidi allmärkustes: VÕS III komm.

vorminguta kokkulepitud protseduuride kogumid (sh internetipanga tehnilised ja õiguslikud tingimused), on autori hinnangul seaduse tasandil ühtse, kõiki maksevahendeid hõlmava mõiste defineerimine ökonoomsem lahendus. Varasem regulatsioon nägi ette elektroonilise maksevahendi mõiste (VÕS § 734) ning sätestas eraldi veel kaugjuurdepääsuga maksevahendi (VÕS § 735) ning e-raha[20] mõisted. Taolise mõistete eristamise jätkamine võib aga pikemas perspektiivis tuua kaasa olukordi, kus ühel hetkel teatud maksevahendid eelnimetatud mõistete alla ei mahu ning tekib küsimus, kas seda vahendit saab üldse maksevahendina käsitleda, sest ehkki ta olemuslikult maksevahendile vastab, ei ole ta seaduse normiga hõlmatud. Seetõttu leiab autor, et direktiivi 2007/64/EÜ eeskujul ühtse mõisteaparaadi sisseviimine ka siseriiklikku õigusesse oli õigusselguse huvides mõistlik lahendus.

Võttes siseriiklikkusse õigusesse direktiivi 2007/64/EÜ eeskujul üle eelnimetatud avarama maksevahendi mõiste, mille alla kuuluvad erinevad maksevahendid nende alaliigitustest sõltumata, on seadusandja seejuures tunnustanud ka Riigikohtu poolt 13. oktoobril 2005. aastal väljaöeldud seisukohta.[21] Nimetatud lahendis leidis Riigikohus, et maksevahendite mõistet reguleerivate sätete eesmärgiks tuleb pidada seda, et seadusliku regulatsiooniga oleksid hõlmatud kõik käibes kasutatavad elektroonilised maksevahendid sõltumata nende nimetustest ning reguleeritud oleks maksevahendite väljajate ning omajate õigused ja kohustused. Riigikohtu poolt antud tõlgenduse kohaselt ei kohaldata seega elektroonilise maksevahendi regulatsiooni mitte ainult pangakontol olevate vahendite käsutamist võimaldavatele maksevahenditele, vaid seda tuleb kohaldada palju laiemalt ka kaupade ja teenuste käsutamist võimaldavatele elektroonilistele vahenditele.[22]

Kuigi VÕS-st on kaotatud elektroonilise maksevahendi legaaldefinitsioon *per se*, ei tähenda see nimetatud mõiste kadumist Eesti õiguskorrast. 2010. aastal muudetud kujul jõustunud VÕS-ga võttis seadusandja endale üksnes Eesti õiguse kooskõlastamisest EL õigusega palju suurema eesmärgi. VÕS-i ümberkujundamisega loodeti parandada ka seni kehtinud seaduse struktuuri ning mõisteaparaati, mis peagi ajale jalgu ei jääks. Kuivõrd maksevahendite turg on pidevalt arenev, millel autor peatub pikemalt töö alapeatükis 1.2, tuleb maksevahendite mõiste alla koondada ka sellised maksmist võimaldavad vahendid, mis ei pruugi olla

[20] Enne 2010. aastal jõustunud VÕS-i muudatusi ning MERAS-e vastuvõtmist sätestas e-raha mõiste e-raha asutuste seadus, millise § 3 lg 1 kohaselt oli e-raha elektrooniline maksevahend, mis vastab kõikidele järgmistele tunnustele: 1) e-raha salvestatakse elektroonilisele seadmele, milleks võib olla kaart, arvuti mälu või muu kliendi jaoks rahaühikute elektroonilist salvestamist võimaldav vahend (edaspidi e-raha seade); 2) e-raha väljastamisel ei või e-raha seadmele salvestatud summa olla suurem selle vastu antud rahasummast; 3) e-raha aktsepteerib maksevahendina lisaks seda väljastavale e-raha asutusele või krediidiasutusele vähemalt üks ettevõtja, kellel on e-raha kasutamisel maksevahendina e-raha asutuse kliendiga otsene võlasuhe.
[21] RKTKo 3-2-1-92-05, p 14.
[22] A. Hinrikus. VÕS III komm, *opt.cit.*, § 734/p 3.1.

elektroonnsed. Seega kujutades endast olemuslikult isikustatud seadet või toimingute kogumit, kuulub ka varem kehtinud VÕS-s kasutusel olnud elektroonilise maksevahendi mõiste kehtiva VÕS § 709 lg-s 8 toodud definitsiooni alla. Internetipanganduse puhul saab aga elektroonilist maksevahendit vaadelda kui osapoolte vahel kokkulepitud protseduuride kogumit, hõlmates endas nii tehnilisi kui õiguslikke tingimusi.[23] Seega kuuluvad ka internetipanka sisselogimiseks vajalikud personaalsed identifitseerimisvahendid maksevahendite hulka.

Kuivõrd internetipanganduse kasutamistrend on inimeste seas viimaste aastate jooksul kõvasti tõusnud ning kindlasti jätkub tõus ka edaspidi, on pankade esmaseks huviks konkurentsieelise saavutamise eesmärgil pakkuda tarbijatele turvalisi ning mugavaid internetipanka sisselogimise viise.

Hetke seisuga pakuvad kõik Eesti suuremad pangad[24] internetipanka sisselogimise viisideks paroolikaarte, ID-kaardiga ning mobiil-ID-ga sisenemise võimalusi. Lisaks eelnimetatutele pakub Swedbank[25] lisavõimalusena ka PIN-kalkulaatori kaudu sisenemist. Danske Bank'i ning Nordea panga puhul tuleb seoses paroolikaartidega välja tuua aga järgnev erinevus. Kui SEB ning Swedbank kasutavad jätkuvalt korduskasutusega paroolikaarte, siis 2010. aastal alustas Danske Bank esimese pangana Eestis taoliste paroolikaartide järk-järgulise kaotamisega. Nimelt lähtus pank seejuures turvalisuse kaalutlustest – kuivõrd korduskasutusega paroolikaardid on isikutuvastusvõimalustest kõige vähem turvalisemad[26], soovis pank nende kasutamisest loobuda ning asendada need unikaalsete ning kordumatute paroolikaartidega.[27] Seega on isikutel endiselt võimalus end Danske Bank'i internetikeskkonnas paroolikaartidega identifitseerida, kuid vahe SEB ning Swedbank'i poolt pakutavaga seisneb selles, et paroolikaartidel toodud koodid on unikaalsed ning kui isik on ära kasutanud kõik kaardil olevad paroolid, kaotab kaart oma kehtivuse ja isikule väljastatakse uus unikaalne paroolikaart. Tänaseks on samasuguse süsteemi võtnud kasutusele Nordea pank, mille paroolikaartidel on 120 koodi ning kui paroolikaardi kasutaja on ära kasutanud 90. koodi sellelt kaardilt, saadetakse talle posti teel uute koodidega kaart, mis soovitatakse turvalisuse kaalutlustest tulenevalt koheselt kasutusele võtta.[28]

---

[23] A. Hinrikus. VÕS III komm, *opt.cit.*, § 734/p 3.1.
[24] Arvesse on võetud pankade turuosalusi ning populaarsust Eesti turul – Swedbank, SEB, Nordea Pank Eesti ning Danske Bank.
[25] Swedbank. Koduleht. Arvutivõrgus. Kättesaadav: www.swedbank.ee. 13.04.2015.
[26] I-G. Linkgreim. Eestlased ei raatsi panga paroolikaartidest loobuda. Arvutivõrgus. Kättesaadav: http://uudised.err.ee/v/majandus/14b8cbb6-f1cb-4902-ade4-1c958ae1a72a. 13.04.2015.
[27] H. Roonemaa. Koodikaartide kaotamist alustab Eestis Sampo pank. http://epl.delfi.ee/news/eesti/koodikaartide-kaotamist-alustab-eestis-sampo-pank.d?id=51274617. 13.04.2015.
[28] Nordea. Koduleht. Arvutivõrgus. Kättesaadav: www.nordea.ee. 13.04.2015.

Kuna üldistatult öeldes on valikus 4 erinevat internetipanka sisenemise võimalust, peaks igal inimesel olema võimalus valida just temale mugavaim ja kõige turvalisem variant internetipanka sisenemiseks.

Siiski ei takista juba väljakujunenud ja inimestele mugavaks muutunud identifitseerimisvahendite kasutamine uute võimaluste leiutamist teadlaste poolt. Kasutades ära tehnoloogia pidevat arengut, on välja töötatud mitmeid uusi maksealgatamis- ning isiku identifitseerimise meetmeid, kasutades selleks internetti, mobiilvõrke või teisi informatsiooni ning kommunikatsiooni tehnoloogiaid.[29] Näiteks 30. oktoobril 2008. aastal avalikustas Euroopa *smart card*'ide [30] müüja Gemalto ultraõhukese, krediitkaardi suuruse identifitseerimisseadme internetipanganduse kasutajatele, mis võimaldab neil luua ühekordseid paroole, kasutades selleks isikute enda pangakaarti ning paroole.[31] Kuigi ka Eestis kasutatav PIN-kalkulaator toimib samal põhimõttel, seisneb kahe seadeldise erinevus selles, et *smart card*'i kasutamiseks peab kasutajal olema füüsiliselt olemas ka pangakaart, mille alusel parasjagu soovitakse internetipanka siseneda. See muudab seadeldise kasutamise võrreldes PIN-kalkulaatoritega veelgi turvalisemaks, kuna üksnes paroolide teadmisega ei ole võimalik internetikeskkonda siseneda. Nimetatud *smart card*'i kujul on tegemist küll identifitseerimisvahendiga, mida Eesti pangad ühe võimalusena isiku identifitseerimiseks käesoleval hetkel ei paku, ent sellele vaatamata pole tegemist täiesti innovaatilise lahendusega Eesti turu jaoks. Nimelt nagu autor eelnevalt välja tõi, on Eesti pankade poolt võetud kasutusele PIN-kalkulaatorid, mis põhinevad samuti põhimõttel, et genereerivad igakordselt selle kasutajale uue unikaalse koodi isiku identifitseerimiseks, ent erisusena *smart card*'dest ei nõua PIN-kalkulaatorid maksevahendi füüsilist olemasolu. Teisalt on aga Eestis kasutusel ID-kaardi põhine identifitseerimine, mis pole jällegi mujal maailmas väga levinud. Ka ID-kaardi abil isiku identifitseerimist võib sarnaselt *smart card*'i kasutamisele pidada üheks turvalisemaks identifitseerimisvõimaluseks, kuivõrd see eeldab samuti maksevahendi füüsilist kasutamist identifitseerimisprotsessis – see välistab võimaluse kasutada maksevahendile salvestatud andmeid ilma seda füüsiliselt omamata. Nagu autor põhjalikumalt käesoleva töö alapeatükis 1.2 käsitleb, eeldab ka mobiilimaksete teostamine sarnaselt ID-kaardile maksevahendi füüsilist olemasolu.

[29] *The Payment System*, *opt.cit.*, p 33.
[30] *Smart card* on välimuselt ning suuruselt krediitkaardi tüüpi kaart, mis erineb viimasest oma sisu poolest – kui krediitkaart on tavaline plastikkaart kiibiga, siis *smart card* koosneb sisseehitatud mikroprotsessorist. Allikas: http://computer.howstuffworks.com/question332.htm. 13.04.2015.
[31] Finextra. *Gemalto releases mini online banking authentication device, News Release, October 30, 2008*. Available at http://www.finextra.com/news/fullstory.aspx?newsitemid=19204 . 13.04.2015.

Uute tehnoloogiate väljatöötamine on eelkõige õigustatud sellest aspektist, et tänasel päeval äärmiselt populaarseid identifitseerimisvahendeid on hakatud pidama üsnagi ebaturvaliseks. Ehkki erinevate pankade kinnitusel peetakse paroolikaartide kaudu enda identifitseerimist internetikeskkonnas kõige ebaturvalisemaks, kasutavad enamik inimesi just nimetatud võimalust panka sisselogimisel.[32] Paroolikaartide ebaturvalisuse võib ennekõike välja tuua selles, et nendel olevat infot on kerge kopeerida ning edaspidi kasutada ka paroolikaarti kui identifitseerimisvahendit füüsiliselt omamata. Selline kopeerimine võib seega toimuda ka selliselt, et maksevahendi omaja ei pruugi isegi olla teadlik sellest, et tema paroole on kopeeritud ning et on tekkinud oht, et keegi neid pahatahtlike kavatsustega kasutada püüab. Taolises olukorras sõltub maksekaardi omaja enda vastutuse küsimus paljuski selles, kes kannab maksevahendi kaotamise või kopeerimise korral riisikot ning millises ulatuses peab kaardi omaja ise vastutama. Teised identifitseerimisvõimalused – mobiil-ID ning ID-kaardi abil identifitseerimine – eeldavad siiski seda, et isik, kes soovib internetipanka siseneda, peab identifitseerimisvahendit reaalset ka füüsiliselt omama, et oleks võimalik identifitseerimisprotsess lõpule viia. Kuna aga pangad peavad ka ise paroolikaarte kõige ebaturvalisemaks identifitseerimisvahendiks ja samas on nende maine hoidmiseks äärmiselt oluline, et teenuse kasutajad hindaksid teenuse pakkujapoolseid pingutusi turvalisuse saavutamisel, võiksid teenuse pakkujad ka ise mõelda lihtsasti rakendatavatele võimalustele, kuidas ennetada koodikaartidega kaasnevaid turvariske. Nimelt saab autori isikliku kogemuse pinnalt tuua näite, kus ta on olnud praeguse Swedbank'i, endise Hansapanga klient juba üle 15 aasta ning alates 2004. aastast ka internetipanga kasutaja. 2004. aastal autorile väljastatud paroolikaart internetipanka sisselogimiseks on aga siiani kehtiv – ehkki pank on vahepeal nime muutnud ning möödunud on üle kümne aasta, ei pea makseteenuse pakkuja sellele vaatamata oluliseks vahetada välja kliendile üle 10 aasta tagasi väljastatud paroolikaart. Taoline vahetamisvõimalus on küll olemas, ent see eeldab kliendi enese initsiatiivi. Panga poolt on küll turvalisuse huvides ette nähtud ka makseteenuse kasutaja kohustus regulaarselt vahetada muutuvparoolide kaarti pangakontoris[33], ent nimetatud kohustusega seonduvad mõned probleemkohad. Nimelt ei ole Swedbank nimetatud kohustuse täitmiseks rakendanud ühtegi sunnivahendit, samuti puudub igasugune makseteenuse pakkujapoolne kontroll ning meeldetuletus osas, kas maksevahendi omajad on regulaarselt oma paroole vahetanud. Samuti on küsimus selles, kas sellise regulaarse vahetamiskohustuse ettenägemisel on ikka õigustatud teenuse pakkuja poolt teenustasu küsimise võimalus ning selles, mida on silmas peetud

[32] I-G. Linkgreim. Eestlased ei raatsi panga paroolikaartidest loobuda. Arvutivõrgus. Kättesaadav: http://uudised.err.ee/v/majandus/14b8cbb6-f1cb-4902-ade4-1c958ae1a72a. 13.04.2015.

[33] Swedbank. Teleteenuste lepingu tingimused, p 7.6. Arvutivõrgus. Kättesaadav: https://www.swedbank.ee/static/pdf/private/home/useful/cond_teleservices_2012_12_01_est.pdf. 13.04.2015. Edaspidi allmärkustes: Swedbank'i lepingu tingimused.

“regulaarse vahetamiskohustuse” all. Kuivõrd mõiste “regulaarse” puhul on tegemist sisustamata õigusmõistega, ei pruugi osapooled antud definitsiooni sisu osas ühisel arvamusel olla. Autorile jäävad siinkohal mõistmatuks makseteenuse pakkujate motiivid sellise tegutsemismustri puhul, sest kuigivõrd paroolikaarte võib tõepoolest üheks kõige ebaturvalisemaks identifitseerimisvahendiks pidada, kasutavad üle poole kõigist internetipanga kasutajatest identifitseerimisvahendina just koodikaarti.[34]

Teema kompaktse käsitluse huvides on siinkohal oluline avada ka maksejuhise mõiste.

Olemuslikult seisneb maksevahendi kasutamine makseteenuse lepingu raames maksejuhiste andmises vahendi kasutaja poolt ja selle tulemusena tekkiva maksekäsundi täitmises. Direktiivi 2007/64/EÜ eestikeelses tõlkes defineeritakse artikkel 4 lg-s 16 maksekäsundit kui makseteenuse pakkujale maksja või saaja poolt antud juhist maksetehingu täitmiseks. Seletuskirjas makseasutuste ja e-raha asutuste seaduse eelnõu juurde on aga toodud, et maksekäsund väljendab kolmnurksuhet käsundaja, käsundisaaja ja soodustatud isiku vahel, ent direktiivi eesmärk ei ole mitte reguleerida nimetatud kolmnurksuhet, vaid selle reguleerimise esemeks on teatud tunnustele vastav konkreetne teenuse leping ning selle alusel antavad täitekorraldused.[35] Seega on asutud seisukohale, et direktiivi eestikeelses tõlkes kasutatud maksekäsundi mõistet on kasutatud vääras kontekstis – maksekäsundi asemel peaks olema kasutatud lepingukohase maksejuhise ehk ülekandejuhise (ingl.k *payment order*) mõistet. Ehkki selle tõttu tekib direktiivi eestikeelse tõlke ning VÕS-s sätestatud mõistete vahel teatud ebakõla, on oluline siiski lähtuda direktiivi mõttest, milleks on reguleerida maksejuhise andmist. Ka käesolevas töös on lähtutud direktiivi 2007/64/EÜ mõttest, mitte eestikeelsest tõlkest ning autor loeb direktiivi artiklile 4 lg 16 vastavaks alternatiiviks Eesti õiguses VÕS § 709 lg 7, millise kohaselt on maksejuhis igasugune maksetehingu tegemise korraldus, mille maksja annab makseteenuse pakkujale. Antud definitsioon on avatud ega sätesta piire sellele, millisel viisil võib maksja nimetatud korraldusi anda – see võib toimuda nii vahendatult kui vahendamata, st kas isiklikult või mõne süsteemi kaudu.

Reeglina saab maksejuhise andmisest rääkida eelkõige olukorras, kus makseteenuse pakkuja ning maksja vahel on sõlmitud makseteenuse osutamise leping. Nimetatud lepingu täitmise raames on VÕS § 724^2 lg 1 kohaselt maksejuhis makseteenuse pakkujale siduv hetkest, mil maksja makseteenuse pakkuja selle kätte saab. VÕS § 724^3 lg 4 sätestab, et makseteenuse pakkujal ei ole õigust keelduda autoriseeritud maksejuhise täitmisest, kui maksejuhis vastab

[34] I-G. Linkgreim. Eestlased ei raatsi panga paroolikaartidest loobuda. Arvutivõrgus. Kättesaadav: http://uudised.err.ee/v/majandus/14b8cbb6-f1cb-4902-ade4-1c958ae1a72a. 13.04.2015.
[35] Seletuskiri, *opt.cit.*, lk 22.

makseteenuse lepingus määratud tingimustele ning maksejuhise täitmisega ei rikuta mõnes muus õigusaktis sätestatud kohustust. Seega on makseteenuse pakkuja reeglina kohustatud maksejuhise täitma alates hetkest, mil ta on selle kätte saanud, välja arvatud juhul, kui maksja ei ole end korrektselt autoriseerinud VÕS § 724[1] mõttes.

2010. aastast jõustunud VÕS-i muudatustega on seaduses uue terminina võetud kasutusele autoriseerimise mõiste, mis on otsetõlkena võetud üle makseteenuste direktiivis 2007/64/EÜ kasutatud *authorisation* mõistest. Autoseerimise mõiste on tugevas seoses nõusoleku mõistega – nimelt seisneb VÕS § 724[1] kohaselt autoriseerimine maksetehingu tegemiseks nõusoleku andmises ning selle viisi ja korra määravad pooled omavahelise kokkuleppega. Seega saab maksetehingut lugeda autoriseerituks üksnes juhul, kui maksja on andnud oma nõusoleku maksetehingu täitmiseks. Ehkki selguse huvides viitab autor ka käesolevas töös seaduses kasutatud mõistele autoriseerimine, jääb sellise tõlke kasutamine seadusandja poolt kohati selgusetuks. Kuivõrd sisu poolest tähendab autoriseerimine nõusoleku andmist, oleks võinud viimast mõistet kasutada ka VÕS-i uuenenud mõisteaparaadis. See oleks vähendanud segadust selles osas, et mida tuleb mõista võõrsõna "autoriseerimine" all ning mille poolest ta tavalisest nõusoleku andmisest erineb. Autori hinnangul puudub vajadus nendel kahel mõistel VÕS-i kontekstis vahet teha, kuna tegemist on sünonüümidega. Direktiivi 2007/64/EÜ üheks eesmärgiks tuleb küll pidada liikmesriikide makseteenuste turu ühtlustamist, ent seejuures ei tohi ära unustada liikmesriikide õiguskordade eripärasid ning õigusselguse põhimõtet. Asendades autoriseerimise mõiste keeleliselt korrektsema nõusoleku mõistega, ei läheks seadusandja vastuollu direktiivi 2007/64/EÜ eesmärkidega, ent tagaks seejuures siseriikliku regulatsiooni selguse. Eeltoodust tulenevalt peab autor põhjendamatuks seadusandja poolt vastu võetud mõisteaparaadi uuendamist nimetatud kujul, kuna see tekitab pigem segadust, kui loob õigusselguse.

Internetipanganduse puhul saab autoriseerimisest rääkida eelkõige isiku tuvastamise kontekstis paroolide sisestamise teel – kui isik on end internetipanka sisselogides korrektselt identifitseerinud ning maksejuhist andes sisestanud ka õiged paroolid, on isik end üldjuhul makseteenuse pakkuja silmis autoriseerinud ning viimane peab maksetehingu täitma. Võimalikke erandeid eeltoodud seisukohast käsitleb autor käesoleva töö teistes peatükkides, tuues välja nii makseteenuse pakkuja kui ka kasutaja kohustused maksevahendiga seotud autoriseerimisprotsessis.

Ehkki internetipangas isiku identifitseerimiseks ettenähtud vahendid kuuluvad VÕS § 709 lg 8 mõttes maksevahendi legaaldefinitsiooni alla, tuleb vahet teha maksekaardil ning makse teostamist võimaldaval vahendil. Viimase puhul saabki eelkõige rääkida ülalmainitud

internetipanganduse identifitseerimisvahenditest, kuivõrd nimetatud vahendid tagavad võimaluse pääseda ligi isiku elektroonilisele pangakontole ning teostada makseid, pakkumata seejuures näiteks kohest võimalust tasuda kaupmehe juures tarbitud teenuste eest. Maksekaardi puhul on seevastu tegemist maksevahendiga, millisega isik saab elektroonilise sidevahendi, eelkõige makseterminali kaudu makseid teostada ning seda mugavalt kaupmehe juurest lahkumata. Ehkki eelnimetatud maksevahendid erinevad üksteisest nende rakendamisvõimaluste poolest, on nad sellele vaatamata olemuslikult ning õiguslikult sarnased. Lisaks sellele, et mõlemad maksevahendid eeldavad sidevahendi kasutamist näiteks arvuti või pangaterminali kujul, on ka nende õiguslik kontseptsioon samane – mõlemad võimaldavad edastada makseteenuse pakkujale maksejuhise makse algatamiseks.

Maksekaartidena on käesolevas töös käsitletud eelkõige deebet- ja krediitkaarte. Läbi maksejuhiste andmise saab maksekaardi omaja käsutada oma rahalisi õigusi elektrooniliste vahendite kaudu – eelkõige sooritada makseid kaupade ja teenuste eest tasumiseks.[36]

Ehkki käesolevas alapeatükis toodu viitab sellele, et kasutusel on mitmeid erinevaid maksevahendeid, mis kõik kuuluvad VÕS § 709 lg 8 kohaldamisalasse, ei piirdu tehnoloogia areng üksnes olemasolevate vahenditega. Tehnoloogia on arenev valdkond, kus otsitakse pidevalt uusi võimalusi inimestele suurema kasutusmugavuse ning rohkem turvalisemate võimaluste loomiseks, ning selle poolest ei erine ka maksevahendite valdkond. Järgmises peatükis käsitleb autor maksekaardi erinevusi maksekaardi tüüpi maksevahenditest ehk nendest tehnoloogilisest saavutustest, mis pakuvad tugevat konkurentsi eelmainitud maksekaartidele, ent mida pole siiani veel maksekaardi koondnimetuse alla viidud.

1.2 Elektrooniliste maksevahendite olemuslik erinevus maksekaardi tüüpi maksevahenditest

Nagu eelmises alapeatükis lühidalt mainitud, peavad inimesed reeglina maksekaartide all silmas eelkõige krediit- ja deebetkaarte, mis võimaldavad teatud sidevahendi ehk makseterminali vahendusel tehinguid sooritada. Samas kuuluvad legaaldefinitsiooni alusel ka internetipanga kasutamiseks vajalikud identifitseerimisvahendid elektrooniliste maksevahendite hulka, kuivõrd olemuslikult võimaldavad ka nemad anda raha ülekandmiseks või muu tehingu sooritamiseks maksevahendi kasutajal juhiseid käsundisaajale ehk makseteenuse pakkujale tehingu sooritamiseks.

[36] T. Runnel, *opt.cit.*, lk 367.

Tehnoloogia on aja jooksul pidevalt arenev valdkond, mistõttu on turule ilmunud lisaks traditsioonilistele maksevahenditele ka hulgaliselt alternatiive, mida hetkel kehtiva regulatsiooni kohaselt küll õiguslikult veel maksevahenditena ei kvalifitseerita, ent mis oma olemuselt siiski maksevahendite definitsiooni alla kuuluvad. Vältimaks olukordasid, kus turul on kasutusel mitmeid maksevahendeid, mis ei kuulu ühegi definitsiooni alla, tulekski maksevahendi legaaldefinitsioon hoida võimalikult avatuna. Levinumatest alternatiividest saab siinkohal välja tuua mobiilimaksed ehk lühendatult m-maksed, *PayPal*'i-laadsed tehnoloogilised lahendused ning lojaalsusprogrammi raames kaupmeeste poolt väljastatavad boonuspunktid, mida punktide omaja saab soovi korral sama kaupmehe juures tulevikus tehtavate ostude eest tasumisel kasutada.

Mobiilne finantsteenus on termin, mida omistatakse erinevatele finantsilistele tegevustele, mille jaoks on kasutatud tänapäeval laialdaselt levinud nutikaid mobiiltelefone ehk nutitelefone. Selliseid tegevusi saab laias mõttes jagada kaheks – mobiilipangandus ning mobiilimaksed.[37] Käesoleva magistritöö teemast lähtudes on asjakohane peatuda viimati nimetatud, mobiilimaksete temaatikal. Ehkki sarnaselt identifitseerimisvahenditele on ka mobiilimaksete kujul tegemist nn maksevahendiga, mis eeldab sidevahendi kasutamist maksejuhise andmiseks, on nende erinevus peamiselt tehniline. Kui mobiilimaksete puhul on nii maksevahend kui maksevahendi kasutamiseks vajalik sidevahend mobiiltelefoni kujul samad, siis internetipanga identifitseerimisvahendite puhul peab neid rangelt eristama. Näiteks identifitseerimisvahend kui paroolikaart koos vastavate salasõnadega internetipanka sisenemiseks on maksevahend VÕS § 709 lg 8 mõistes, ent arvuti või ka mobiiltelefon on sellisel juhul üksnes sidevahendiks, mis võimaldab maksevahendiga kaasnevaid hüvesid kasutada. Mobiilimaksete puhul langevad aga makse- ning sidevahend ühte, kuivõrd mobiili tuleb sellisel juhul vaadelda nii sidevahendi kui ka maksevahendina.

M-maksed on oma olemuselt maksed, mille puhul makse andmed ja maksekorraldus aktiveeritakse, edastatakse või kinnitatakse mobiiltelefoni või -seadme abil ning mobiilimaksega saab tasuda teenuste ja digitaalsete või füüsiliste kaupade ostmisel Interneti kaudu või ostukohas.[38] Seega m-makseid on võimalik kasutada erinevate teenusepakkujate veebilehtedel, mobiililehtedel ja nutitelefoni rakendustes, tasudes pakutavate teenuste/kaupade eest mobiiltelefoni arvega.[39] Lisaks arve-põhisele teenuse tarbimisele on võimalik m-maksed siduda ka isiku krediitkaardiga, mistõttu kui isik saadab mobiiltelefoni

[37] J. S. Cheney. *An Examination of Mobile Banking and Mobile Payments: Building Adoption as Experience Goods?* 2008, p 6.
[38] Roheline raamat, *opt.cit.*, lk 5.
[39] Maksed mobiiliga. AS EMT. Arvutivõrgus. Kättesaadav: https://www.emt.ee/era/teenused/maksed-mobiiliga. 13.04.2015.

vahendusel juhise toote/teenuse ostmiseks, kajastatakse vastava toote või teenuse hind tema krediitkaardi väljavõttel.

M-maksetega seonduvad eelised seisnevad peamiselt taolise maksmisviisi mugavuses ning mõningate mööndustega öeldes ka krediidipõhisel ostmisel – nimelt piisab toote või teenuse eest tasumiseks üksnes etteantud numbrile helistamisest või sõnumi saatmisest ning nimetatud summa lisatakse arvestusperioodi lõpus isiku mobiiliarvele. Selliselt toimimiseks vajab isik üksnes m-maksete lepingut enda telefonioperaatoriga ega vaja täiendavaid maksekaarte või paroole tehingu sooritamiseks. Ostetud kauba või tarbitud teenuse hinnale vastav summa lisatakse telefonioperaatori poolt arvestusperioodi lõpus maksevahendi kasutajale väljastatavale arvele ning maksevahendiks sellisel juhul oligi isiku enda mobiiltelefon. Taolise arve esitamist ei tule siinkohal mõista klassikalise arvena tsiviilõiguse mõttes tarbitud kauba või teenuse eest, vaid makseteenuste kontekstis tuleb nimetatud arvet pidada eelkõige kulutuste hüvitamise nõudeks maksejuhise täitmise eest makseteenuse pakkuja poolt. Tarbijatele mõeldud mugavus on nimetatud protsessis tunnetatav – üksnes mobiili kasutades on võimalik tasuda kaupade/teenuste eest, saades hüve kohe kätte, ent maksta tuleb alles mobiilteenust osutava operaatoriga kokkulepitud arvestusperioodi saabumisel. Samuti ei saa alahinnata tehingute kiiruse poolt tekkivat mugavust, kuivõrd isikutel on võimalik teha makseid ajahetkest, asukohast ning ka parasjagu pooleliolevast tegevusest sõltumata.

Vähemlevinud võimalusena pakub m-maksete lahendus võimalust sooritada ka kontaktivabasid makseid otse müügikohas. Kasutades lähiväljasidet (*Near Field Communication*), mis on praegu juhtiv kontaktivaba tehnoloogia, on mobiilimakse tegemiseks vaja erivarustusega mobiiltelefoni, mille müügikohas (nt kaupluses või ühistranspordivahendis) asuv kaardilugeja ära tunneb, kui telefon selle lähedusse asetatakse.[40] Lähiväljasideme idee seisneb selles, et asetades mobiiltelefoni andmeid lugeva tehnoloogilise seadme vahetusse lähedusse, on võimalik vahetada seadmetel olevat informatsiooni.[41] Selleks on vajalik, et mõlemale seadmele oleks lisatud lähiväljasidet toetav kiip.[42] Ka nimetatud tehnilise lahendusega on m-maksete kasutusmugavust veelgi laiendatud. Lähiväljasideme loojad on läinud isegi nii kaugele, et pidanud seda uuendust võimaluseks, mis kaitseb isikute rahakotte varguste ning pettuste eest.[43]

[40] Roheline raamat, *opt.cit.*, lk 5.
[41] CNET. *Everything you need to know about NFC and mobile payments*. Available at: http://www.cnet.com/how-to/how-nfc-works-and-mobile-payments/. 15.04.2015.
[42] *Ibid.*
[43] *Ibid.*

Mobiiltelefoniga tehtavate maksete maht kasvab praegu kõigist makseviisidest kõige kiiremini, kuivõrd seda toetab keerukate makserakenduste installeerimise võimalusega nutitelefonide kiire levik.[44] Uuringute kohaselt on m-maksete väärtus maailmas 2014. aastal üle ühe triljoni USA dollari, olles ainuüksi Euroopas 350 miljardit USA dollarit.[45]

M-maksete turg on käesoleval hetkel vaatamata selle populaarsuse kasvule siiski üsnagi killustatud, kuivõrd peamised turul tegutsevad ettevõtjad (mobiilsideoperaatorid, makseteenuse osutajad, mobiiltelefonide tootjad) ei ole veel toimivas ärimudelis kokku leppinud, mis võimaldaks rakendada koostalitusvõimelisi makselahendusi ning seepärast on suurimad ja paljulubavaimad üleilmsed m-makse algatused tehtud praegu väljaspool Euroopat.[46] Euroopa m-maksete turg võib jäädagi killustatuks, kui puudub konkreetne Euroopa raamistik, milles käsitletakse peamisi probleeme, näiteks tehnilisi standardeid, turvalisust, koostalitusvõimet ja turuosaliste vahelist koostööd.[47]

Teise maksevahendi alternatiivina on alates 2007. aasta sügisest ka Eesti tarbijatele avanenud võimalus saata ja võtta raha vastu läbi *PayPal*'i süsteemi. *PayPal* on tasuta globaalne maksevahend, mis võimaldab teha *online* makseid kiirelt ja turvaliselt, samuti võtta neid vastu ning seda riigipiire tundmata.[48] Maksekaartidest erineb *PayPal* lahendus eelkõige selle poolest, et nimetatud lahendust ei paku krediidiasutused ise, vaid see käib läbi iseseisva portaali ning turvalisuse aspektist vaadatuna on läbi *PayPal*'i keskkonna ostude eest tasumine turvalisem, kuivõrd kaupmehele ei edastata tarbija krediitkaardi andmeid. Olles reklaaminud end kui kaasaegset ning turvalist makseteenuse portaali, on *PayPal*'i peamisteks konkurentideks just internetipanga ning m-maksete teenuste pakkujad.[49]

PayPal'i plussiks on sarnaselt m-maksetega võimalus kasutada selle poolt pakutavaid teenuseid ajast ning kohast sõltumata. Samuti on tegemist üsnagi atraktiivse variandiga inimestele, kes sooritavad oma oste enamasti portaalides nagu *eBay*, kuivõrd *PayPal* pakub tavaliste panga kaudu tehtavate maksetega mõnevõrra turvalisemat lahendust. Nimelt olukorras, kus üks tarbija ostab internetist teise tarbija käest kaupu, ise neid seejuures nägemata, ei saa ta kunagi kindel olla, kas saabuv kaup ka tegelikkusele vastab. *PayPal* pakub siinkohal võimalust, kus ostja kannab raha küll müüja *PayPal* kontole enne tehingu lõpuleviimist, ent müüja saab oma raha kätte alles siis, kui ostja on ostetud kauba kätte saanud

[44] *Ibid*, lk 5.
[45] *Ibid*, lk 5.
[46] *Ibid*, lk 5.
[47] *Ibid*, lk 6.
[48] Mis on *PayPal*? *PayPal* Eesti kogukond. Arvutivõrgus. Kättesaadav: http://www.paypal-eesti.maksed.net. 13.04.2015.
[49] J. L Trautman. *E-commerce and Electronic Payment System Risks: Lessons from PayPal*, p 12.

ning kinnitanud selle kokkulepitud omadustele vastavust. Mõlema poole jaoks on tegemist kasuliku variandiga – ostja saab kindel olla, et kui talle peaks saadetama ebakvaliteetne või vale kaup, saab ta oma raha kergesti tagasi ning teiselt poolt saab müüja taolise müügiviisiga nõustudes tekitada ostjates usaldust, et kuna on nõus raha saamisega ootama, garanteerib ta sellega, et kaup vastab kokkulepitule.

Kolmanda alternatiivse maksevahendina väärib antud teema juures esile toomist Eesti kaubanduses viimastel aastatel populaarseks muutunud boonuspunktide süsteem. Selle süsteemi on kaupmehed vastu võtnud loojalsusprogrammi raames, meelitamaks kliente sooritama oma igapäeva oste just nende juures.

Nimetatud süsteem eeldab tarbijate poolt kaupmehe juures kliendiks registreerumist, mille kinnituseks väljastatakse ka personaalne kliendikaart. Samas ei pruugi kliendikaart esineda füüsilisel kujul, kuivõrd kaupmehed pakuvad võimalust ühendada kliendiprogramm isikutel juba olemasoleva ID-kaardiga. Selliselt saab kaupmees reklaamida end ka kui keskkonnateadliku kauplejana, samas aga olla kindel, et kliendiprogrammi hüvesid kasutab üksnes selleks õigustatud isik – reeglina hoiavad isikud oma ID-kaarte kui isikut tõendavat dokumenti enda valduses, mis ei pruugi nii olla aga tavaliste kliendikaartide puhul.

Boonuspunktide süsteemi kui alternatiivse maksevahendi kasutamisel on isiku huvides igakordset ostu sooritades registreerida ka kliendikaart, kuivõrd vastutasuks iga kulutatud summa eest annab kaupmees isikule krediiti järgneva ostu sooritamiseks. Seega sisuliselt saab isik eeliseid nii püsiklientidele ette nähtud soodustustelt kui ka ostusummalt laekuva boonusraha kujul, mida saab kasutada järgnevate ostude eest tasudes.

Autori kogemusel on nimetatud boonussüsteem leidnud kõige rohkem kasutust Kaubamajas ning Selveri, Rimi ja Prisma peremarketites. Laekunud boonussumma kujul on tegemist maksekaardi tüüpi maksevahendiga, kuivõrd kliendikaart, millele boonussummad kogunevad, ei ole oma olemuselt maksekaardiks, mis *per se* võimaldaks kaupmehe juures oma ostude eest tasuda[50], vaid kliendikaardiks, ning kogunev boonussumma suurus sõltub eelnevalt tehtud ostude kogusummast. Sellele vaatamata on boonussummade puhul olemuslikult tegemist maksevahendiga, kuivõrd kaardile kogunenud summa on reaalseks maksevahendiks järgmise ostu sooritamisel, ent seda erisusega, et kogunenud summa kehtib maksevahendina üksnes nimetatud kaupmehe juures, kelle püsikliendiks ollakse. Eeltoodu on üheks oluliseks

[50] Siinkohal ei ole arvestatud selliseid kliendikaarte, mida kaupmehed väljastavad koostöös pankadega ning millega pakutakse klientidele krediidi saamise võimalust. Näitena võib siinkohal tuua LHV Partner Krediitkaardi: https://www.partnerkaart.ee/et/lhv-partner-krediitkaart-ainus-pangakaart-mida-sa-vajad_archived. 15.04.2015.

erisuseks, mis eristabki VÕS § 709 lg-s 8 defineeritud maksevahendit selle alternatiivsetest võimalustest – kui seaduses reguleeritud maksevahendid on universaalsed ning sõltumata sellest, millise makseteenuse pakkujaga on makseteenuse kasutaja lepingu sõlminud, kehtivad need maksevahendina enamike kaupmeeste juures, siis boonussüsteemide raames laekuvad punktid, mida saab järgnevate ostude eest tasumisel kasutada, kehtivad need üksnes boonussumma väljastanud kaupmehe juures. Põhjus, miks boonussüsteemi raames kogutud punktisummasid ei saa VÕS-i mõttes maksevahendina käsitleda, seisneb tema mõneti keerulises konstruktsioonis, mis ei vasta seaduses toodud maksevahendi mõistele. Makseteenuse osutamise leping seisneb olemuslikult selles, et teenuse kasutaja ehk maksja usaldab makseteenuse pakkuja valdusesse oma vara ehk rahalised vahendid ning kui tal tekib selleks soov või vajadus, edastab makseteenuse pakkujale maksejuhise, kes selle siis maksja asemel täidab. Boonuspunktide süsteemi puhul on olukord mõneti erinev – ehkki ka sellisel juhul on maksejuhise algatajaks maksja, kes kaupade eest tasumisel edastab soovi kasutada tema kontole kogunenud boonuspunkte, ei ole selle summa, mis boonuspunktide arvule vastab, esialgseks omanikuks maksja, vaid hoopis kaupmees, kes ostjate lojaalsuse tänutäheks jagab neile teatud tingimustel krediiti järgmiste ostude eest tasumiseks. Kuigi ka nimetatud boonussüsteemi võib teatud mööndustega pidada VÕS § 709 lg 8 tähenduses poolte vahel kokku lepitud toimingute kogumiks, ei ole autori hinnangul seadusandja taolist maksmise võimalust nimetatud sätte all siiski silmas pidanud.

Kokkuvõtlikult on ülaltooduga toodud välja peamised erinevused maksevahendite ning maksevahendite tüüpi võimaluste vahel. Peamiselt puudutavad erinevused just maksevahendite kasutamisviisi ning –võimalusi ja on pigem tehnilised. Kuuludes aga samuti maksevahendite legaaldefinitsiooni alla, on maksekaartide ning maksekaardi tüüpi maksevahendite juriidiline konstruktsioon sarnane käesoleva töö peatükis 1.1 toodule. Mõlema vahendi puhul peab maksja andma maksejuhise makseteenuse pakkujale, mis muutub viimasele siduvaks selle kättesaamise hetkest. Enne maksejuhise täitmist peab makseteenuse pakkuja kontrollima, kas maksja on end korrektselt autoriseerinud ning ega maksejuhise andmisega ei rikuta mõnda õigusaktides sätestatud kohustust. Kui nimetatud tingimused on täidetud, on makseteenuse pakkuja kohustatud täitma maksja poolt esitatud maksejuhise.

2. Identifitseerimisvahendite kasutamisest tulenevate riskide jagunemine

2.1 Identifitseerimisvahendite kasutamisele iseloomulikud turvariskid

Põhjuseks, miks internetipanganduse populaarsus kogu maailmas pidevalt kasvav, on sellega kaasnev võimalus teiste olemasolevate kanalitega võrreldes kasutada panganduse poolt pakutavaid teenuseid võimalikult väikeste kulutustega. Sellele vaatamata ei saa internetipangandust pidada pangandussektori imeks, mida iseloomustaks riskide ning muude ebakõlade puudumine.

Koos tehingute suhteliselt madalate kuludega on internetipanganduse kiire levik toonud endaga kaasa ka mitmed uued ja seni tundmatud võimalused riskide tekkeks; samuti ka mitmeid uusi riskiliike, millega makseteenuse pakkujad peavad internetipanganduse teenust tarbijatele osutades arvestama.[51] Kuigi pangad peavad tänapäeva keerulistes konkurentsi tingimustes pidevalt võistlema parima ning seejuures ka hinnasõbralikuma teenuse pakkumises, ei tohiks nad seejuures ära unustada panganduses oluliselt hinnatud ning kaalukat turvalisuse aspekti. Ehkki pangandusteenuste kasutajad hindavad selliseid finantsteenuste osutajaid, kes suudavad pakkuda neile vajalikke ja kaasaegseid teenuseid efektiivselt ning võimalikult madalate kuludega, ei ole kasutajate jaoks seejuures vähem olulisem ka teenustega kaasnev turvalisuse aste. Kuivõrd kliendid usaldavad makseteenuste pakkujate valdusesse oma vara, ei ole nad huvitatud teenusest, mis võib turul olla küll uus ja ainulaadne, pakkudes kasutajatele varasemaga võrreldes enneolematut mugavust, ent mille suhtes teenuse pakkuja ei suuda piisavat turvalisust tagada. Turvalisust ei ole aga pidevalt muutuvas informatsiooni tehnoloogias kerge saavutada, kuna finaalsust ei ole nii riski liikides kui ka nende kontrollimismehhanismides, kuivõrd mõlemad on pidevas muutumises.[52]

Riskide liike, mis internetipanganduse kasutamisega kaasneda võivad, on mitmeid, kuid käesoleva töö temaatikaga haakub eelkõige makseteenuse pakkuja poolt loodud internetikeskkonna turvalisuse ehk identifitseerimise risk. Kasutatavate tehnoloogiatega seonduvatel riskidel peatub autor töö 3. peatükis.

Nagu eelmise peatüki alateema 1.1 juures on välja toodud, on inimestel enese identifitseerimiseks internetipanga keskkonnas mitmeid võimalusi, mille vahel valida. Kuigi identifitseerimisvõimalusi ja -vahendeid on mitmeid ning pangad tegelevad pidevalt nende

[51] Report on Internet Banking. Reserve Bank of India. Arvutivõrgus. Kättesaadav: http://www.rbi.org.in/scripts/PublicationReportDetails.aspx?ID=243#ch5. 13.04.2015.
[52] *Ibid.*

turvalisemaks muutmisega, ei saa eitada, et identifitseerimisvahendite kasutamine ei ole ega tõenäoliselt saagi olla päris riskivaba.

Internetipanganduse korrektsel kasutamisel taandub peamiselt kõik teenust kasutada sooviva isiku tuvastamisele. Korrektse tuvastamise põhjus peitub ennekõike selles, et makseteenuse pakkuja on kohustatud tuvastama makseteenuse kasutaja tegelikku tahet teenuse kasutamiseks ehk internetipanka sisenemiseks enne, kui juurdepääs teenustele võimaldatakse.[53] Isikule on küll makseteenuse pakkuja poolt väljastatud personaalsed tunnuskoodid, mida identifitseerimisprotsessis kasutada, ent võrreldes teiste maksevahenditega on internetipanganduse puhul isiku korrektselt tuvastamine tunduvalt komplitseeritum. Põhjus seisneb selles, et makseteenuse pakkujal puudub kindel teadmine sellest, kes parasjagu internetikeskkonda siseneda proovib. Makstes kaupmehe müügikohas pangakaardiga, tegutseb kaupmees panga nn käepikendusena, kes peab makse autoriseerimise korrektsust jälgima. PIN-koodi ning pangakaardi kui maksevahendi kombineeritud kasutamine annavad seejuures kaupmehele piisava kaudse tõendi selle kohta, et maksejuhise andja on selleks õigustatud ning et tehing vastab omaja tahtele[54], ehkki ka sellisel juhul ei ole igakordselt välistatud võimalus, et maksevahendit kasutab selleks õigustamatu isik (nt õigusnäivusel põhineva volituse korral). Kui aga isik siseneb maksevahendit kasutades internetipanka, toimub see sidevahendi abil ning pangal puudub tegelik kontrollimisvõimalus selle üle, kas siseneda proovib selleks õigustatud isik või tegemist on kellegi teise identifitseerimisvahendit kasutada prooviva isikuga. Kuivõrd internetipanga keskkonda sisselogijat ei valva ükski makseteenuse pakkuja või kaupmehe volitatud töötaja / esindaja, puudub viimastel ka sisselogija isiku 100%-liselt korrektselt tuvastamise võimalus.

Isiku korrektne tuvastamine maksevahendi kasutamisel on seotud eelkõige konto debiteerimise õiguse ning makseteenuse pakkujal lasuva tõendamiskoormisega. Makseteenuse pakkujal on õigus teenuse kasutaja kontot debiteerida üksnes tingimusel, et maksja on maksetehingu täitmiseks andnud oma nõusoleku ehk autoriseerinud end korrektselt VÕS § 724^1 mõttes. Kui aga tegemist on olukorraga, kus on vaieldav, kas maksetehing on autoriseeritud, lasub makseteenuse pakkujal kohustus § 733^4 lg 1 mõttes tõendada, et maksetehing on autenditud, korrektselt dokumenteeritud, kontodel kajastatud ning et tehingu täitmist ei ole mõjutanud ükski puudus. Seega on makseteenuse pakkujal kohustus tagada kontrollmehhanism selle üle, kas maksetehing on korrektselt autenditud ning kas maksejuhis pärineb selleks õigustatud isikult. Kui makseteenuse pakkuja ei kontrolli maksetehingu

[53] European Central Bank. *Assessment Guide for the Security of Internet Payments.* February 2014. Available at: https://www.ecb.europa.eu/pub/pdf/other/assessmentguidesecurityinternetpayments201402en.pdf. 16.04.2015.
[54] T. Runnel, *opt.cit.*, lk 368.

autoriseerimist ning selle tulemusel täidab maksejuhise, mis pärineb selleks õigustamatult isikult, vastutab makseteenuse pakkuja § 733[2] mõttes ning kohustub taastama olukorra maksja kontol, mis oleks olnud, kui autoriseerimata makset ei oleks toimunud.

Põhimõtteliselt on olukord sarnane ka internetipanga kasutamise puhul, ent erisusena võib makseteenuse pakkuja tulenevalt §-s 733[8] sätestatust debiteerida maksja kontot ka juhul, kui maksejuhis ei pärine selleks õigustatud isikult. Kuivõrd §-s 733[8] sätestatu kohaselt kannab makseteenuse kasutaja maksevahendi kadumisest või varastamisest teatamiseni maksevahendi väärkasutamise riisikot, on võimalik olukord, kus enne makseteenuse pakkuja teavitamist on maksevahendit kasutanud selleks õigustamatu isik. Tegemist on sellisel juhul olukorraga, kus maksevahendit kasutab küll selleks õigustamatu isik, ent kuna identifitseerimine toimub sidevahendi kaudu ning isiku valduses on korrektsed salasõnad ning kasutajatunnused, ei ole makseteenuse pakkuja teadlik, et tegelikult algatab maksejuhise selleks õigustamatu isik. Kuna aga makseteenuse kasutaja on maksevahendi otsene valdaja, omades seeläbi maksevahendi üle praktiliselt ainuisikulist kontrolli, kannab tema ka riisikot maksevahendi väärkasutamise eest perioodil, mil ta makseteenuse pakkujat maksevahendi kaotamisest või varastamisest ei teavita. Seega eeltoodud erandiga võib teatud tingimustel olla õigustatud olukord, kus makseteenuse pakkuja täidab maksejuhise ning debiteerib teenuse kasutaja konto siis, kui maksejuhis ei pärinenud tegelikult selleks õigustatud isikult.

Eeltoodust tulenevalt saab internetipangandusega seonduvad riskid jaotada eelkõige tulenevalt sellest, kas tegemist on riskidega makseteenuse pakkuja või teenuse kasutaja jaoks. Makseteenuse pakkuja puhul saab peamise riskina välja tuua eelnevalt mainitud olukorra, kus internetipanga teenust proovib kasutada isik, kelle valdusesse on sattunud teisele isikule makseteenuse pakkuja poolt väljastatud identifitseerimisvahendid. Teise turvariskina, mis makseteenuse pakkuja poolse tegevusega seondub, saab välja tuua IT-süsteemide ning – lahendustel esinevad puudujäägid – siinkohal on mõeldud olukorda, kus identifitseerimisprotsess jääb mõne tarkvaralahendustes esineva vea tõttu poolikuks või süsteemiviga lubab identifitseerimisprotsessi tulemuslikult lõpetada, ehkki sisselogimisel esitati väärad identifitseerimisvahendid või sellel olnud andmed. Samuti kannab makseteenuse pakkuja tema ja kasutaja vahelises lepingulises suhtes riisikot selles osas, millises ta võimaldab panka sisse logida teiste teenusepakkujate poolt võimaldatavate tehniliste lahenduste kaudu, nt ID-kaardi ning mobiil-ID kasutamise läbi.[55] Kuna

[55] Autor on siinkohal pidanud silmas olukorda, kus makseteenuse pakkuja kasutab teenuse osutamisel maksevahendajaid. Nimetatud olukorda reguleerib VÕS § 733[3] lg 8, mis sätestab, et makseteenuse pakkuja vastutab käesoleva paragrahvi kohaselt ka juhul, kui vastutus on tegelikult omistatav makseteenuse pakkuja

makseteenuse pakkuja on see, kellel on teenuse kasutajaga lepinguline suhe ning kellel lasub kohustus teha kindlaks, kas talle saadetud maksejuhis pärineb selleks õigustatud isikult, vastutab just teenuse pakkuja selle eest, kui viimati nimetatud maksevahendite kasutamisel tekib nende tehnilistes kanalites mõni tõrge ning identifitseerimisprotsess jääb selle tõttu poolikuks või täidetakse ebaõigesti. Nimetatu ei kuulu kohaldamisele aga olukorras, kus makseteenuse pakkuja klient on isiklikult VÕS § 733^3 lg 8 mõttes maksevahendaja valinud.

Ehkki ülalmainitud tehnilist laadi tõrked ei ole identifitseerimisprotsessi puhul praktikas välistatud, räägib antud teemal praktiliselt olematu kohtupraktika selle kasuks, et peamised turvariskid identifitseerimisvahendite puhul seonduvad enamasti siiski nende kopeerimise ning edaspidise kuritarvitamise võimalikkuses.

Kõige kergemini kopeeritav ja seetõttu ka makseteenuse pakkujate poolt kõige ebaturvalisemaks peetavaks identifitseerimisvahendiks on paroolikaart, millel olevad andmed on võrreldes teiste identifitseerimisvahenditega kõige kergemini kättesaadavad. Ehkki üksnes paroolikaardil olevatest koodidest ei piisa internetipanka sisselogimiseks, vaid selleks on vajalikud ka teenuse kasutaja personaalne kasutajatunnus ning salasõna, ei ole pahatahtlike kavatsustega isikutel väga keeruline nende olemasoluta internetikeskkonda sisse logida. Tänapäeval on küberkurjategijate oskused juba sedavõrd arenenud, et üksnes isiku arvutisse sisse murdes on nad võimelised paigaldama sinna nuhkvara ja seeläbi avastama nende kasutajanime ning salasõnasid.[56] Seega kui isiku identifitseerimisvahend satub kas viimase kaotamisel või varguse korral professionaalse küberkurjategija valdusesse, ei tal tõenäoliselt erilisi probleeme häkkida sisse ka maksevahendi omaja arvutisse ning leida sealt maksevahendiga seotud kasutajanimi ning salasõna, mille kaudu omaja internetipanka sisse logida ning sellelt kontolt autoriseerimata makseid teostada. Tekkivat kahju saab teenuse kasutaja ära hoida või vähendada teenuse pakkuja kohesel teavitamisel, ent sellel kohustusel peatub autor töö järgmistes peatükkides.

Samuti ei ole harvad ka juhtumid, kus paroolikaarte hoitakse üheskoos paberiga, millele on kasutajatunnus ning salasõna juurde kirjutatud.[57] Kui pahatahtlike kavatsustega isik saab sellise identifitseerimisvahendi enda valdusesse ning selle abil internetipanga keskkonda sisse logib, puudub makseteenuse pakkujal tegelikkuses selle kohta igasugune teadmine ja kontroll

---

valitud maksevahendajale, kuid makseteenuse pakkuja ei vastuta juhul, kui tegelikult vastutava maksevahendaja on valinud makseteenuse pakkuja klient.

[56] Arvutikaitse. Nuhkvara. Arvutivõrgus. Kättesaadav: http://www.arvutikaitse.ee/arvutikaitse-algtoed/nuhkvara/. 13.04.2015

[57] Näiteks lahendas Harju Maakohus kriminaalasja nr 1-12-7896, kus süüdistatav varastas kannatanu autost Sampo panga deebetkaardi ja internetipanga paroolikaardi koos PIN-koodide, kasutajatunnuse ning salasõnaga, tekitades üksnes internetipanga vahendusel ülekannete teostamisega kannatanule üle 1200 euro suuruse kahju.

– teenuse pakkuja silmis on kasutaja end korrektselt identifitseerinud ning tal ei tekigi kahtlust, et tegemist võiks olla kellegi teise kui autoriseeritud kasutajaga. See on ka mõistetav, kuivõrd makseteenuste pakkujatel on mitmekümneid tuhandeid internetipanganduse kasutamiseks lepingu sõlminud kliente, kes igapäevaselt nimetatud keskkonda sisse logivad, mistõttu mõne täiendava kontrolli, seejuures kas või pistelise, läbiviimine sisseloginud kasutajate tuvastamiseks on välistatud. Samuti leiab autor, et sellise kontrolli, isegi kui see oleks võimalik või mõistlik, läbiviimiseks on põhjendatud alust raske leida – makseteenuse pakkuja silmis on identifitseerimisprotsess korrektselt läbitud ning põhjuseid, mis peaksid teenuse pakkujas tekitama kahtluse, kas sisselogijaks on ikka õigustatud isik, on internetipanga kasutamise puhul äärmiselt keeruline, kui mitte võimatu leida. Olukord oleks vastupidine, kui tulenevalt §-st 733^8 on maksevahendi omaja teavitanud makseteenuse pakkujat, et tema maksevahend on kaotatud või varastatud. Kui taolise teavitamise järgselt proovitakse siiski maksevahendiga maksejuhist algatada, peaks ka makseteenuse pakkujal tekkima põhjendatud kahtlus isiku identifitseerimise korrektsuses, isegi kui sisestatud andmed on korrektsed, ning maksejuhist mitte täitma. Kui aga makseteenuse pakkuja sellele vaatamata õigustamatult isikult pärineva maksejuhise täidab, siis kuivõrd makseteenuse kasutaja on nõuetekohaselt makseteenuse pakkujat teavitanud maksevahendi kadumisest või varastamisest, kannab makseteenuse pakkuja kõik maksejuhise täitmisega kaasnevad kahjud ning peab § 733^2 mõttes taastama makseteenuse kasutaja kontol olukorra, mis oleks olnud, kui autoriseerimata makset ei oleks toimunud.

Nimetatud seisukoht ei lähe vastuollu ka Riigikohtu 21. mai 2002. aasta otsusega, millises Riigikohus leidis, et panganduses tuleb lähtuda mõistlikuks peetavast hoolsusastmest, mistõttu pangal on kohustus keelduda ülekande tegemisest mitte ainult siis, kui turvaelemente kasutatud valesti või pangal tekkis kahtlus isiku identifitseerimisel, vaid ka siis, kui turvaelemente kasutati õigesti, aga pangal pidi tekkima kahtlus isiku identifitseerimisel.[58] Õiguses leidub Riigikohtu seisukoha analoog VÕS §-s 724^3, mis annab makseteenuse pakkujale õiguse keelduda maksejuhise täitmisest objektiivselt põhjendatud kaalutlustel. Kui aga makseteenuse kasutaja siseneb internetipanka enda isikliku arvuti vahendusel ning sisestab kõik nõutavad kasutajatunnused ja paroolid korrektselt, on pea võimatu, et makseteenuse pakkujatel ka mõistlikku hoolsusastet rakendades tekiks kahtlus isiku identifitseerimisel – autori hinnangul on see juba üksnes tehnoloogilisest aspektist võetuna põhimõtteliselt võimatu. Eeltoodud seisukoht ei pruugi aga kuuluda kohaldamisele juhul, kui

[58] RKTKo 3-2-1-73-02, p 10.

maksejuhis algatatakse nn kolmanda maailma riikidest.[59] Kuivõrd paljud pangaandmete kopeerimise ning nuhkvarade saatmise juhtumid, millel autor peatub põhjalikumalt käesoleva töö alapeatükis 3.2.3, saavad alguse just kolmanda maailma riikidest[60], on ka makseteenuse pakkujad võtnud võimalike kahjude ennetamiseks kasutusele lisameetmeid andmete kopeerimise tuvastamiseks. Kuivõrd paljud nuhkvarade varjatud paigaldamist sisaldavad e-kirjad pärinevad tihti kolmanda maailma erinevatest riikidest, on makseteenuse pakkujad muutunud ettevaatlikuks, kui avastavad, et mõne internetipanga kasutaja kontolt tehtud maksejuhis pärineb mõne nimetatud riigi IP-aadressilt. Sellise avastuse tegemisel on pankade tavapraktikaks kujunenud makseteenuse kasutajatega kontakteerumine, et kinnitada, kas makse pärineb ikka õigustatud isikult. Seega ehkki internetipanganduse puhul on reeglina võimatu saada aru, kas maksejuhise algatas selleks õigustatud isik või mitte, on makseteenuse pakkujad suutnud luua tehnilised võimalused, mis teatud tingimuste esinemisel võimaldavad selekteerida välja need juhtumid, kus maksejuhise algatajaks ei pruugi olla selleks tegelikult õigustatud isik.

2.2 Identifitseerimisvahendi õigustamatu kasutamisega seotud riisiko kandmine

Riigikantselei poolt hallatav Eesti Õigustõlke Keskus avab riisiko mõiste läbi definitsiooni, mille kohaselt on riisiko raha kaotamise võimalus majandusürituses, eriti investeerimisel.[61] Seega teeb riisiko mõiste vihje sellele, et kuivõrd riisikoga seondub raha kaotamise võimalus, pannakse selle mõistega sisuliselt paika osapooltevahelise vastutuse[62] piirangud – kes ja millisel juhul kannab riski, et tekkida võivate rahaliste kahjude osas jääb vastutus tema kanda. Kuna eeltoodust tulenevalt on riisiko ning vastutus oma olemuselt tihedalt seotud, on oluline avada ka riisiko olemus ning seetõttu toob autor käesolevas alapeatükis välja riisikoga seonduvad muudatused VÕS-s ning analüüsib, millist mõju see seadusele avaldas ja kas selline riisiko jaotus osapoolte vahel on õigustatud.

Kehtivas seaduses reguleerib maksevahendi kasutamisega seotud riisiko kandmist VÕS § 733[8] lg 1, mis sätestab, et kui autoriseerimata makse on tehtud, kasutades kadunud või varastatud maksevahendit, kannab maksja riisikot, kuid mitte rohkem kui maksevahendi

[59] Autor peab siinkohal eelkõige silmas Aasia ja Aafrika riike ning Ladina-Ameerikat.
[60] Nimetatud seisukoht on kujunenud peamiselt Eesti ajakirjanduses levinud informatsiooni kohaselt. Näitena võib tuua 9. veebruaril 2013. aastal Postimehes avaldatud artikli "Nigeeria petukirjadega petetakse Soomest sadu tuhandeid eurosid". Arvutivõrgus. Kättesaadav: http://www.postimees.ee/1132430/ajaleht-nigeeria-petukirjadega-petetakse-soomest-sadu-tuhandeid-eurosid. 13.04.2015.
[61] Riisiko definitsioon. Eesti Õigustõlke Keskus. Arvutivõrgus. Kättesaadav: http://mt.legaltext.ee/esterm/concept.asp?conceptID=2855&term=riisiko. 13.04.2015.
[62] Seda, millises kontekstis siinkohal nimetatud vastutuse terminit tegelikult kohaldada tuleks, vt käesoleva töö peatükist 2.3.1.

väljajaga[63] kokkulepitud piirsumma ulatuses, kõige enam aga summa ulatuses, mis vastab 150 eurole. Riisiko kandmine osapoolte vahel tähendab sisuliselt seda, et maksevahendi omaja kannab maksevahendi kasutamisest tingitud kahjulike tagajärgede eest riski ka juhul, kui maksevahendi alusel makseteenuse pakkujale antud maksejuhis ei pärinenud tegelikult temalt. See tähendab, et kui makseteenuse pakkuja silmis on konkreetsel ajahetkel maksevahendi valdaja end korrektselt identifitseerinud ning maksejuhise algatanud, siis olukorras, kus ei esine muid objektiivseid põhjuseid, miks makseteenuse pakkujal peaks identifitseerimisprotsessi korrektsuse osas kahtlusi tekkima, võib makseteenuse pakkuja maksevahendi omaja kontot debiteerida isegi siis, kui maksejuhis ei pärine tegelikult maksevahendi omajalt. See on tihedalt seotud VÕS § 733[8] lg-s 3 sätestatuga – makseteenuse kasutaja ei kanna eelnevalt nimetatud riisikot alates ajast, kui kahju on tekkinud pärast seda, kui maksevahendi omaja on teenuse pakkujat kaardi kaotamisest või varastamisest teavitanud. Selliselt on seadusandja soovinud luua regulatsiooni, mis sunniks maksevahendi omajat võimalikult kiiresti makseteenuse pakkujat kaotatud või varastatud maksevahendist teavitama, misläbi maksevahendi omaja vabaneks ka edasiste kahjulike tagajärgede kandmise kohustusest – riisikot kahjulike tagajärgede eest kannab teenuse kasutaja seni, kuni on makseteenuse pakkujat teavitanud, et maksevahend on varastatud või kadunud ning võib eksisteerida risk autoriseerimata maksete algatamiseks.

Eelnevalt nimetatud piirsumma – 150 eurot – kohaldamise puhul ei ole aga tegemist absoluutreegliga, mis kuuluks rakendamisele igas olukorras. VÕS § 733[8] lg 2 kohaselt ei kuulu nimetatud summaline piirang kohaldamisele juhtudel, mil maksevahendi omaja rikkus tahtlikult või raske hooletuse tõttu makseteenuse pakkujale maksevahendi kaotamisest või varastamisest teavitamise kohustust või ka siis, kui seejuures oli tegemist maksevahendi omaja poolse pettusega. Samuti ei kuulu piirsumma kohaldamisele, kui makseteenuse kasutaja rikkus tahtlikult või raske hooletuse tõttu maksevahendi väljastamise ja kasutamise tingimusi[64]. Riisikot maksevahendi kaotamise või varguse või maksevahendi väljastamise ja kasutamise tingimuste rikkumise korral kannab maksevahendi omaja seega üksnes ajahetkeni, mil ta maksevahendi kaotamisest või vargusest teenuse pakkujat teavitab, ning alates selle kohustuse täitmisest vabaneb ta riisiko kandmisest. Nimetatud sätte eesmärgiks on motiveerida maksevahendi omajat kiiresti teavitama makseteenuse pakkujat maksevahendi kaotamisest või vargusest, mille tulemusel läheks riisiko tekkivate kahjude osas üle

[63] Muudatustele eelnenud VÕS-i regulatsioonis tähistas maksevahendi väljaja hetkel kehtiva seaduse tähenduses makseteenuse pakkujat. Seadusandja on mõisteaparaati uuendanud, ent ekslikult jätnud sisse vana mõisteaparaadi mõiste.
[64] Tingimused, mille kehtestab makseteenuse pakkuja makseteenuse lepingus.

makseteenuse pakkujale, kes saab makse- või abivahendi kehtetuks tunnistada ja võimaliku edasise kahju minimeerida.[65]

Enne 2010. aastal jõustunud VÕS-i muudatusi oli maksevahendi kasutamisest tuleneva riisiko kandmine sätestatud VÕS §-s 742. Nimetatud VÕS-i sätte aluseks oli Euroopa Komisjoni soovitus nr 97/489/EÜ[66], mis on aluseks olnud ka direktiivi 2007/64/EÜ koostamisel, kuivõrd selles ettenähtud põhitõed on viimati nimetatule sarnased.[67] Ehkki direktiivi 2007/64/EÜ sõnastus on mitmekesisem ning rohkem sätteid lahti seletav kui Komisjoni soovitus, on selles toodud sätete põhimõtted samased 2010. aastal jõustunud VÕS-ga võrreldes. See on ka põhjendatav, kuivõrd 2010. aastal jõustunud VÕS-i muudatuste eesmärgiks oligi EL liikmesriikide õigusnormide ühtlustamine direktiivis 2007/64/EÜ toodud regulatsiooni alusel. Eeltoodust tulenevalt ei sisalda 2010. aastal VÕS-i sisseviidud muudatused pooltevahelise riisiko reguleerimisel olulises osas mastaapseid muudatusi, kuna muudeti peamiselt paragrahvide sõnastusi ning mõisteaparaati tervikuna, jättes kehtivad põhimõtted samaks.

Varasemalt kehtinud riisiko sätte § 742 ülesehitus erineb mõneti hetkel kehtiva sätte omast – autori hinnangul dubleerisid § 742 lg 1 ja 3 teineteist. Nimelt sätestas § 742 lg 1, et maksevahendi varguse või kaotsimineku korral kannab maksevahendi omaja riisikot seni, kuni on vahendi vargusest või kaotsiminekust makseteenuse pakkujat teavitanud, ning lg 3 lisas, et maksevahendi omaja ei kanna alates makseteenuse pakkuja teavitamisest riisikot. Lõikes 3 sisalduv põhimõte tulenes tegelikult ka juba lõikes 1 sätestatust, mistõttu selle dubleerimine ei olnud otstarbekas. Autori hinnangul on kehtiv regulatsioon selgem - § 733^8 lg-st 1 tuleneb, et kui maksevahend on kaotatud või varastatud, kannab makseteenuse kasutaja riisikot maksimaalselt 150 euro ulatuses. Alates hetkest, mil teenuse kasutaja on teenuse pakkujat teavitanud maksevahendi kaotamisest või vargusest, vabaneb ta edasise riisiko kandmisest (§ 733^8 lg 3). Selliselt sõnastatuna ei jää ebaselgeks asjaolu, et kui maksevahendi kaotamise / varastamise ning sellest teenuse pakkuja teavitamiseni jääva vahepealse perioodi jooksul tehakse autoriseerimata tehing, mille tagajärjel tekib kahju, kannab need kahjud maksimaalselt 150 euro ulatuses maksevahendi omaja.

Kuna riisiko kandmine on tugevalt seotud kaotamise või varastamise situatsiooniga, on siinkohal teema kompaktsuse ning arusaadavuse huvides oluline avada varguse või kaotsimineku definitsioon tsiviilõiguses, kuivõrd see on mõnevõrra erinev karistusõiguses kehtivatest arusaamadest. VÕS-i regulatsiooni kohaselt tähendab maksevahendi vargus või

[65] T.Runnel, *opt.cit.*, lk 370.
[66] Komisjoni soovitus, *opt.cit*.
[67] Vt direktiivi 2007/64/EÜ artikkel 61.

kaotsiminek elektroonilise maksevahendi füüsilise kandja – näiteks pangakaardi või koodikaardi – väljumist makseteenuse kasutaja valdusest.[68] Internetipanga poolt pakutavate teenuste kasutamiseks vajalike identifitseerimisvahendite (eelkõige PIN-koodide ja salasõna) puhul on aga tegemist maksevahenditega, mille füüsilist valdust ei ole võimalik kaotada ega varastada – eeldusel, et teenuse kasutaja ei ole neid paberile jäädvustanud. Sellistel maksevahenditel lasuvaid andmeid on võimalik kopeerida ilma, et nende kasutaja kaotaks seejuures oma otsese valduse maksevahendile, kuna seda, mida ei eksisteeri füüsiliselt, ei saa teadlikult ka kaotada. Seetõttu ei pruugi maksevahendi omaja olla isegi teadlik sellest, et tema maksevahendil olevaid andmeid on kopeeritud. Enne makseteenuste direktiivi 2007/64/EÜ jõustumist reguleeris elektroonilisi maksetehinguid Euroopas Euroopa Komisjoni soovitus nr 97/489/EÜ, millise kohaselt tuleks eeltoodud olukorras käsitleda maksevahendi vargust laiemalt, kui ainult karistusseadustiku regulatsioon seda võimaldab – oluline ei ole mitte elektroonilise maksevahendi füüsiline vorm, vaid selles sisalduv info.[69] Nimetatud põhimõte ei ole muutunud ka ajal, mil 13. novembril 2007. aastal jõustunud makseteenuste direktiiv 2007/64/EÜ hakkas eelnimetatud Euroopa Komisjoni soovituse asemel reguleerima maksetehingute valdkonda.

Kuigi eelneva pinnalt nähtub, et kahe seadusregulatsiooni põhiprintsiibid suures osas ei erine, on oluline rõhutada järgnevat. Regulatsioonid erinevad olemuslikult selle poolest, et 2010. aastal jõustunud VÕS-i regulatsiooni on võrreldes varem kehtinud regulatsiooniga lisandunud uus säte. Nimelt on direktiivi 2007/64/EÜ eeskujul lisatud VÕS § 733[8] lõikesse 1 lause, millise kohaselt kannab maksja riisikot ka siis, kui maksevahendit on kasutatud muul õigustamatul viisil ja kui maksja ei ole isikustatud turvaelemente nõuetekohaselt hoidnud.[70] Selle lause aluseks on direktiivi 2007/64/EÜ artikkel 61 lg 1, mis näeb ette, et maksja kannab kuni 150 euro ulatuses autoriseerimata maksetehinguga seotud kahjusid, mis on tekkinud seoses /.../ maksja isikustatud turvaelementide avalikuks muutumisest põhjustatud makseviisi väärkasutamisega. Taolise lisandusega on soovitud luua regulatsioon, mis hõlmaks sõnasõnaliselt ka selliseid maksevahendeid, mis ei esine füüsilisel kujul (nagu esineb näiteks maksekaart), vaid protsessina – ehk on isikustatud turvaiseloomuga (nt PIN-kood). Ka viimati nimetatu puhul on tegemist maksevahendiga, ent seda ei saa traditsioonilises mõttes varastada

[68] A. Hinrikus. VÕS III komm, *opt.cit.*, § 742/p 3.1.
[69] *Ibid*, § 742/p 3.1.
[70] Võlaõigusseaduse III kommenteeritud väljaande kohaselt oli ka eelmises seaduses §-ga 742 hõlmatud need maksevahendid, mis ei esinenud füüsilisel kujul, ent nimetatud klausli selgesõnaline sätestamine seaduses teenib eelkõige õigusselguse ning arusaadavuse huve.

ega kaotada.[71] Regulatsiooni täiendamisega on seega soovitud VÕS-i maksevahendite regulatsiooni värskendada[72] ning seeläbi ka efektiivsemaks muuta.

Teine lisandus VÕS-i regulatsiooni puudutab vastutuse seost makseteenuse pakkuja poolsete teavitamistingimuste loomisega. Kui VÕS-i varasema regulatsiooni kohaselt ei kandnud maksja maksevahendi varguse või kaotsimineku riisikot alates ajast, kui ta on vargusest või kaotsiminekust teatanud makseteenuse pakkujat (v.a kui maksja tegutses pettusega), siis uue regulatsiooniga on direktiivi 2007/64/EÜ artikkel 61 lõike 5 eeskujul nähtud ette veel üks olukord, mil maksja vabaneb riisiko kandmisest. Nimelt näeb § 733^8 lg 4 uudse lahendusena ette võimaluse, et maksja ei kanna maksevahendi vargusest või kaotsiminekust tulenevalt riisikot, kui makseteenuse pakkuja ei ole täitnud seaduses sätestatud kohustust tagada maksevahendi kasutajale tehnilisi võimalusi teatamaks varastatud või kaotsiläinud maksevahendist. Kuivõrd regulatsiooni mõtte ja eesmärgi kohaselt on taunitav igasugune pettuse korraldamine maksevahendi omaja poolt, on ka eelmainitud sättele lisatud klausel, et see säte ei kuulu kohaldamisele juhul, kui maksja on maksevahendi kaotamisel või varastamisel tegutsenud pettuse teel – st isegi juhul, kui makseteenuse pakkuja ei ole taganud tehnilisi võimalusi maksevahendi kaotamisest või varastamisest teavitamiseks, ei vabane makseteenuse kasutaja riisiko kandmisest, kui maksevahendi kaotamisel või varastamisel tegutses ta pettusega.

Nimetatud makseteenuse pakkuja poolse kohustuse lisamine regulatsiooni on autori hinnangul ootuspärane ning õigustatud. On ebaõiglane näha maksevahendi omajale ette kohustus teavitada maksevahendi vargusest või kaotsiminekust, pannes selle seejuures sõltuvusse ka riisiko kandmisega, ent jätta samal ajal reguleerimata olukord, kus makseteenuse pakkuja ei ole taganud tehnilisi võimalusi nimetatud kohustuse täitmiseks. Riisiko kandmise seisukohalt on õiglane jätta riisiko makseteenuse pakkuja kanda, kui maksevahendi omaja soovib maksevahendi vargusest või kaotsiminekust viimast teavitada, tegutsemata seejuures pettusega, ent makseteenuse pakkuja ei ole võimalda nimetatud teavitamist.

Autorile jääb siinkohal mõistmatuks seadusandja soov muuta uue VÕS-i regulatsiooniga ka paragrahvide pealkirju, ehkki sisuline osa jäi suures osas muutmata; lisatud on vaid üksikud klauslid, mis olemasolevat regulatsiooni pigem täiendavad, kui muudavad. Kui eelnevalt oli VÕS § 742 pealkirjast üheselt aru saada, et sättega soovitakse reguleerida maksevahendi kasutamisest tuleneva riisiko kandmist, siis uue seadussätte §-i 733^8 kohta ei saa sama öelda – nimetatud paragrahv on pealkirjastatud kui maksja vastutus seoses autoriseerimata

[71] Seletuskiri, *opt.cit.*, lk 44.
[72] Seletuskiri, *opt.cit.*, lk 38.

maksetega. Ehkki riisiko ning vastutus on teineteisega tõepoolest tihedalt seotud, ei saa neid sellegipoolest sünonüümidena käsitleda. Ka hea õigusloome ja normitehnika eeskirja[73] § 23 lg 3 näeb ette, et paragrahvile tuleb anda sisu iseloomustav lühike pealkiri nimetavas käändes. Ehkki eelnimetatud säte reguleerib seaduseelnõus sisalduvate paragrahvide pealkirjastamist, ei saa kahtlust olla, et ka seadusesisesed paragrahvide pealkirjad peavad olema võimalikult lühikesed ja täpsed ning andma edasi paragrahvi sisu.

2010. aastal jõustunud VÕS-i regulatsioonist on seadusandja pidanud vajalikuks jätta välja eelmises seaduse redaktsioonis olnud § 742 lõiked 4 ja 5. § 742 lg 4 sätestas, et maksevahendi omaja ei kanna maksevahendi abil tehtud toimingust tulenevat riisikot, kui maksevahendit kasutati maksevahendi füüsilise esitamiseta või maksevahendi elektroonilise kindlaks tegemiseta. Samuti ei piisanud toodud sätte kohaselt maksevahendi omaja suhtes vastutuse kohaldamiseks sellest, et kasutati isiklikku tunnuskoodi või muud sarnast võimalust maksevahendi omaja kindlaks tegemiseks. § 742 lg 5 täpsustas, et lõikes 4 sätestatu ei kuulu kohaldamisele telefoni- või võrgupanga vahendusel tehtud toimingutele. Arvestades, et muud VÕS-s kehtinud põhimõtted jäid praktiliselt samaks, jääb arusaamatuks seadusandja kavatsus nimetatud sätete väljaarvamisel kehtivast regulatsioonist. Kontrolltoimingute teostamine, mille sisuks on eelkõige maksevahendite ebaseadusliku valduse ja muude väärkasutuste kindlaks tegemine, on tavaliselt maksevahendit aktsepteeriva kolmanda isiku ehk kaupmehe kohustus vastavalt tema ja makseteenuse pakkuja vahelisele lepingule.[74] Eelnimetatud § 742 lg 4 on mõeldud eelkõige reguleerimaks maksevahendiga tehingute tegemist internetis, kus maksevahendi isikule kuuluvuse tuvastamise võimalused üldjuhul puuduvad ning tehingut on võimalik teha üksnes maksekaardi andmete alusel, nt krediitkaardil oleva numbri ning kehtivusaja sisestamise kaudu.[75] Kui makseteenuse pakkujal on sellise tehingu tagasitäitmisel rahvusvaheliste kaardiorganisatsioonide reeglitest lähtuvalt regressiõigus kaupmehe vastu, on maksevahendi kuritarvitamisega seotud riisiko panemine maksevahendi omajale ülemäära koormav.[76] Kuivõrd nimetatud ohud ei ole ka käesoleval ajal kadunud, ei ole autori hinnangul seadusandja soov ülaltoodud regulatsiooni välja jätmiseks kehtivast õigusest põhjendatud.

Maksevahendi kasutamisest tuleneva riisiko kandmise kohta osapoolte vahel on Eesti kohtupraktika olnud minimaalne. Riigikohus rakendas oma otsuses 3-2-1-125-08[77] lahendi tegemise ajal kehtinud VÕS §-i 742 selliselt, et rõhutas riisiko hindamiseks raske hooletuse väljaselgitamise olulisust. Nimetatud lahendis oli tegemist olukorraga, kus isik jättis oma

[73] Hea õigusloome ja normitehnika eeskiri. Vastu võetud 22.12.2011 nr 180. RT I, 29.12.2011, 228.
[74] A. Hinrikus. VÕS III komm, *opt.cit.*, § 742/p 3.6.
[75] *Ibid*, § 742/p 3.6.
[76] *Ibid*, § 742/p 3.6.
[77] RKTKo 3-2-1-125-08, p 13-16.

pangakaardi autosse, kust see varastati ning mille abil võeti pangaautomaadist sularaha välja. Pank esitas kaardiomaniku vastu hagi varastatud summade sissenõudmiseks, väites, et kaardiomanik oli kaarti autosse jättes VÕS § 742 lg 2 mõttes raskelt hooletu, mistõttu sama paragrahvi lõikes 1 ette nähtud 150 euro piir vastutuse osas ei kohaldu. Riigikohus leidis, et üksnes pangakaardi järelvalveta jätmist autosse ei saa käsitleda raske hooletusena VÕS § 742 lg 2 mõttes. Kohtu hinnangul oleks raske hooletusega tegu eelkõige siis, kui maksevahend oleks autosse koos PIN-koodiga jäetud. Rasket hooletust kui süüvormi käsitleb autor põhjalikumalt käesoleva töö alateemas 3.2.1.

Tulles aga uuesti riisiko mõiste juurde, milline on peaasjalikult seotud raha kaotamise võimalikkusega, tõusetub küsimus sellest, kuidas toimub VÕS §-st 733[8] tuleneva riisiko tõendamine. Ehkki Eesti kohtupraktika on antud paragrahvi kohta põhimõtteliselt olematu, ei tähenda see automaatselt, et nimetatud paragrahvi kohaldamine on selge ning praktikas probleeme ei tekita. Nimetatud teemal on Riigikohus teinud üksnes ühe lahendi, leides oma 13. oktoobril 2005. aasta otsuses 3-2-1-92-05, et tsiviilkohtumenetluse seadustiku § 91 lg-st 1[78], mis sätestab, et kumbki pool peab tõendama neid asjaolusid, millele tuginevad tema nõuded ja vastuväited ning VÕS §-st 742 tulenevalt saab asuda seisukohale, et 150-eurolise piirangu kohaldamata jätmise aluseid peab tõendama kaardi väljaja, kui ta on esitanud hagi vastavate summade saamiseks[79].

Seadus on riisiko osas ülesehitatud selliselt, et sätestatud on olukord, millal ning millises ulatuses kannab riisikot maksekaardi omaja ning millistel juhtudel nimetatud riisiko kohaldamisele ei kuulu – eelkõige kui maksevahendi omaja soovib maksevahendi vargusest või kaotsiminekust makseteenuse pakkujat teavitada, ent viimane ei ole selleks vastavaid tehnilisi võimalusi loonud. Eeltoodust saab seega järeldada, et kõikidel teistel juhtudel, mis ei ole §-ga 733[8] kaetud, langeb riisiko kandmine makseteenuse pakkujale.

Siinkohal võib tekkida küsimus, kas see on õigustatud – panna suurema riisiko kandmise koormus makseteenuse pakkujale ning maksjale ettenähtud riisikole piirsumma, mille ulatuses viimane vastutab (v.a ülalmainitud juhtudel, mil maksja tegutseb tahtlikkuse, pettusega või oli raskelt hooletu). Autor on seisukohal, et osapoolte lepingulisi kohustusi ning võimaluses vastavaid tõendeid esitada on taolise riisiko kandmise vahekorra seadmine õigustatud ja seda eelkõige makseteenuse kasutaja kaitse seisukohalt. Makseteenuse kasutaja on maksevahendi väljastamise järgselt selle ainus valdaja – makseteenuse pakkujal kui juriidilisel isikul puudub

[78] Remargi korras märgib autor, et nimetatud Riigikohtu lahendi tegemise ajast on tsiviilkohtumenetluse seadustikku oluliselt uuendatud ning kohtu poolt viidatud põhimõte on hetkel kehtivas seadusandluses sätestatud hoopis § 230 lõikes 1.
[79] RKTKo 3-2-1-92-05, p 15.

igasugune võimalus kontrollida, kas ja kuidas teenuse kasutaja maksevahendi väljastamise ja kasutamise tingimusi täidab. Selliselt on ka loogiline, et kui maksevahend on makseteenuse kasutaja ainuvalduses, kannab ta sellel ajal ka riisikot võimalike maksevahendiga seonduvate autoriseerimata maksete eest. Kui autoriseerimata makse peaks toimuma, on makseteenuse pakkujal peaaegu võimatu tõendada, et makseteenuse kasutaja ei rakendanud vahendi valdamisel piisavat hoolsusastet – üksnes vahendi omajal on võimalik tõendada, et vahendi kaotamisel või varastamisel ei olnud ta raskelt hooletu või ei tegutsenud tahtlusega (nagu sätestab VÕS § 733^8 lg 2). Kui aga maksevahend on kaotatud või varastatud ning teenuse kasutaja on sellest nõuetekohaselt makseteenuse pakkujat teavitanud, on just viimasel paremad võimalused hoidmaks ära tekkida võivaid kahjusid või selle võimatuse ilmnemisel kahjusid vähendada. Kui enne teavitamist oli üksnes maksevahendi kasutaja valduses see, kas ja kuidas maksevahendit vallata, siis pärast makseteenuse pakkuja teavitamist maksevahendi kaotamisest või varastamisest on makseteenuse kasutaja võimalused tekkivate kahjude ärahoidmiseks nullilähedased, kui mitte võimatud – tal puudub ligipääs maksevahendit haldavatele tehnoloogilistele süsteemidele, millega edasisi kahjusid vältida või vähemalt vähendada.

Selliselt on mõistetav, et maksevahendi omamise ajal kannab selle kasutamisega seonduvat riisikot maksevahendi kasutaja, ent olukorras, kus maksevahend on varastatud või kaotatud ning maksja on sellest makseteenuse pakkujat teavitanud, on viimase tehnoloogilisi võimalusi ning juurdepääse arvestades põhjendatud [80], et maksja kannab riisikot üksnes kuni maksevahendi kaotamisest või varastamisest teavitamiseni ning edasise osas jääb riisiko makseteenuse pakkuja kanda.

Eelnevast tulenevalt on autori hinnangul õigustatud ka maksja vastutust reguleerivate sätete ammendavus – see tähendab, et makseteenuse pakkujal ei ole võimalik esitada nõudeid muudel alustel, näiteks kahju hüvitamise nõuet üldistel alustel muude kohustuste, kui §-s 733^8 nimetatud rikkumise eest mõnes teises vormis, kui tahtluse või raske hooletusega tegutsemise eest.[81] Seega näiteks olukorras, kus maksevahendi omaja on oma maksevahendit hoidnud lihtsalt hooletuna, mitte raskelt hooletuna, kohaldub tema suhtes §-s 733^8 ette nähtud riisiko ülemmäär 150 eurot ning kui tegelikult tekkinud kahju on suurem, puudub makseteenuse pakkujal võimalus esitada 150 eurot ületav kahju hüvitamise nõue maksja vastu teistel VÕS-s ette nähtud õiguskaitsevahendite kasutamist võimaldavatel alustel.

[80] Makseteenuse pakkuja on maksevahendi väljaandmise ja haldamise süsteemi peamine haldaja, kui mitte isegi looja, mistõttu oleks põhjendamatu jätta riisiko kahjude osas makseteenuse kasutaja kanda ka pärast seda, kui ta on maksevahendi kaotamisest või varastamisest teenuse pakkujat nõuetekohaselt teavitanud.
[81] Seletuskiri, *opt.cit.*, lk 44.

2.3 Riskide realiseerumisel tekkiv vastutus

2.3.1 Vastutuse üldolemus

Üldjuhul vastutavad pooled lepingulises suhtes VÕS §-st 100 tulenevalt lepingulise kohustuse rikkumise ehk võlasuhte sisuks oleva kohustuse täitmata jätmise või mittekohase täitmise eest, sealhulgas täitmisega viivitamise eest. Vastutust võib seega defineerida kui võlausaldaja õigust kohaldada kohustust rikkunud võlgniku suhtes õiguskaitsevahendeid, tuginedes kohustuse rikkumisele.[82] VÕS-s on omaks võetud nn range vastutuse ehk garantiivastutuse kontseptsioon, mis erineb klassikalisest tsiviilõiguslikust arusaamast oluliselt. [83] Garantiivastutuse kontseptsiooni kohaselt vastutab võlgnik § 103 lg 1 alusel eelduslikult alati oma kohustuse rikkumise eest, v.a juhul, kui ta tõendab, et rikkumine on vabandatav vääramatu jõu tõttu.[84] Õiguskaitsevahendite kohaldamise eelduseks on see, et võlgnik kohustuse rikkumise eest vastutaks ning puuduvad ka vastutust välistavad asjaolud, näiteks vabandatavus § 103 mõttes. VÕS § 103 lg 1 teise lause kohaselt kehtib eeldus, et rikkumine ei ole üldjuhul vabandatav. Seega võlgniku vastutuse tõendamine kohustuse rikkumise eest ei lasu mitte võlausaldajal, vaid võlgnikul endal, kuivõrd seadusest tulenevalt kehtib eeldus, et kohustuse rikkumine ei ole vabandatav.

Enne 2010. aasta muudatusi kehtinud VÕS-i regulatsioonis oli maksevahendiga seotud vastutuse küsimus sätestatud kahes paragrahvis – § 742 sätestas maksevahendi omaja vastutuse läbi riisiko mõiste ning §-s 745 oli toodud maksekaardi väljaja ehk uue terminoloogia kohaselt makseteenuse pakkuja vastutus. 2010. aastal jõustunud muudatused täiendavad oluliselt eelmist regulatsiooni, laiendades normide sisu ning koondades kõik asjakohased sätted eraldi jaotisesse ühise pealkirja alla, mis lihtsustab seaduse sisemist struktuuri.

Makseteenuste regulatsiooni kontekstis on kehtivas seaduses vastutust mainitud VÕS-i 40. peatüki 2. jao 3. jaotises. Nimetatud jaotise terminoloogia on otsetõlkena siseriiklikkusse õigusesse üle võetud makseteenuste direktiivist 2007/64/EÜ. Ka eelmises VÕS-i regulatsioonis oli kasutusel vastutuse mõiste, kuivõrd §-i 745 aluseks oli Euroopa Komisjoni soovituse nr 97/489/EÜ artikkel 8.[85] Võttes otsetõlkena üle direktiivi mõisteaparaadi, on

[82] P. Varul jt (koost). Võlaõigusseadus I. Üldosa (§§ 1-207). Komm vlj. Tallinn: Juura 2006. V.Kõve. VÕS § 101, p 6.2.1. Edaspidi allmärkustes: VÕS I komm.
[83] V. Kõve. VÕS I komm, *opt.cit.*, § 101 / p 6.2.2.1.
[84] *Ibid*, § 101/p 6.2.2.1.
[85] Komisjoni soovitus, *opt.cit*.

seadusandja läinud kergema vastupanu teed ning kahjustades sellega õigusselgust, loonud olukorra, kus vastutuse mõistet kasutatakse sellele mitteomases kontekstis – st ei kasutata kontekstis, kus vastutus tähendab võlausaldaja õigust kohaldada kohustust rikkunud võlgniku suhtes õiguskaitsevahendeid, tuginedes kohustuse rikkumisele.[86] Eesti seadusandja eeskujulikkust direktiivi sätete praktiliselt otsesõnastuses siseriiklikkusse õigusesse ülevõtmist on täheldatud ka hindamisraportis[87], mille koostamise eesmärgiks oli hinnata liikmesriikide poolt direktiivi 2007/64 rakendamist siseriiklikkuse õigusesse. Siiski ei ole taoline otsene ülevõtmine autori hinnangul alati põhjendatud, nagu ilmneb ka nimetatud juhul mõistete ebaselguse saavutamisel.

Kehtivas VÕS-i 40. peatüki 2. jao 3. jaotises ei reguleerita vastutuse mõistega mitte seda, millal üks lepingu pool saab kasutada lepingu rikkumisele tuginedes õiguskaitsevahendeid teise lepingupoole vastu, vaid nimetatud jaotisega reguleeritakse ennekõike seda, millal makseteenuse pakkuja on või ei ole õigustatud makseteenuse kasutaja kontolt raha debiteerima. Kuigi ka nendel juhtudel võib lepingu rikkumine olla aset leidnud, ehkki tingimata ei pruugi, ei ole autori hinnangul VÕS §-des 733^1-733^3 ning 733^8 vastutuse mõistet otstarbekalt rakendatud ning seadusandja ei ole terminoloogia kasutamist läbi mõelnud. Makseteenuse osutamise lepingu sisuks § 709 lg 1 kohaselt on see, et makseteenuse pakkuja kohustub tegema maksja korraldusel maksetehinguid ning maksja kohustub maksma selle eest tasu. §-des 733^1-733^3 ning 733^8 ette nähtud nn vastutus seondub eelkõige aga autoriseerimise mõistega, ehk eelnevalt viidatud õigusega kontolt raha debiteerida. Autoriseerimata maksejuhise täitmist makseteenuse pakkuja poolt ei saa aga igas olukorras pidada automaatselt vastutuse tekkimiseks aluseks lepingu rikkumise kontekstis, kuna teatud juhtudel, nt §-s 733^8 sätestatu kohaselt kannab autoriseerimata maksete toimumise riisikot ka makseteenuse kasutaja.

Nimetatud paragrahvide sõnastus on näide sellest, kuidas seadusandja on lähtunud direktiivi 2007/64/EÜ üks-ühele ülevõtmisest Eesti õiguskorda otsetõlke kujul, ent pole seejuures arvestanud Eesti võlaõigusele omaste põhimõtetega. Ehkki igakordselt ei toimu kohaldatava normistiku valik vastutuse üldprintsiibist lähtuvalt ning teatud juhtudel määrab seadus poolte tahtest sõltumata imperatiivselt kohaldatava vastutuse ja seda ka juhul, kui lepingupool ei ole kohustust rikkunud[88], võib makseteenuste regulatsioonis nimetatud termini kontekstiväline kasutamine põhjustada tarbetut segadust. Kasutades mõisteid nende tavapärase konteksti

[86] Vt ülalt.
[87] Tipik Communications Agency. *Conformity Assessment of Directive 2007/64/EC. Estonia. July, 2011.* Available at: http://ec.europa.eu/internal_market/payments/docs/framework/transposition/estonia_en.pdf. 16.04.2015.
[88] A. Hinrikus. VÕS III komm, *opt.cit.*, § 745/p 3.1.

väliselt, saab oluliselt kannatada õigusselguse põhimõte ning sisult vastuoluliste normide sätestamine ei tohiks olla seadusandja eesmärgiks.

Kuivõrd lepingu rikkumisele järgneva vastutuse ning VÕS §-des 733^1-733^3 ning 733^8 ette nähtud vastutuse regulatsioonid erinevad üksteisest sedavõrd printsipiaalselt, tuleks seadusandjal kaaluda VÕS-s sätestatud mõisteaparaadi muutmist vastavas ulatuses.

Võrdlusena võib välja tuua Ühendkuningriikide õiguse, kus makseteenuste direktiivi 2007/64/EÜ jõustamiseks võeti vastu siseriiklik akt *the Payment Services Regulations 2009*[89], mis jõustus 1. novembril 2009. aastal.[90] Nimetatud regulatsioonis reguleerib makseteenuse pakkuja vastutust autoriseerimata maksejuhise täitmise eest artikkel 61, millises on öeldud, et kui makseteenuse pakkuja täidab maksejuhise, mis oli autoriseerimata, peab ta viivitamata hüvitama nimetatud maksega seotud kulutused ning kui see kohaldub, siis taastama maksja kontol olukorra, mis oleks olnud, kui autoriseerimata makset ei oleks toimunud. Ehkki Ühendkuningriikide vastavasisuline regulatsioon on Eesti siseriiklikest normidest lühem, jääb nende kontseptsioon põhimõtteliselt samaks.

Nagu juba lühidalt mainitud, tuleneb hetkel kehtiva maksevahenditega seonduva vastutuse regulatsioon peaasjalikult direktiivist 2007/64/EÜ. Kuivõrd makseteenuste direktiivi eesmärk on ammendavalt reguleerida makseteenuse pakkuja ja makseteenuse kasutaja vastutust, võeti direktiivi asjakohased sätted Eesti seadusesse üle tervikuna, asumata muutma vastuvõtmisele eelnenud VÕS-i redaktsiooni mitmeid põhimõtteid.[91] Direktiivis toodud regulatsiooni siseriikliku õigusega kooskõlla viimisel oli ühe variandina võimalik ka enamik direktiivist tulenevaid põhimõtteid integreerida juba kehtiva seaduse tekstiga, kaotades seejuures direktiiviga mittehaakuvad sätted. Seadusandja pidas aga regulatsiooni selguse ja arusaadavuse huvides optimaalsemaks lahenduseks asendada vastutuse regulatsiooni tervikuna.[92] Ehkki VÕS-s tehtud muudatustega ei muudetud fundamentaalselt juba kehtinud põhimõtteid vastutuse osas, ei ole ka kehtiva regulatsiooniga saavutatud seda selguse ning arusaadavuse astet, milleni seadusandja lootis jõuda. Kuivõrd seaduse mõisteaparaadi muutmisel ning täiendamisel ei mõeldud terminoloogiat korralikult läbi, on tulemuseks olukord, kus seaduse tekst kõneleb osapoolte vastutusest, ent nimetatud mõistet ei saa vaadelda ainult tavatähenduses võlaõiguse kontekstis, milleks on vastutus lepinguliste

[89] The Payment Services Regulation 2009. Entered into force 01.11.2009. Arvutivõrgus. Kättesaadav: http://www.legislation.gov.uk/uksi/2009/209/pdfs/uksi_20090209_en.pdf. 13.04.2015.
[90] Payments Council. The Payment Service Directive. Arvutivõrgus. Kättesaadav: http://www.paymentscouncil.org.uk/what_do_we_do/european_payments/the_payment_services_directive/. 13.04.2015.
[91] Seletuskiri, *opt.cit.*, lk 22.
[92] *Ibid.*

kohustuste rikkumise eest, vaid tuleb tabada selle tegelik olemus, mis jääb antud hetkel terminoloogia varju. Kuivõrd tegemist on õigusspetsiifilise küsimusega, võib taoline vahetegemine jääda õigusteadmisteta isikute jaoks ebaselgeks, mistõttu ei teeni seadus selles osas ka oma eesmärki.

Makseteenuse kasutaja kaitse efektiivsuse seisukohalt on aga VÕS-i sisseviidud muudatused regulatsiooni laiendamise kujul igati tervitatavad. Tulenevalt sellest, kas tegemist on kordumatu tunnuse alusel tehtud maksetehinguga, autoriseerimata maksega, täitmata või valesti täidetud maksega, on seadusest ilma suuremate probleemideta leitav kõnealust situatsiooni reguleeriv säte. Käesoleva magistritöö teemat silmas pidades on asjakohane tuua esile just § 733[2], mis reguleerib makseteenuse pakkuja vastutust autoriseerimata makse korral. Kuivõrd põhiliseks teenuseks, mille pärast isikud internetipanga kasutamise lepinguid makseteenuse pakkujatega sõlmivad, on maksete teostamine, siis just autoriseerimata maksete tegemise oht on internetipanga kasutamiseks vajalike maksevahendite puhul see, mis peaasjalikult identifitseerimisvahendite kuritarvitamisega selleks õigustamata isikute poolt seondub.

Eeltoodust tulenevalt on oluline pidada silmas ka autoriseerimise definitsiooni, millel autor käesoleva töö alapunktis 1.1 peatus. Nagu seal on välja toodud, tähendab autoriseerimine sisuliselt nõusoleku andmist ning kuna makseteenuste kontekstis on nende puhul praktiliselt tegemist sünonüümidega, oleks ülereguleerimise vältimise huvides mõistlik kaaluda ka võõrsõna kasutamisest loobumist ning asendamist eestikeelse nõusoleku mõistega. Võõrsõna kasutamine võib viia olukorrani, kus inimesed ei ole selle sõna tähendusest teadlikud ning sisu jääb nende jaoks arusaamatuks. Internetipanganduse poolt pakutavate teenuste kasutamisel tuleb eristada identifitseerimisprotsessi ning maksejuhise algatamise protsessi. Kui maksejuhise algatamisele eelneb identifitseerimisvahendi ehk maksevahendi kasutamine (õigete tunnuskoodide ja turvaelementide esitamine isiku tuvastamiseks makseteenuse pakkuja silmis), siis autoriseerimine on tihedalt seotud üksnes maksejuhise algatamisega. Üksnes internetipanga keskkonda sisselogimise teel ei väljenda isik enda nõusolekut kõikide esitada võivate maksejuhiste suhtes. Kui isik on end internetipanka sisse loginud ning soovib seejärel ka maksejuhist algatada, siis oma nõusoleku väljendamiseks peab ta taaskord sisestama mõne parooli oma paroolikaardilt või muu makseteenuse pakkujaga eelnevalt kokkulepitud tunnuse oma maksevahendilt. Kuivõrd elektrooniliseks maksevahendiks on ka

kaugjuurdepääsuga maksevahend[93], siis võib probleeme tekitada isiku tegeliku tahte välja selgitamine. Eemalviibijale tehtava tahteavaldusega on tegemist juhul, kui maksejuhise andmine toimub kasutades mõnda elektroonilist vahendit (nt ülekande tegemiseks internetipangas on vajalik eelnevalt arvuti või mobiiltelefoni vahendusel sisse logida), mis ei võimalda reeglina vahetut dialoogi tahteavalduse tegija (maksja) ja saaja (makseteenuse pakkuja) vahel. Sellisel juhul on maksetehingu aluse ehk maksejuhise andmise puudumise väljaselgitamine raskendatud, kuivõrd õige tunnuskoodi kasutamine ei tähenda automaatselt seda, et makseteenuse kasutaja tahteta tehtud toiming oleks õiguspärane. Ometi on see oluline elektroonilise maksevahendi kasutamisest tuleneva riisiko ja vastutuse määramisel.[94]

2.3.2 Omavastutuse ulatus

Autoriseerimata maksetehinguga kaasneda võivate riskide ning võimalike kahjulike tagajärgede vältimiseks või vähendamiseks peaks makseteenuse kasutaja olema motiveeritud teatama makseteenuse pakkujat maksevahendi väärkasutamisest esimesel võimalusel. Kuivõrd internetipangas tehtavateks toiminguteks, sh maksete tegemiseks on vajalik eelnev sisselogimine isikustatud kasutajatunnuse ning koodide alusel, seonduvad ka autoriseerimata maksega kaasnevad riskid käesoleva töö temaatikaga.

Nagu käesoleva töö alapeatükis 2.2 on autor välja toonud, on maksevahendi kaotamisest või vargusest teatamise tehniliste võimaluste loomise kohustus makseteenuse pakkujal, ning kui vastavaid lahendusi ei ole loodud, kannab kahjulike tagajärgede riisikot just makseteenuse pakkuja. Et olukorras, kus makseteenuse pakkuja on vastavad tehnilised võimalused loonud, oleks makseteenuse kasutajal teatav stiimul viimase teavitamiseks maksevahendi kaotamisest või vargusest, vähendades seeläbi autoriseerimata maksetehingute tegemise riski, peaks kasutaja vastutama üksnes piiratud summa eest, v.a juhul, kui makseteenuse kasutaja on kasutanud pettust või olnud raskelt hooletu.[95] Pärast seda, kui maksevahendi kasutaja on makseteenuse pakkujale teatanud, et maksevahend on kaotatud või varastatud ning seeläbi esineb oht maksevahendi väärkasutamiseks, ei peaks maksevahendi omajalt nõudma nende

[93] Enne 2010. aastat jõustunud seaduse redaktsioon kasutas seda mõistet, ent siinkohal aitab see avada autori mõtte sisu – internetipanga poolt pakutavate teenuste kasutamiseks peab isik kasutama teatud sidevahendeid, milleks võib olla (tahvel)arvuti või mobiiltelefon.
[94] A. Hinrikus. VÕS III komm, *opt.cit.*, § 735/p 3.2.
[95] Direktiiv 2007/64/EÜ, preambula lg 32.

edasiste kahjude kandmist, mis tulenevad kaotatud või varastatud maksevahendi autoriseerimata kasutamisest.[96]

Maksevahendi omaja omavastutuse küsimus on tihedalt seotud riisiko kandmise temaatikaga osapoolte vahel, millest autor kirjutas pikemalt töö alapeatükis 2.2. Kehtiva VÕS-i § 733[8] lg 1 sõnastusest nähtub, et maksja kannab autoriseerimata makse puhul riisikot, kui makse tegemisel on kasutatud kadunud või varastatud maksevahendit. Lisaks tuleneb normist ka nõue, et maksja kannab sellisel juhul küll riisikot, ent mitte rohkem kui maksevahendi väljajaga[97] kokkulepitud piirsumma ulatuses, kõige rohkem aga summa ulatuses, mis vastab 150 eurole.

Eelnimetatud 150 euro suurune piirmäär tuleneb makseteenuste direktiivi artiklist 61, mille kohaselt kannab makseteenuse kasutaja kuni 150 euro ulatuses autoriseerimata maksetehingutega seotud kahjusid, mis on tekkinud seoses kaotatud või varastatud makseviisi kasutamisega või seoses maksja isikustatud turvaelementide avalikuks muutumisest põhjustatud makseviisi väärkasutamisega. Maksimaalseks omavastutuse määraks, mida makseteenuse pakkuja võib teenuse kasutajalt nõuda, kui viimase maksevahend oli kaotatud või varastatud, on seega 150 eurot – kui tekkinud kahju oli suurem, peab kahju kandma makseteenuse pakkuja. Nimetatud piirmäär kuulub kohaldamisele ka olukorras, kus teenuse kasutaja maksevahendiga seotud turvaelemendid on muutunud avalikuks ning see on võimaldanud maksevahendit väärkasutada. Selle hulka kuuluvad ka internetipanga kasutamist võimaldavad identifitseerimisvahendid ja nendega seonduvad salasõnad. .

Nimetatud summalise omavastutuse piir – 150 eurot – ei ole aga summa, millise maksimaalmääras nõudmise õigus tekib makseteenuse pakkujal igal juhtumil, kui maksevahend on kaotatud või varastatud ning seeläbi on kahju tekkinud. Sätte sõnastusest ilmneb, et seadusandja sooviks nimetatud normi formuleerimisel oli eelkõige lähtuda pooltevahelises lepingus kokkulepitust. Kui aga pooltevahelises lepingus peaks nimetatud kokkulepe vastutuse piirmäära osas puuduma, on seadusandja siiski soovinud näha ette maksevahendi kasutaja kui nõrgema osapoole kaitse ja sätestanud seetõttu vastutuse piirmäära. Kui maksevahend on kaotatud või varastatud ning maksevahendi omaja on sellest ka makseteenuse pakkujat teavitanud, ent sellegipoolest on kadumise või varguse ning makseteenuse pakkuja teavitamiseni jäävas ajavahemikus kahju tekkinud, siis seaduse sätte

[96] *Ibid.*
[97] 2010. aastal jõustunud VÕS-ga muudeti oluliselt ka seni kasutusel olnud mõisteaparaati, asendades sh mõiste "maksevahendi väljaja" sõnapaariga "makseteenuse pakkuja". § 733[8] lg 1 on seejuures aga seadusandjal jäänud tähelepanuta, kuivõrd ainsa sättena seaduses on kasutusel vananenud mõistepaar. Õigusselguse huvides peaks seadusandja nimetatud ebakorrapärasuse seadusest kõrvaldama.

ega mõtte kohaselt ei ole makseteenuse pakkuja õigustatud automaatselt nõudma makseteenuse kasutajalt 150 euro suuruses summas vastutuse kandmist. Vastutuse kandmine 150 euro ulatuses sõltub eelkõige sellest, kas maksevahendi kaotamise või varastamise järgselt on üldse kahju tekkinud. Kui kahju tekkimise moment on tuvastatud, ei anna ka see asjaolu makseteenuse pakkujale õigust nõuda koheselt maksevahendi omajalt 150 eurot. Ehkki maksevahendi omaja omavastutuse maksimaalmääraks on 150 eurot, peab hüvitise suurus, mida teenuse pakkuja võib kasutajalt nõuda, olema põhjuslikus seoses kahju summaga, mis maksevahendi kaotamisest või varastamisest tekkis. Seega tuleb igal konkreetsel juhul välja selgitada, kas maksevahendi kaotamise või varguse tõttu on üldse kahju tekkinud ning kui on, siis millises ulatuses. Kui kahju suurus vastab 150 eurole või on vähemgi, siis §-s 733[8] toodud tingimuste täitmisel on makseteenuse pakkujal õigus see summa makseteenuse kasutajalt sisse nõuda, ent kui selliste tingimuste esinemisel on kahjusumma suurem, siis paraku peab makseteenuse pakkuja kahjud, mis ületavad 150 eurot, kandma ise, kuivõrd seadus ei võimalda tal makseteenuse kasutajalt üle 150 euro nõuda.

Säilitamaks juba olemasolevat ja väljakujunenud taset tarbijakaitses ning suurendamaks usaldust elektrooniliste maksevahendite ohutult kasutamise suhtes, peab liikmesriikidele olema tagatud võimalus kehtestada direktiivi normidest, sealhulgas omavastutuse piirmäära osas leebemaid eeskirju.[98] Direktiivi kohaselt peab liikmesriikidel olema võimalik vähendada maksja vastutust või vabastada maksja täielikult vabadusest, välja arvatud juhul, kui maksja on tegutsenud pettuse teel.[99]

Eesti seadusandja ei ole pidanud kehtivat VÕS regulatsiooni arvesse võttes vajalikuks kehtestada direktiivis toodust leebemaid eeskirju, kuivõrd § 733[8] lg 1 sätestab selgesõnaliselt maksja omavastutuse piirmääraks 150 eurot. Mõneti võib selline otsustus olla Eesti kodanike elatustaset arvestades olla küsitav. Arvestades mõne teise EL liikmesriigi lähenemist antud küsimusele, millest autor alljärgnevalt ka ülevaate teeb, võib kohati mõistetamatuna tunduda, miks on pidanud Eesti seadusandja vajalikuks kehtestada just maksimaalne omavastutuse piirmäär, mida direktiiv lubab. Sellele küsimusele ei leia vastust ka VÕS-i muudatusi kajastavas seletuskirjas[100], ehkki vastavasisuline analüüs võiks seal regulatsiooni selguse huvides olemas olla.

[98] Direktiiv 2007/64/EÜ, preambula lk 7, p 34.
[99] *Ibid*.
[100] Seletuskiri, *opt.cit*.

Sarnaselt seadusandjale on ka Eesti makseteenuse pakkujad[101] tüüptingimuste koostamisel lähtunud seaduses toodud sõnastusest ning mis on nende majanduslikke huvisid silmas pidades ka mõistetav. Nii Nordea pank[102] kui Swedbank[103] oma tüüptingimuste lepingutes kasutatava sõnastuse võtnud otse üle seaduse tekstist, sätestades, et kontoomaniku vastutuse piirmääraks on 150 eurot iga konto kohta, ning omavastutuse piirmäär ei kuulu kohaldamisele, kui kahju on tekkinud kontoomaniku tahtluse, raske hooletuse või pettuse tõttu. Danske Bank[104] on tingimuste sätestamisel olnud aga põhjalikum ning näinud ette regulatsiooni, mille kohaselt on omavastutuse piirsummaks pooltevahelises lepingus kokku lepitud päeva limiit iga päeva kohta kuni panga poolt teate saamiseni, et maksevahend on kadunud või varastatud, ent mitte rohkem kui summa, mis vastab 150 eurole. Sellises sõnastuses on limiidi suuruse ettenähtavuse hindamine teenuse kasutaja jaoks kõige mugavam – maksevahendi omaja on teadlik sellest, et iga päeva eest, mille jooksul ta makseteenuse pakkujat maksevahendi kaotamisest või varastamisest ei teavita, maksab ta konkreetse, eelnevalt kokku lepitud summa, ent maksimaalmäärana saab makseteenuse pakkuja temalt siiski küsida 150 eurot. Swedbank'i ning Nordea panga klientidel nimetatud kindlust teavitamiseks kuluvate päevade nö kulukuse osas ei ole, kuivõrd nende lepingus on üksnes maksimaalmäärana 150 eurot sätestatud ning kriteeriumid, mille alusel nimetatud omavastutuse summa suurus kujuneb, ei ole lepinguga reguleeritud. Ehkki makseteenuse pakkuja poolt küsitav summa ei saa baseeruda juhuslikkusel ning peab olema põhjuslikus seoses tekkinud kahjulike tagajärgedega, on makseteenuse kasutaja aspektist hinnatuna siiski aktsepteeritavam see, kui kasutajal on võimalik eelnevalt hinnata tekkida võiva omavastutuse piirmäära suurust. Selliselt lahendatuna on regulatsioon läbipaistvam ning tagab makseteenuse pakkuja vastu suurema usalduse.

Nagu autor eelnevalt mainis, on EL liikmesriigid lahendanud makseteenuste direktiivist 2007/64/EÜ tulenevat omavastutuse piirmäära kohaldamise küsimust erinevalt, nähes ette teistsuguse summa piirmäära, kui direktiiv maksimaalselt lubab. Nimetatud õigus tuleb liikmesriikidele direktiivi 2007/64/EÜ preambulast, kus on selgesõnalist ette nähtud teistsuguse summa kohaldamise võimalus.

---

[101] Antud juhul on silmas peetud Eestis tegutsevaid pankasid, kes pakuvad klientidele internetipanga kasutamise lepingu sõlmimise võimalust.

[102] Nordea pank. Telefoni- ja internetipanga tingimused eraisikule, p-d 10.3 ja 10.4. Arvutivõrgus. Kättesaadav: http://www.nordea.ee/sitemod/upload/root/content/nordea_ee_ee/eeee_private/eeee_pr_igapaevapangandus_pr/e-pangandus/TIP_tingimused.pdf. 13.04.2015. Edaspidi allmärkustes: Nordea panga leping.

[103] Swedbank'i lepingu tingimused, *opt.cit.*, p-d 8.2 ja 8.3.

[104] Danske Bank. Teleteenuste tingimused, p 9.2. Arvutivõrgus. Kättesaadav: http://www.danskebank.ee/public/terms/Teleteenused_tingimused_EST.pdf. 13.04.2015. Edaspidi allmärkustes: Danske Bank'i teleteenuste tingimused.

Ühendkuningriikide õiguses on makseteenuse kasutaja omavastutus sätestatud seaduse *the Payment Services Regulations 2009* artiklis 62, milline reguleerib, et kui maksevahend kaotatakse või varastatakse või kui maksja ei ole hoidnud maksevahendiga seotud personaalseid turvameetmeid[105] turvaliselt, on maksja omavastutuse piirmääraks kuni 50 naelsterlingit (£), kui tehtud on autoriseerimata maksetehing, mille tagajärjel tekkis kahju. Käesoleva alapeatüki kirjutamise hetkel oli Ühendkuningriikide naelsterlingi vahetuskurss Eesti Panga kodulehe andmetel 1 EUR = 0,7217 GBP.[106] Võttes arvesse eeltoodud vahetuskurssi, on ligikaudu[107] 50 naelsterlingi väärtus 70 eurot.

Seega on Ühendkuningriikide seadusandja pidanud õiglaseks vähendada võrreldes Eestis kehtiva omavastutuse piirmääraga makseteenuse kasutaja vastutust, suurendades seeläbi makseteenuse pakkuja vastutuse ulatust. Ilmselt on Ühendkuningriikide seadusandja pidanud direktiivis toodud piirmäära suurusest väiksema omavastutuse piirmäära sätestamisel vajalikuks just väljakujunenud tarbijakaitse taseme säilitamisest ning usalduse suurendamist elektrooniliste maksevahendite ohutu kasutamise suhtes, mida ei saa talle ka ette heita.

Ehkki ka Eesti õiguses ei tohiks tarbijate õigusi ja usaldust alahinnata, on autori hinnangul õigustatud seisukoht, et olukorras, kus maksevahendi omajal on füüsilise maksevahendi (või sellega seotud turvaelementide nagu PIN-koodid) üle pärast selle väljastamist põhimõtteliselt ainuisikuline kontroll, ei saa maksevahendi omaja vastutust viia minimaalsele tasemele, jättes ebaproportsionaalselt suure vastutuse makseteenuse pakkujale. Konkreetse tekkiva kahju suurus sõltub seejuures oluliselt ka kasutatava identifitseerimisvahendi liigist, kuna sõltuvalt vahendi liigist on selle kasutamiseks nähtud ette teatavad summalised piirangud. Näiteks on paroolikaartidega võimalik teha ühes kalendripäevas makseid maksimaalselt 200 euro väärtuses ning suuremate tehingute tegemiseks peab isik ent autentima teiste identifitseerimisvahenditega, nt ID-kaardi või mobiil-ID-ga.[108]

Kuigi ka 150 eurot on tänapäeval eestlase keskmist kuusissetulekut[109] hinnates suur summa, võivad autoriseerimata maksete tagajärjel tekkivad kahjud kujuneda oluliselt suuremaks, pannes seeläbi makseteenuse pakkuja rahaliselt vastutama olukorras, kus tal sisuliselt puudus

[105] Selle all on mõeldud nii maksevahendiga seotud PIN-koode kui ka kasutaja personaalset kasutajatunnust ning salasõna.
[106] Eesti Panga koduleht. Naelsterlingi vahetuskurss 14.04.2015.a seisuga. Arvutivõrgus. Kättesaadav: http://www.eestipank.ee. 15.04.2015.
[107] Täpne summa on 50 GBP = 69,280 EUR.
[108] 200 eurost päevalimiiti rakendavad paljud pangad, nt Swedbank (https://www.swedbank.ee/private/home/more/channels/internet/password) ning SEB (http://www.seb.ee/igapaevapangandus/teeninduskanalid/erakliendi-internetipank).
[109] 2014. aasta IV kvartalis oli Eesti keskmine brutokuupalk 1039 eurot. Allikas: Statistikaameti koduleht. Keskmine palk 2014. aasta IV kvartalis. Arvutivõrgus. Kättesaadav: http://www.stat.ee/13105. 13.04.2015.

võimalus tagajärgede ärahoidmiseks, kuivõrd maksevahend ja sellega seotud turvaelemendid olid maksevahendi omaja valduses ja hoole all. Autori hinnangul on küll omavastutuse piirmäära vähendamine see, mille poole Eesti seadusandja võiks püüelda, ent kõrgem piirmäär võib hetkeolukorras olla ainsaks stiimuliks, mis motiveerib maksevahendi omajaid makseteenuse pakkujat võimalikust maksevahendi kaotusest või vargusest viivitamatult teavitama. Kui autoriseerimata maksete puhul oleks makseteenuse kasutajate omavastutus piiratud üksnes 50 euroga, võib teenuse kasutajate motivatsioon makseteenuse pakkuja teavitamiseks võimalikult varases maksevahendi väärkasutamise avastamise staadiumis olla madalam kui siis, kui vastutuse piirmäär on kõrgem.

Euroopa Liidu ja Tipik *Communication Agency* koostöö raames on koostatud 26 Euroopa Liidu liikmesriikide kohta aruanded, milles hinnatakse direktiivi 2007/64 ülevõtmise vastuvõtmist direktiivi sisule. Autor võrdles siinkohal mõnede liikmesriikide sätteid, millega võeti üle direktiivi 2007/64 artikkel 61 – säte, mis kehtestab omavastutuse maksimaalmäärana 150 eurot. Võrdluse tulemusel peab autor tõdema, et enamus liikmesriike on üle võtnud direktiivi sõnastuse ning määranud ka siseriiklikus seadusandluses omavastutuse piirmääraks 150 eurot. Eranditena võib välja tuua eelnevalt nimetatud Ühendkuningriigid[110] ning Rootsi[111], viimase puhul on maksimaalmääraks seatud 1200 Rootsi krooni, mis on ligikaudu 129 eurot.[112] Küll aga ei saa vahetegu maksimaalmäärade summade vahel teha üksnes selle põhjal, milline on liikmesriigi valuuta – direktiivi ülevõtmise hetkel ei olnud eurotsooniga liitunud ka Läti, ent ka Läti on siseriiklikkuse õigusesse üle võtnud direktiivi sõnastuse, kehtestades maksimaalmääraks 150 eurot.[113]

Käesolevas alapeatükis kirjeldatud omavastutus ja selle piirmäär ei kuulu kohaldamisele aga olukordades, kus maksevahendi omaja on pooltevahelises lepingus kokkulepitud tingimuste rikkumisel, maksevahendi kaotamisel või varastamisel käitunud tahtlikult või olnud raskelt hooletu, samuti kui ta tegutses seejuures pettusega. Pikemalt analüüsib aga autor omavastutuse kohaldamata jätmise aluseid töö järgmises peatükis.

---

[110] Tipik Communications Agency. *Conformity Assessment of Directive 2007/64/EC. United Kingdom. August, 2011.* Available at: http://ec.europa.eu/internal_market/payments/docs/framework/transposition/united_kingdom_en.pdf. 16.04.2015.

[111] Tipik Communications Agency. *Conformity Assessment of Directive 2007/64/EC. Sweden. August, 2011.* Available at: http://ec.europa.eu/internal_market/payments/docs/framework/transposition/sweden_en.pdf. 16.04.2015.

[112] Eesti Panga koduleht. Rootsi krooni vahetuskurss 14.04.2015.a seisuga. Arvutivõrgus. Kättesaadav: http://www.eestipank.ee. 15.04.2015.

[113] Tipik Communications Agency. *Conformity Assessment of Directive 2007/64/EC. Latvia. August, 2011.* Available at: http://ec.europa.eu/internal_market/payments/docs/framework/transposition/latvia_en.pdf. 16.04.2015.

3. Omavastutuse kohaldamata jätmise alused

3.1 Teatamis- ja hoolsuskohustuse olemus ning selle täitmata jätmise tagajärjed

Lepingu sõlmimisel tõusetub igakordselt küsimus sellest, millest pooled üksteisele teatavad ning kas nimetatud andmetest teatamine on kohustuslik või mitte. Lisaks lepingu sõlmimiseks vajalikest andmetest teavitamisele ei ole vähem olulisem ka küsimus poolte kõrvalkohustusest, millisest üheks võib olla lepingupoole kohustus teist osapoolt teatud sündmuse esinemisel teavitada. Järgnevalt analüüsib autor teatamiskohustuse kui mõiste sisustamist ning kohaldamisala Eesti õiguses.

Et isikul oleks võimalik teha põhjendatud ning mõistlike otsuseid, on selle üheks eelduseks isiku informeeritus valitsevast olukorrast – tõese ning asjakohase informatsiooni olemasolu konkreetse olukorra kohta.[114] Euroopa lepinguõiguses tunnustatud lojaalsuse ja vastastikuse koostöö mudel on muutunud üldiselt aktsepteeritavaks käitumisstandardiks ja mõjutanud teatamiskohustuse kontseptsioonide lähenemist ka Euroopa õiguskordades. [115] Teatamiskohustuse konkreetne sisu, koht teiste kõrvalkohustuste kõrval ja teatamiskohustuse rikkumise õiguslikud tagajärjed võivad aga õigussüsteemide raames erineda,[116] samuti ei ole välistatud ka selle kohustuse tähistamine erinevate terminitega. Seega on oluline igal juhtumil eraldi hinnata, mis on konkreetse kohustuse sisuks, mitte lähtuda üksnes sõnastuse vormilisest ja välisest poolest, kuna üksnes terminist lähtumine ei pruugi viia õige järelduseni.

Vaatamata eelmainitule, ei tähenda alati erinevate terminite kasutamine seda, et kohustused oma olemuselt üksteisest väga suures mahus erineksid. Näiteks tehakse Saksa õigusdogmaatikas selget vahet selgitamiskohustusel ja informeerimis- ehk teavitamiskohustusel, teada andmise, tähelepanu juhtimise, avaldamise ning teabe jagamise kohustusel.[117] Eeltoodu annab märku sellest, et õiguskordades kasutatav terminoloogia ei ole sageli ühtne, ning sisu leidmiseks tuleb lähtuda konkreetsest lepingust. Nägemaks sarnasusi ja erinevusi erinevates õiguskordades kasutatavates mõistetes, on võimalik hinnata nende kohustuste sisulist poolt, kuivõrd üksnes mõistete alusel ei ole võimalik tabada nende tegelikku sisu.

Teatamiskohustust saab liigitada aktiivseteks ja passiivseteks ning tekkimise aja alusel kas teatamiskohustuseks enne lepingu sõlmimist, lepingu täitmise ajal või pärast lepingu

[114] I. Kull, I. Parrest. Teatamiskohustus võlaõigusseaduse kontekstis. Juridica IV 2003, lk 213. Edaspidi allmärkustes: I. Kull jt.
[115] *Ibid*.
[116] *Ibid.*
[117] *Ibid*.

täitmist.[118] Aktiivse teatamiskohustuse all tuleb mõista isiku kohustust ise teavet avaldada, samal ajal passiivse all on silmas peetud keeldu varjata teist poolt huvitavad informatsiooni.[119] Siinkohal nimetab autor kohustuse tekkimise aja alusel liigitatavat teatamiskohustust tinglikult teatamis- ning teavitamiskohustuseks, kuivõrd selline liigitus võimaldab Ühendkuningriikide ning Eesti õiguskordade võrdluse alusel kõige paremini sarnased jooned esile tuua.

Ühendkuningriikide õiguses tehakse vahet informeerimis- ning teavitamiskohustustel.[120] Kohustuste peamine erinevus seisneb selles, et millises etapis tuleb teist poolt informeerida või teavitada – nt makseteenuse pakkuja kohustus avaldada teatud info enne individuaalse makse sooritamist (art 44) või makseteenuse kasutaja kohustus teavitada teenuse pakkujat pärast mingi sündmuse toimumist (art 59). Makseteenuse lepinguga seonduv informeerimiskohustus lasub peamiselt makseteenuse pakkujal ning väljendub eelkõige selgitava info avaldamises – näiteks sätestab eelnevalt viidatud artikkel 44, et olukorras, kus maksja soovib makset teostada, peab makseteenuse pakkuja enne makse teostamist informeerima maksjat sellest, milline on maksimaalne aeg makse teostamiseks, kas soovitava tehinguga seonduvad ka mingid tehingukulud ning kui seonduvad, siis kuidas need kulud osapoolte vahel jaotuvad. Teatamiskohustus tekib Ühendkuningriikide õiguse alusel reeglina aga siis, kui maksetehing ei sujunud plaanipäraselt või maksja on avastanud mõne muu puudujäägi.[121] Sisuliselt tähendabki see makseteenuse pakkuja teavitamist mõne ebatavapärase olukorra kohta, mille täitmisega seonduvad tihtipeale ka teised õigused – näiteks peab artikli 59 kohaselt makseteenuse kasutaja viivitamatult teavitama makseteenuse pakkujat, kui saab teada tehtud autoriseerimata või valesti teostatud maksest. Eelnimetatud kohustuse täitmisest sõltub, kas tehtud tehingu eest saab vastutusele võtta makseteenuse pakkuja või on vastutajaks teenuse kasutaja.[122] Kui makseteenuse kasutaja jätab õigeaegselt makseteenuse pakkuja teavitamata, kannab ta art 59 kohaselt ise riisikot tehtud makse kahjulike tagajärgede eest.

Sarnaselt Ühendkuningriikide õigusele on ka Eesti õiguses kasutusel erinevad mõisted ehk terminoloogiliselt ei ole valdkonnale ühtselt lähenetud – kasutusel on järgmised mõisted: andmete esitamine, teavitamiskohustus ning teatamiskohustus.

[118] I. Kull jt, *opt.cit.*, lk 215.
[119] *Ibid,* lk 215-216.
[120] Vt *The Payment Services Regulation* 2009 art 44 (*obligation to provide information*) ja art 59 (*obligation to notify*).
[121] Nt *The Payment Services Regulation* 2009 art 59.
[122] Artikli 59 lg-st 1 tuleneb, et kui makseteenuse kasutaja on õigeaegselt täitnud enda teavitamise kohustuse, peab art 61 kohaselt kandma autoriseerimata tehingust tulenevad kahjud makseteenuse pakkuja.

Eesti õiguses jälgivad ka teavitamiskohustused VÕS-s kehtivat üldist struktuuri – eristada tuleb üldosa, mis kehtib kogu seaduse ulatuses ning eriosa, mis väljendab valdkonna spetsiifilisi norme. Enne lepinguliste suhete sõlmimist tuleneb osapooltele VÕS § 14 lg-st 1 kohustus arvestada üksteise huvide ja õigustega, ning lepingu sõlmimise ettevalmistamise käigus esitatavad andmed peavad olema tõesed. § 14 lg 2 lisab, et pooltel on samuti kohustus teavitada teist poolt kõigist asjaoludest, mille vastu teisel poolel on lepingu eesmärki arvestades äratuntav oluline huvi. Nagu mainitud, on nimetatud sätete kujul tegemist VÕS-i üldosast tulenevate kohustustega, millega pooled peavad igakordselt enne lepingu sõlmimist arvestama. Üksikjuhtudel aitavad nimetatud kohustuste kontrollimist täpsustada tsiviilseadustiku üldosa seaduse (TsÜS) §-s 95 toodud reeglid, mille kohaselt tuleb andmete teisele lepingupoolele esitamisel hinnata, kas asjaolu on talle ilmselt tähtis, millised on poolte eriteadmised ja võimalused ise nimetatud andmete saamiseks ja kui suured oleksid nende saamisega seonduvad kulutused. TsÜS § 95 on alus hindamaks, kas lepingu sõlmimisel poolte poolt esitatud andmed põhjustasid eksimuse või pettuse.

Eelnevalt nimetatud üldiste lepingueelsete teavitamiskohustuste spetsiifilisem vorm väljendub VÕS-i eriosas. Näiteks on selliste andmete esitamise all peetud silmas VÕS § 711 lg-st 1 tulenevaid andmeid, mille makseteenuse pakkuja peab teenuse kasutajale enne lepingu sõlmimist esitama, nt makseteenuse pakkuja nimi, osutatava teenuse kirjeldus ning maksmisele kuuluvad tasud.

Teavitamiskohustus on sisult sarnane Ühendkuningriikide õiguses kasutusel oleva informeerimiskohustusega – see seisneb eelkõige teise poole teavitamises tema õigustest ning muudatustest, mis lepinguga seonduvad – nt VÕS § 719^{1} lg 1 kohaselt peab makseteenuse pakkuja teavitama teenuse kasutajat lepingu muudatustest vähemalt 2 kuud ette. Teatamiskohustus seondub peamiselt aga poolte kõrvalkohustustega. Nt § 733^{10} p 2 kohaselt lasub makseteenuse kasutajal kohustus teatada teenuse pakkujale maksevahendi kaotamisest. Seega eksisteerivad ka Eesti õiguses erinevad teavitamiskohustused sõltuvalt sellest, millises lepingu faasis need täitmisele kuuluvad.

Eeltoodust saab järeldada, et kuigi terminoloogiliselt on eeltoodud mõisted sarnased ning võivad olla eksitavad, tähistavad nad sisu poolest erinevaid kohustusi, sõltuvalt kohustuse tekkimise ajast ning olemusest lepingus. Kuivõrd käesoleva töö teemaga haakub kõige tihedamalt teatamiskohustus, keskendubki autor alljärgnevalt peamiselt sellele kohustusele.

Teatamiskohustuse, milleks on näiteks eelnevalt mainitud maksevahendi kasutaja kohustus teavitada makseteenuse pakkujat maksevahendi kaotamisest, aluseks lepinguõiguses on

lojaalsus ja vastastikune koostöö, [123] lojaalsus omakorda on tihedalt seotud teise poole usaldamisega. Kuna teatamiskohustus on tihedalt seotud sellega, kas maksevahendi väärkasutamise järgselt kahju tekib või kui suur on selle kahju ulatus, peab pooltevaheline usaldussuhe olema mõlemapoolne, et saavutada soovitud tulemus – mõlema osapoole aktiivne tegutsemine lisaks enda huvidele ka teise lepingupoole huvides, kaitsmaks seeläbi enda huve. Vastastikuse koostöö printsiip on seega peamine, mis eelnevalt kirjeldatud usaldussuhet rakendada aitab. Teatamiskohustuse korrektne täitmine teenib mõlema osapoole huvisid – õigeaegne reageerimine tekkinud olukorrale võib aidata vältida võimaliku tekkiva kahju teket või seda vähendada.

Internetipanga identifitseerimisvahendite kasutamise kontekstis tuleb teatamiskohustus eelkõige kõne alla VÕS § 733^{10} tähenduses – identifitseerimisvahendite ebahoolas hoidmine võib viia olukorrani, kus need satuvad pahatahtlike kavatsustega isiku kätte, kes sooritab autoriseerimata makse. Kui makseteenuse kasutaja märkab makset, mis on tehtud ilma temapoolse eelneva õiguspärase autoriseerimiseta, on tal § 733^{7} kohaselt kohustus makseteenuse pakkujat sellest viivitamata teavitada. Makseteenuse kasutaja usalduse seisukohalt usaldab ta teavitamisjärgse tegutsemise kahjude ärahoidmiseks makseteenuse pakkujale, samal ajal kui makseteenuse pakkuja usaldab teenuse kasutajat selles, et viimane on maksevahendi valdamisel hoolas ning kui vaatamata rakendatud hoolsusele maksevahend kaotatakse või varastatakse, teavitab ta makseteenuse pakkujat koheselt, et viimane saaks võtta kasutusele täiendavaid meetmeid kahjude ärahoidmiseks või minimeerimiseks. Mõlemapoolsed huvid on seega võtmesõnaks, mis õigustavad makseteenuse lepingu puhul teavitamiskohustuse panemist makseteenuse kasutajale.

Lisaks teatamiskohustusele lasub makseteenuse kasutajal ka teine oluline kohustus maksevahendi valdamisel – hoolsuskohustus. Küll aga tuleb märkida, et nimetatud kohustusi ei saa üksteisest täielikult lahutada – järgnevalt analüüsimisele tulev hoolsuskohustus on tegelikult mingil määral sisse põimitud ka teatamiskohustusse, kuna nt maksevahendi varguse või kaotamise korral hinnatakse raske hooletuse kriteeriumi täitmist muuhulgas selle järgi, kui kiiresti maksevahendi omaja selle kaotamisest või varastamisest teenuse pakkujat teavitas. Raske hooletuse kriteeriumi sisustamist analüüsib autor töö 3.2.1 peatükis.

Kohustuse olla hoolas saab tuletada direktiivi 2007/64/EÜ artikkel 56 lõike 1 p-st a, mis sätestab makseteenuse kasutaja kohustuse kasutada maksevahendit kooskõlas selle väljastamisele ning kasutamisele kehtestatud tingimustega. Siseriiklikus õiguses on nimetatud

[123] A. Hinrikus. VÕS III komm, *opt.cit.*, § 741/p 3.3.

kohustus kehtestatud VÕS § 733[10] punktis 1, mille kohaselt on makseteenuse kasutaja kohustatud kasutama maksevahendit vastavalt vahendi väljastamise ja kasutamise tingimustele, muuhulgas tagama alates maksevahendi saamisest selle, et maksevahend ja selle kasutamist võimaldavad abivahendid, sealhulgas ka isikustatud turvaelemendid, oleksid hoitud kaitstuna. Siinkohal ei saa aga hoolsuskohustus tähendada seda, et makseteenuse kasutaja on pidevalt kohustatud kontrollima, kus tema kaart parasjagu on ning kas see on alles. Hoolsuskohustus seondub käibes vajaliku hoole järgimisega, mis aga oma olemuselt seondub sellega, kuidas käituks sarnases olukorras tavaline mõistlik isik (käibekohustuse sisustamisel peatub autor pikemalt töö 3.2.1. peatükis). Kuigi makseteenuse pakkujad võivad hoolsuskohustuse raames makseteenuse kasutajalt eeldada, et viimane on pidevalt teadlik sellest, kus tema identifitseerimisvahendid asuvad, ei saa nad sellele vaatamata teenuse kasutajalt nõuda, et viimane vahendi asukohta ka pidevalt kontrolliks, veendumaks, kas maksevahend tõepoolest seal asub. Kui vahendi kaotamise või varguse tagajärjel tehakse autoriseerimata makse, millest tekib kahju, siis tuleb juba eraldi analüüsida küsimust, kas makseteenuse kasutaja oli vahendi pidevalt mitte kontrollimisel raskelt hooletu või mitte.

Eelmine VÕS-i redaktsioon sätestas makseteenuse kasutaja hoolsuskohustuse põhjalikumalt, kui seda teeb kehtiv seadus. Nimelt tulenesid maksevahendi omaja kohustused VÕS § 741 lg-st 1, millise kaks esimest alapunkti on ka kehtivas seaduses olemas – nendeks on maksevahendi omaja kohustus kasutada maksevahendit vastavalt selle väljastamise ja kasutamise tingimustele ning teavitada makseteenuse pakkujat viivitamatult, kui maksevahend on kaotatud või varastatud. Kehtivast regulatsioonist on aga seadusandja poolt peetud vajalikuks kaotada § 741 lg 1 punktis 3 sätestatud reegel, millisest tulenes maksevahendi omaja kohustus mitte jäädvustada maksevahendi kasutamist võimaldavat isiklikku tunnuskoodi või muud koodi kergesti äratuntavas vormis, muuhulgas jäädvustada kood maksevahendil endal või esemel, mida ta kannab koos elektroonilise maksevahendiga. Selliselt sõnastatuna soovis seadusandja tõenäoliselt reguleerida seda, kus ja kuidas võib maksevahendi omaja enda maksevahendiga seotud tunnuskoode hoida, vältimaks olukordasid, kus kaotatud maksevahendi leidjal on tunnuskoode teades äärmiselt lihtne maksevahendit vääralt kasutada ning nii maksevahendi omajale kui makseteenuse pakkujale varalist kahju tekitada.[124]

Nagu eelnevalt mainitud, ei ole makseteenuste direktiivis 2007/64/EÜ selgesõnaliselt reguleeritud makseteenuse kasutaja hoolsuskohustust, kuid selle saab välja lugeda artikli 56 lg

[124] Ajakirjanduses on palju kirjutatud teemadel, kus inimesed on maksevahendeid koos tunnuskoodidega hoidnud ning rahakoti kaotamisel või varastamisel on tekkinud varaline kahju. Näiteks http://www.ohtuleht.ee/383105/pin-kood-pangakaardi-juures-varas-sai-saagiks-1600-krooni. 13.04.2015.

1 punkti a sõnastusest. Põhjusel, et makseteenuste direktiiv ei sätesta selgesõnaliselt maksevahendi omaja hoolsuskohustust, on ka direktiivi ülevõtmisel siseriiklikku õigusesse hoolsuskohustust puudutavaid sätteid muudetud. Kehtivas regulatsioonis on makseteenuse hoolsuskohustus reguleeritud VÕS § 733[10] punktis 1, millise kohaselt on maksevahendi omaja kohustatud kasutama maksevahendit selle väljastamise ja kasutamise tingimuste kohaselt. Kuigi üldine hoolsusstandard tuleneb VÕS-i üldosast (§ 104), ei anna see eelneva analüüsi pinnalt igakordselt piisavat alust raske hooletuse sisustamiseks. Seega näeb VÕS § 733[10] p 1 ette võimaluse makseteenuste pakkujatele sisustada hoolsuskohustus täpsemini. Nimetatud sättes väljendatud maksevahendi väljastamise ja kasutamise tingimuste reguleerimine saaks praktikas toimuda üksnes tüüptingimuste kaudu (VÕS § 35 jj) – ei ole mõeldav, et makseteenuse pakkuja koostaks igale maksevahendi omajale personaalsed tingimused, kuidas tema suhtes rakendatavat hoolsuskohustust sisustada. Kuigi printsiibis on täiendava hoolsuskohustuse sisustamise õiguse sätestamine makseteenuse pakkujatele põhjendatav, võib esiti tunduda, et regulatsioon kitsaskoht peitub selle väljendusvormis ehk tüüptingimustes – nende osas on makseteenuse kasutajal läbirääkimisvõimalused nullilähedased kui mitte olematud (VÕS § 35 lg 1). Siinkohal tulebki märkida, et ehkki seadusandja on näinud makseteenuse pakkujatele ette võimaluse teatud ulatuses hoolsuskohustuse sisustamiseks, ei ole see piiramatu õigus. Piirangud sellele seab tüüptingimuste regulatsioon – VÕS § 42 lg 1 kohaselt ei saa kehtestada selliseid hoolsusnõudeid, mis asjaolusid arvestades teist lepingupoolt ebamõistlikult kahjustaks. Autori hinnangul saab siinkohal ebamõistlikult kahjustavaks pidada selliste hoolsusnõuete kehtestamist, mis erinevad oluliselt tavakäibes isikute poolt järgitavast hoolsusest. Nimelt tuleneb viidatud sättest, et tüüptingimus on tühine, kui see kahjustab teist lepingupoolt ebamõistlikult ning ebamõistlikku kahjustamist eeldatakse, kui tüüptingimusega kaldutakse kõrvale seaduse olulisest põhimõttest.

Mõned makseteenuse pakkujad on põhjendatult pidanud siiani vajalikuks jätta makseteenuse kasutajaga sõlmitavasse lepingusse sisse klausel, mis keelab maksevahenditega kaasakantavate PIN-koodide säilitamise. Näiteks tuleneb SEB panga rahvusvahelise deebetkaardi kasutamise tingimuste punktist 3.1.1, et kaardi valdaja on kohustatud /.../ mitte jäädvustama maksevahendi PIN-koodi ühelegi andmekandjale.[125] Arvestades asjaoluga, et makseteenuse kasutaja omavastutuse piirmääraks on 150 eurot ning ülejäänud ulatuses kannab tekkinud kahju makseteenuse pakkuja, võib seadusandja soovi anda makseteenuse pakkujale suurem sõnaõigus hoolsuskohustuse sisustamisel pidada õiglaseks.

[125] SEB. Rahvusvahelise Deebetkaardi Lepingu Tingimused, p 3.1.1. Arvutivõrgus. Kättesaadav: http://www.seb.ee/files/tingimused/rahvusvahelise_deebetkaardi_tingimused_est.pdf. 13.04.2015.

Makseteenuse kasutaja hoolsuskohustuse legaaldefinitsiooni kehtivast Eesti õigusest sarnaselt direktiivile ei leia. Seetõttu tuleb hoolsuskohustuse mõistele läheneda negatiivse defineerimise kaudu, st selgitada välja hoolsuse vastandiks oleva hooletuse olemus ning seeläbi sisustada ka hoolsuskohustus.

VÕS § 104 lg 3 kohaselt on hooletus käibes vajaliku hoole järgimata jätmine. Nimetatud sättest tuleneb, et hoolsus on käibe ehk ühiskonna poolt kokkulepitud asjadesse suhtumise vorm, mis on vajalik käibe tagamiseks. Kui isiku käitumises puudub hoolsus, on tegemist selle vastandi ehk hooletusega, mis omakorda tähendab, et isik ei ole järginud ühiskonnas kokkulepitud ning aktsepteeritava hoolsuse määra. Õiguskirjanduses on leitud, et hoolsus nõuab teatud standardite järgimist – käibes ettenähtud hoolt.[126] Hoolsuse järgimata jätmine tähendab seega sisuliselt isiku poolt kohustusse suhtumist väiksema hoolsusastmega, kui temalt antud situatsioonis eeldatakse või isegi nõutakse. Hooletuse kriteerium jaguneb oma olemuselt kaheks: väliseks ehk objektiivseks ja sisemiseks ehk subjektiivseks.[127] Kuivõrd subjektiivse kriteeriumitega analüüsitakse asjaolusid, mis mõjutavad kahju tekitaja isikut[128], ei ole see makseteenuse lepingute kontektsis asjakohane – eelkõige tuleb subjektiivne kriteerium kõne alla deliktilise vastutuse puhul.[129] Seetõttu on makseteenuse kontekstis asjakohane hooletuse objektiivne aspekt, mis küsib selle järele, kas tegevus või tegevusetus objektiivses mõttes on tekitanud kahju.

Kehtivas seaduses on sätestatud regulatsioon, kus on kehtestatud teatud tasemel hoolsusstandard, mida võib pooltevahelise lepinguga konkretiseerida ning täpsustada – nagu autor eelnevalt ka mainis, on see põhjendatud, kuivõrd seaduses toodud standardid ei ole kuigi konkreetsed. Kõige selle juures on hoolsuskohustuse sisustamisel oluline silmas pidada ka seda, et ei kaldutaks kõrvale sellest, et kuidas käituks sarnases olukorras tavaline mõistlik isik – vastasel juhul oleks nimetatud tüüptingimus VÕS § 42 lg 1 kohaselt tühine. Käesoleva töö teemat silmas pidades oleks kõige mõistlikum eeldada, et makseteenuse pakkujad sätestavad maksevahendi omajatele kohustuse hoida seotud salasõnasid ja koode turvaliselt ning maksevahendist eraldi, teostada korralist järelevalvet maksevahendi üle ning võtta kasutusele meetmed, mis aitavad hoida maksevahendi kasutamiseks vajalikke sidevahendeid viirustest vabana.

Eestis tegutsevad makseteenuse pakkujad on kasutanud neile direktiiviga jäetud võimalust täpsustada osapoolte vahel sõlmitavas lepingus makseteenuse kasutaja poolset

[126] P. Schlechtriem. Võlaõigus. Üldosa II trükk. Tallinn: Juura Õigusteabe AS, 1999, lk 107.
[127] P. Schlechtriem. Võlaõigus. Eriosa. Tallinn: Juura Õigusteabe AS, 2000, lk 261.
[128] *Ibid*.
[129] V. Kõve. VÕS I komm, *opt.cit.*, § 104 p 6.2.1.

hoolsuskohustust. Nordea panga telefoni- ja internetipanga lepingus[130] on makseteenuse kasutaja hoolsuskohustuse sisuks pidada silmas järgmiseid asjaolusid:

1) kasutaja peab hoidma kasutajatunnust, koodikaardi koode ning ID-kaardi PIN-koode saladuses mistahes muude isikute eest;
2) kasutajatunnust ja koodikaarti ning ID-kaarti ja selle PIN-koode tuleb hoida teineteisest eraldi ning muudele isikutele ligipääsmatus kohas;
3) internetipanga kasutamiseks koodide sisestamisel peab kasutaja jälgima, et kõrvaline isik ei näeks sisestavaid koode;
4) kasutajatunnuse või koodikaardil toodud koodide mistahes muule isikule teatavaks saamisel või sellise ohu või kahtluse tekkimisel, samuti ID-kaardi varguse, kaotamise või muul viisil kaardikasutaja valdusest väljumise korral või selle PIN-koodi mistahes muule isiku teatavaks saamisel või sellise ohu või kahtluse tekkimisel peab kasutaja sellest kohe pangale teatama;
5) kasutaja peab panka viivitamata teavitama ebaõige kande avastamisest kontol, samuti koodide muule isikule teatavaks saamise asjaoludest.

Lisaks eelnimetatud kohustustele on SEB pank näinud enda internetipanga kasutustingimuste lepingus[131] ette veel ühe kasutajapoolse hoolsuskohustuse, mille täitmist ta nõuab. Nimelt on punkti 2.5 kohaselt makseteenuse kasutaja toimingute tegemisel turvalisuse tagamiseks kohustatud vahetama perioodiliselt paroole panga kehtestatud perioodi ja korra kohaselt. Selliselt on SEB kõrvaldanud puuduse, mis on autori poolt käesoleva töö alapunktis 1.1 toodu kohaselt jäänud Swedbank'l korrigeerimata – kui Swedbank on üksnes sätestanud klientide kohustuse ise regulaarselt pangakontorisse pöörduda paroolikaarte vahetamiseks, siis SEB panga kasutamistingimustes on reguleeritud, et teenuse kasutaja kohustub alluma paroolide vahetamisele perioodiliselt, mille näeb ette panga poolt kehtestatud kord. Autori hinnangul ei teki üldiselt eelnevalt nimetatud hoolsuskohustuste puhul küsimust nende kehtivusest, st makseteenuse pakkujad ei ole ületanud neile seadusega ette nähtud pädevust hoolsuskohustuse sisustamisel, mistõttu ei ole nende kehtivus VÕS § 42 lg 1 mõttes küsimuse all. Küll aga, laskudes detailidesse, võiks kahtluse alla seada Nordea panga tingimuse nr 2 – kohustuse hoida PIN-koode muudele isikutele ligipääsmatus kohas. Arvestades isikute praktikat salasõnade ja muude oluliste dokumentide hoiustamisel kodustes tingimustes, võib nimetatud kohustus olla liigselt koormav – näiteks on neljaliikmelise pere puhul raske leida

[130] Nordea panga leping, *opt.cit.*, p 8.
[131] SEB. Internetipanga kasutamistingimused, p 2.5. Arvutivõrgus. Kättesaadav: http://www.seb.ee/files/tingimused/u-neti_lepingu_tingimused_est.pdf. 13.04.2015. Edaspidi allmärkustes: SEB internetipanga tingimused.

kohta, mis oleks teistele isikutele ligipääsmatu (kui just igale pereliikmele ei ole eraldi seifi ette nähtud). Eeltoodust tulenevalt võib seega olla võimalik, et nimetatud tingimus on VÕS § 42 lg 1 mõistes tühine. Küllap on makseteenuse pakkuja nimetatud tingimuse sätestamisel pidanud silmas teenuse kasutaja kohustust mitte jätta salasõnasid jms selliselt ripakile, et nendele oleks kolmandatel, perekonnavälistel inimestel kerge juurdepääs. Eelnevat silmas pidades võiks makseteenuse pakkuja kaaluda tingimuse teisiti sõnastamist, mis ei oleks nii kategooriline.

Kuigi autori hinnangul on makseteenuse pakkujad hoolsuskohustuse sisustamisel oma lepingute sõnastamisel lähtunud üsna sarnastest nõuetest, on tähelepanuta jäetud mõiste viivitamata defineerimine (nt eelnevalt viidatud Nordea tingimuste p 5). Nimetatud mõiste puhul on tegemist määratlemata õigusmõistega, mille sisustamisega võivad poolte huvid probleemi korral vastanduda.[132] Siinkohal on makseteenuse pakkuja huvides eelkõige see, et makseteenuse kasutaja teavitaks teda sellel samal minutil, kui viimane maksevahendi kaotuse, varguse või autoriseerimata makse avastab. Hinnates taolist võimalust aga praktilisest aspektist, ei pruugi see makseteenuse kasutaja jaoks koheselt maksevahendiga seotud ebakorrapärasuse avastamisel võimalik olla. Sellest tulenevalt peaks makseteenuse pakkujad lähtuma esmajoones õigusselguse põhimõttest ning lisama vastavatesse sätetesse klauslid mõiste viivitamata defineerimiseks. Siinkohal tuleks aga olla ettevaatlik ning arvestada ka VÕS § 42 lg-st 1 tulenevat regulatsiooni. Nimelt ei või mõiste viivitamata sätestamisel lähtuda üksnes makseteenuse pakkuja huvidest, kuivõrd see võib § 42 lg 1 mõttes olla teist lepingupoolt ebamõistlikult kahjustav ning seega ka tühine. Mõiste võiks autori hinnangul sätestada selliselt, et makseteenuse kasutaja peab avastatud puudusest teavitama makseteenuse pakkujat viivitamata, või kui teavitamisel ilmnevad möödapääsmatud takistused, siis hiljemalt esimesel võimalusel. Sellise sõnastusega ei saa pidada makseteenuse kasutajat lepingu rikkujaks, kui ta näiteks avastab küll maksevahendi kaotamise, ent teavitab sellest makseteenuse pakkujat alles mitme tunni möödumisel, kuivõrd varasemalt puudus tal teavitamiseks võimalus – näiteks ei olnud võimalik kasutada mobiiltelefoni teate edastamiseks või pidi koheselt osalema tööga seotud üritusel ega omanud aega teate edastamiseks.

Kui aga makseteenuse kasutaja jätab talle seadusest või lepingust tuleneva teatamis- või hoolsuskohustuse täitmata, tekib küsimus sellest, et millised on kohustuse rikkumise tagajärjed. Seadus näeb ette rahaliselt mõõdetava tagajärje – VÕS § 733^8 lg 1 kohaselt

[132] Sellele, et viivitamata kui ajahetke konkreetne tuvastamine võib olla vaieldav, on viidanud ka Andrus Hinrikus: A. Hinrikus. VÕS III komm, *opt.cit.*, § 741/p 3.3.

vastutab makseteenuse kasutaja 150 euro ulatuses juhul, kui kahju tekkis makse tegemisel, kasutades varastatud või kaotatud maksevahendit, või kui maksevahendit kasutati muul viisil õigustamatult või kui maksja ei hoidnud isikustatud turvaelemente nõuetekohaselt. § 733[8] lõikes 1 määratud summaline piirmäär ei kuulu aga kohaldamisele siis, kui teenuse kasutaja rikkus tahtlikult või raske hooletuse tõttu §-st 733[10] tulenevat hoolsus- või teatamiskohustust või ta tegutses pettusega. Seega tuleneb § 733[8] lg-st 2 põhimõte, et kuna teenuse kasutajal lasub süüline vastutus maksevahendi ebaõige kasutamise tulemusel tekkinud kahju suhtes, peab just tema hüvitama kahjud ise täies ulatuses.

Siiski on seadusandja näinud ette ka teatud erisused vastutuse osas ning sätestanud juhud, mil isik vabaneb vastutuse kandmisest. Selliselt näeb VÕS § 733[9] lg 2 ette, et vastutuse kohaldamist on võimalik välistada siis, kui selle alusel esitatud nõuded tuginevad ebatavalistele ja ettenägematutele asjaoludele, mida neile asjaoludele viitaval poolel ei ole võimalik mõjutada ning mis kõikidest nende takistamiseks ettevõetud jõupingutustest hoolimata oleksid vältimatud, või kui makseteenuse pakkuja täitis seadusest tulenevat kohustust. Nagu autor käesoleva töö alapeatükis 2.3.1 põhjendab, on termini "vastutus" kohaldamine nimetatud sättes põhjendamatu, kuivõrd tegemist ei ole võlaõiguse klassikalises mõttes lepingu rikkumisest tuleneva vastutusega. Siinkohal tuleks vastutuse all mitte mõista lepingu rikkumist, vaid hoopis autoriseerimata maksete tulemusel tekkivat olukorda, mida aga ei saa reeglina lepingu rikkumiseks pidada.

VÕS § 733[9] lg-s 2 viidatud "ebatavalised ja ettenägematud asjaolud" on aga Eesti õiguses sisustamata mõisteteks, mistõttu on vaja nende sisustamiseks õigust tõlgendada või otsida abi kohtupraktikast. Kahjuks tuleb ka siinkohal nentida, et Eesti kohtupraktikas ei ole eelnimetatud mõistetele sisu antud, mistõttu tuleb läheneda nende sisustamisele analoogia ning õigustõlgendamise kasutamisega. "Ebatavaliste ja ettenägematute asjaoludega" seondub kõige lähedasema assotsiatsioonina vääramatu jõu kontseptsioon, mis tuleneb VÕS §-st 103 – vääramatu jõud on asjaolu, mille üle puudub isikul igasugune kontroll ning mõjuvõime. Kuigi VÕS § 733[9] lg 2 kasutab ka terminit asjaolud, mida ei olnud võimalik mõjutada, ei ole see kontseptuaalselt siiski võrreldav vääramatu jõu situatsiooniga. Vääramatu jõuna tuleb mõista midagi sellist, mille üle puudub isikul täielik mõjuvõim. Makseteenuste regulatsiooni puhul ei peaks aga eelnimetatud mõisteid sedavõrd kõrge standardiga siduma, kuivõrd võlasuhte olemust arvestades oleks see põhjendamatu ning lähtuda tuleks madalamast standardist. Tegemist on majandus- ja kutsetegevuses sõlmitavate lepingutega, kus pooltel on siiski teatud tasemeni võimalik hinnata tekkivaid riske ja nendega kaasnevaid tagajärgi, mistõttu VÕS §

733[9] lg-s 2 nimetatud standardi sidumine vääramatu jõu kontseptsiooniga ei oleks autori hinnangul põhjendatud.

Kõige eelneva taustal tõusetub aspektina ka küsimus sellest, et kuidas toimub omavastutuse piirmäära mittekohaldamine praktikas. Autori hinnangul on seadus üles ehitatud selliselt, et eelduse kohaselt kohaldub makseteenuse kasutaja omavastutus alati, st vaikimisi, ning kui esineb seaduses toodud alus piirmäära kohaldamata jätmiseks, peab aktiivseks pooleks olema see, kes soovib seda võimalust kasutada – selleks on makseteenuse pakkuja. Seega kui makseteenuse pakkuja leiab, et esineb alus makseteenuse kasutaja omavastutuse piirmäära kohaldamata jätmiseks, st viimane peaks tekkiva kahju osas olema täielikult vastutav, peaks piirangu kohaldamata jätmist aktiivselt taotlema just teenuse pakkuja, kes peab tõendama teenuse kasutaja poolt kohustuse rikkumise fakti ja samuti süü olemasolu vähemalt tahtluse või raske hooletuse vormis.

Eeltoodu põhjal saab kokkuvõtlikult asuda seisukohale, et makseteenuse osutamise kontekstis seondub teatamis- ning hoolsuskohustus tihedalt sellega, kas makseteenuse pakkujal on õigus rakendada omavastutuse piirmäära või on õigustatud jätta see kohaldamata. Omavastutuse piirmäära kohaldamiseks on makseteenuse kasutaja esmaseks huviks maksevahendi kaotamisel või varastamise avastamisel sellest makseteenuse pakkuja teavitamine – ehk täita korrektselt oma teatamiskohustust. Selliselt toimides saab ta ennetada olukorda, kus maksevahend satub pahatahtlike kavatsustega kolmanda isiku kätte, kes algatab õigustamatu isikuna maksejuhiseid ning tekib kahju. Samuti on ka makseteenuse pakkuja huvides olla aktiivseks pooleks olukorras, kus maksevahend on kaotatud või varastatud ning maksevahendi kasutaja ei ole sellest makseteenuse pakkujat nõuetekohaselt teavitanud. Makseteenuse pakkujal on sellisel juhul õigus taotleda omavastutuse piirmäära kohaldamata jätmist ning nõuda kõikide kahjude, mis tekivad kaotatud või varastatud maksevahendi ebaõigest kasutamisest, hüvitamist maksevahendi omaja poolt.

3.2 Valdamiskohustuste raskelt hooletu rikkumine

3.2.1 Raske hooletuse kui süü vormi hindamine siseriikliku regulatsiooni alusel

Makseteenuste direktiivi preambulast tuleneb, et väidetava hooletuse tõendeid ja selle raskusastet tuleks hinnata vastavalt siseriiklikule õigusele.[133] Tulenevalt direktiivi

[133] Direktiiv 2007/64/EÜ, lk 6.

2007/64/EÜ artikkel 61 lg-st 2 kannab makseteenuse kasutaja kõik autoriseerimata tehingutega seotud kahjud, kui need on tekkinud tema pettuse teel tegutsemise või tema ettekavatsetud käitumise või raske hooletuse tõttu. Kehtivas Eesti õiguses on sama reegel sätestatud VÕS § 733^8 lg-s 2.

Hooletuse mõiste sisustamiseks tuleb pöörduda VÕS-i poole. § 104 lg 2 kohaselt on süü vormideks hooletus, raske hooletus ja tahtlus. Kuivõrd direktiivi 2007/64/EÜ art 61 lg 2 sätestab maksja kohustuse kanda autoriseerimata tehingutega seotud kahjud juhul, kui need on tekkinud pettuse teel tegutsemise või ettekavatsetud või raske hooletuse tõttu, tuleks ka käesolevas töös analüüsida kahju tekkimist tahtluse ja raske hooletuse kontekstis. Kuna nii direktiiv kui VÕS sätestavad riisiko küsimuse kontektsis tagajärjed nii tahtlusele kui raskele hooletusele samasugustena, keskendub ka autor alljärgnevalt neist kahest problemaatilisema analüüsimisele – tahtlus on seotud subjektiivse aspektiga, ent hooletuse kui objektiivse kriteeriumi lahtimõtestamine võib kujuneda keeruliseks. Seetõttu on alljärgnevalt analüüsitud omavastutuse piirmäära kohaldamise küsimust raske hooletuse korral, ent remargi korras tuleb mainida, et sama anlüüs kohaldub ka tahtluse korral.

VÕS § 104 lg-st 4 tuleneb, et raske hooletusega on tegemist siis, kui käibes vajalikku hoolt ei ole olulisel määral järgitud. Kuivõrd käibes vajaliku hoole olulisel määral järgimata jätmine ei ole legaaldefinitsioonina seaduses avatud, tuleb leida vastus küsimusele, kuidas seda sisustada. Mõiste sisustamine on aga eelkõige igakordne tunnetuslik küsimus, mis sõltub konkreetsest olukorrast ning vähem olulisem ei ole ka vastaval majandus- või kutsealal tegutsemisel kehtivate standardite järgimine.[134] Erinevate süüvormide põhjalikult analüüsimisele on keskendunud Janno Lahe oma doktoritöös. Kuigi J. Lahe doktoritöö keskendus süüvormidele deliktiõiguses, on tema analüüsi tulemused kasutatavad ka teistes tsiviilõiguse valdkondades. Oma analüüsi tulemusel leidis J. Lahe, et raske hooletuse eristamisel kergest hooletusest tuleb silmas pidada konkreetse olukorra faktilisi asjaolusid ja püüda vastata küsimusele, kas isik on jätnud rakendamata sellised ettevaatusabinõud, mille kohaldamine tundub antud olukorras igale kahju tekitajale isiklike omaduste poolest sarnasele isikule elementaarne.[135] J. Lahe leiab, et eelnevalt püstitatud küsimusele jaatavalt vastates ongi tegemist raske hooletusega.[136] Kuigi eelnevalt kirjapandu on heaks põhjaks raske hooletuse sisustamisel, ei anna see põhjapanevat alust sellele, et igakordselt raske hooletus tuvastada. Autori arvates on vajalik rõhutada, et sellele küsimusele vastamine, kas tegemist

[134] Kull, I., Käerdi, M., Kõve, V. Võlaõigus I. Üldosa. Tallinn, 2004, lk 201.
[135] J. Lahe. Doktoritöö: Süü deliktiõiguses. Juura 2005, lk 111. Arvutivõrgus kättesaadav: http://dspace.utlib.ee/dspace/bitstream/handle/10062/686/lahejanno.pdf?sequence=5. 13.04.2015.
[136] *Ibid.*

oli raske hooletusega, on ennekõike hinnangu andmine konkreetsele olukorrale, mis sõltub oluliselt ka vastaval majandus- või kutsealal tegutsemiseks kehtivatest standarditest.

Nagu J. Lahe doktoritööst selgus, on hooletuse sisustamisel oluline kolmanda ehk mõistliku isiku arusaam hoole rakendamisest sarnases olukorras. VÕS § 104 lg-s 4 mainitud käibes vajaliku hoole all on mõeldud käibekohustust.[137] Riigikohus on leidnud, et üldine käibekohustus on tuletatav TsÜS § 138 lg-st 2[138] ning on üldise käibekohustusena sätestanud kohustuse tegutseda oma õigusi kasutades viisil, mis ei kahjusta teisi isikuid – st teha kõik mõistlikult vajalik selleks, et teised isikud ei saaks tema tegevuse tagajärjel kahjustada.[139] Tallinna Ringkonnakohus on käibekohustuse sisustamisel märkinud, et käibekohustused on inimeste kooseksisteerimise ohutuse tagamiseks kohtupraktika kaudu kehtestatavad käitumisreeglid, mille olemuslik eesmärk on piiritleda suhteid, mis väärivad vaatamata kaitsenormi puudumisele kaitset hooletu käitumise vastu ning määratleda isikute ring, keda võib pidada kahju tekitamise eest vastutavaks.[140] Käibekohustuse määratlemine kohustusena seada oma käitumine selliselt, et ta ei ohusta teiste isikute õigusi rohkem kui inimlikus kooselus vältimatu, vastab välise hoolsuse mõistele.[141] Selle all mõeldakse hoolsusnõudeid, mida õiguskord esitab isikute õigushüvede kaitsmise eesmärgil konkreetsest situatsioonist lähtudes keskmisele hoolikale isikule (VÕS § 104 lg 3).[142] Kui käibekohustust on objektiivselt rikutud, on jäänud väline hoolsus järgimata.[143]

Tuvastamaks välist hooletust, tuleb otsida vastust küsimusele, mida oleks olnud mõistlik isikult selles olukorras nõuda selleks, et ta ei oleks kahju põhjustanud.[144] Õiguskirjanduses leitakse, et objektiivse hooletuse tuvastamisel tuleb arvestada alljärgnevaga:

1) mõistliku isiku arusaamaga kahju saabumise tõenäosusest ja ähvardava ohu tõsidusega. Sellise olukorrana võiks mõista eelkõige hoolsuse tavalise määra olulist ületamist nii, et tavaline mõistlik inimene sellest ise ka aru saaks;
2) mõistliku isiku arusaamaga käitumiskohustuse olemasolust või teo õigusvastasust välistavate asjaoludega;
3) sellega, kas kahju oleks saanud ära hoida mõistlike kulutuste abil;

[137] Tallinna Ringkonna kohtu otsus 2-10-55812/27, p 42.
[138] RKTKo 3-2-1-161-12, p 10.
[139] RKTKo 3-2-1-73-13, p 10; RKTKo 3-2-1-161-12, p 10.
[140] Tallinna Ringkonna kohtu otsus 2-10-55812/27, p 42.
[141] *Ibid*.
[142] *Ibid*.
[143] *Ibid*.
[144] T. Tampuu. Deliktiõigus võlaõigusseaduses. Üldprobleemid ja delikti üldkoosseisul põhinev vastutus – Juridica II, 2003, lk 79.

4) kas kahju tekitaja järgis ohutuseeskirju.[145]

Enne makseteenuste direktiivi 2007/64/EÜ vastuvõtmist reguleeris elektroonilisi maksetehingutega seonduvat Euroopa Komisjoni soovitus 97/489/EÜ.[146] Nimetatud soovituse artikli 6 punkti 1 kohaselt seoti makseteenuse kasutaja omavastutuse piirmäära kohaldamata jätmise alus veel raskema standardiga – praeguse aluse raske hooletus (*gross negligence*) asemel nähti äärmuslik hooletus (*extreme negligence*). Tõenäoliselt oli soovituses toodud hooletuse standardi eesmärgiks veelgi enam piirata makseteenuse pakkuja pädevust otsustamisel, kuidas rikkumist kvalifitseerida ning kas rikkumine oli sedavõrd tõsine, et annab aluse teenuse kasutaja omavastutuse piirmäära kohaldamata jätmiseks.

Kui tahtlikud ning pettuslikud kontseptsioonid on reeglina üldteada, st nende avanemine ei takerdu keeruka õiguse tõlgendamise taha, seisavad ka teised riigid probleemi ees, et raske hooletuse mõiste ei ole seaduses defineeritud. Nimelt ei tulene ka Iirimaa seadusandlusest raske hooletuse (*gross negligence*) mõistet ning 2014. aastal seisis Iiri Ülemkohus esimest korda küsimuse ees, kuidas nimetatud mõistet sisustada.[147] Oma analüüsis sedastas kohus, et raske hooletuse puhul on tegemist rohkema kui lihtsalt hooletu käitumisega, mistõttu raske hooletus hõlmab endas käitumist, kus näidatakse üles tähelepanuväärset hooletuse astet.[148] Kuigi toodud otsus ei ole Ühendriikides otseselt siduv, ei ole raske hooletuse mõistet Ühendkuningriikide kohtupraktikas analüüsitud ning seetõttu on Iirimaa Ülemkohtu otsus heaks juhendmaterjaliks ka Ühendriikides.[149] Kuigi nimetatud Iirimaa Ülemkohtu lahendis tuuakse teatud vajalikud suunised raske hooletuse sisustamiseks, on siiski fakt see, et ka Iirimaal või Ühendkuningriikides ei ole ühtset alust ja printsiipi raske hooletuse sisustamiseks – kõik sõltub konkreetse kaasuse asjaoludest ning jääb kohtupraktika sisustada.

Kuigi VÕS-s on raske hooletuse mõiste §-s 104 üldjoontes avatud, sidudes selle käibes vajaliku hoole olulisel määral järgimata jätmisega, ei ole käibekohustust seaduses täpsustatud, mistõttu sarnaselt Ühendkuningriikide õigusele on ka Eestis jäänud raske hooletuse mõiste sisustamine kohtupraktika kujundada. Kui üldistes võlaõiguslikes küsimustes on raske hooletuse mõiste paljudes Riigikohtu lahendites käsitlemist leidnud, siis makseteenuse osutamise kontekstis on nimetatud praktika minimaalne. Lühiülevaate nimetatud lahenditest

[145] *Ibid*, lk 81.
[146] Komisjoni soovitus, *opt.cit*.
[147] Interpretation of Gross negligence in commercial contracts. Arvutivõrgus. Kättesaadav: http://www.walkermorris.co.uk/interpretation-gross-negligence-commercial-contracts. 13.04.2015.
[148] Eversheds. *The Meaning of Gross Negligence under the Payment Services Regulation.* Arvutivõrgus. Kättesaadav: http://www.eversheds.com/global/en/what/publications/shownews.page?News=en/ireland/the-meaning-of-gross-negligence-under-the-payment-services-regulations-march-2014. 13.04.2015.
[149] Interpretation of Gross negligence in commercial contracts. Arvutivõrgus. Kättesaadav: http://www.walkermorris.co.uk/interpretation-gross-negligence-commercial-contracts. 13.04.2015.

teeb autor järgnevas töö alapeatükis.

Kokkuvõtlikult tuleb seega raske hooletuse eristamisel kergest hooletusest lähtuda konkreetse olukorra faktilistest asjaoludest ja igakordselt püüda vastata küsimusele, kas isik on jätnud rakendamata sellised ettevaatusabinõud, mille kohaldamine tundub antud olukorras igale kahju tekitajale isiklike omaduste poolest sarnasele isikule elementaarne. Kui nimetatud küsimusele saab vastata jaatavalt, on tegemist raske hooletusega. Kuivõrd raske hooletuse kujul on tegemist määratlemata õigusmõistega, on paratamatu, et igat juhtumit tuleb eraldi hinnata.

3.2.2 Identifitseerimisvahendite raskelt hooletu valdamine

Internetipanga identifitseerimisvahendite raskelt hooletu valdamise temaatika on tihedalt seotud töö eelmises peatükis 3.2.1 käsitletud raske hooletuse mõiste sisustamisega. Kuigi eelmises peatükis analüüsis autor raske hooletuse mõiste ning rakendamise võimalusi identifitseerimisvahendite kontekstis, on teema kompaktsuse huvides mõistlik käesolevas alapeatükis tuua lühidalt välja ka temaatikaga seonduv praktiline väljund.

Direktiivi 2007/64/EÜ artikkel 56 lõike 1 punkt a sätestab, et makseteenuse kasutaja peaks kasutama makseviisi kooskõlas makseviisi väljaandmise ja kasutamise tingimustega. Sarnaselt direktiivile sätestab ka VÕS § 733[10] lg 1, et makseteenuse kasutaja peab kasutama maksevahendit selle väljastamise ja kasutamise tingimuste kohaselt, mis muuhulgas tähendab ka seda, et isik peab alates maksevahendi saamisest tegema kõik vajaliku selleks, et hoida maksevahend ja selle kasutamist võimaldavad abivahendid, sealhulgas isikustatud turvaelemendid, kaitstuna. Kaitstuna hoidmise kohustust sisustav Euroopa ja Eesti kohtupraktika ning õigusteoreetiline kirjandus on vähene.[150] Seega saab üksnes asuda seisukohale, et identifitseerimisvahendi heauskne ning korrektne valdamine selle väljastamise järgselt on makseteenuse kasutaja peamiseks kohustuseks, millise täitmise korrektsusest sõltub see, kas ja millises ulatuses kannab maksevahendi kasutaja vastutust maksevahendi kaotamise või varastamise järel tekkiva kahju eest.

Antud olukorras on sobivaks näiteks juba käesoleva töö alapeatükis 2.2 mainitud Riigikohtu lahend 3-2-1-125-08, milles kohus asus seisukohale, et maksevahendi autosse jätmist ei saa käsitleda raske hooletusena, kuivõrd maksevahendi autosse jätmisel ei rikuta tavalist hoolsuse määra nii oluliselt, et selline käitumine oleks rikkujaga sarnasele isikule mõistlikult

[150] A. Hinrikus. VÕS III komm, *opt.cit.*, § 742/p 3.4.

vastuvõtmatu – sellisel juhul võib eelkõige tegemist olla lihtsalt hooletusega.[151] Samas lahendis märkis kohus ka seda, et maksevahendi autosse jätmisel võib isik olla käitunud raskelt hooletult juhul, kui lisanduvad muud asjaolud, näiteks see, et koos maksevahendiga hoiti ka selle kasutamist võimaldavat PIN-koodi või kui auto jäetakse lukustamata asjaoludel, mille esinemisel rikkujaga sarnane isik autot lukustamata ei jätaks.[152] Kuigi ka autori hinnangul ei ole maksevahendi autosse jätmise kujul tegemist sedavõrd olulise hoolsusmäära rikkumisega, et seda tuleks käsitleda raskelt hooletu käitumisena, ei saa siiski olla aktsepteeritav olukord, kus isik jätab rahvarohkesse kohta pargitud autosse maksevahendi nähtavale kohale. Sellise käitumisviisi puhul tuleks autori hinnangul rasket hooletust pigem jaatada, isegi kui kasutamist võimaldavaid salasõnad jms koos kaardiga ei ole. Nagu autor eelnevalt ka sedastas, on raske hooletuse tuvastamine pigem tunnetuslik küsimus, mis sõltub igal konkreetsel juhtumil esinevatest asjaoludest.

Seega võib asuda seisukohale, et maksevahendi väljastamise järgselt on selle valdamise kohustus pandud makseteenuse kasutajale, kes peab seejuures valdamisel järgima temalt käibes nõutud vajalikku hoolsust. See, kas maksevahendit on vallatud hooletult või raskelt hooletult, sõltub igal konkreetsel juhul kaasuse asjaoludest.

3.2.3 Infotehnoloogiliste vahendite raskelt hooletu valdamine

Maksevahendi kui identifitseerimisvahendi kõrval on oluline ka küsimus maksevahendi kasutamist võimaldava infotehnoloogiliste vahendite valdamisest – antud teema kontekstis on oluline pidada silmas ka nende abivahendite valdamise küsimust, mis teevad võimalikuks identifitseerimisvahendite otstarbelise kasutamise. Internetipanka sisselogimiseks vajalikke maksevahendeid saab eesmärgipäraselt kasutada ning seeläbi omavad nad kasutegurit vaid siis, kui teenust kasutada soovival isikul on olemas teenuse tarbimiseks nõutavad infotehnoloogilised vahendid – olgu selleks siis arvuti, mobiiltelefon või muu tehnoloogiline seade. Identifitseerimisvahendi puhul on võimalik isiku pangakontol olevat raha käsutada pärast tuvastamisprotsessi läbiviimist ehk internetikeskkonda sisse logimist, mis aga toimub sidekanali või muu elektroonilise seadme vahendusel.[153] Eeltoodust tulenevalt on oluline ka elektroonilise maksevahendi abil tehingute teostamiseks kasutatavate IT-süsteemide ja -seadmete turvalisus.[154] Elektroonilise maksevahendi olemust kui vahendit, mille vahendusel

[151] RKTKo 3-2-1-125-08, p 13.
[152] *Ibid.*
[153] A. Hinrikus. VÕS III komm, *opt.cit.*, § 741/p 3.2.2.
[154] *Ibid.*

on selle omajal võimalik teha sidekanalite vahendusel või muul viisil elektroonilisi ülekandeid, on oma otsuses sedastanud ka Riigikohus.[155]

Enne infotehnoloogiliste vahendite valdamise küsimuse juurde minemist on oluline peatuda ka elektroonilise maksevahendi abivahendite olemusel kui sellisel. Makseteenuste direktiivi 2007/64/EÜ ülevõtmise kohta Eesti siseriiklikku õigusesse koostatud seletuskirjast tuleneb, et elektroonilise maksevahendi abivahendiks on isiklik tunnuskood, muu kood või ka seade elektroonilise maksevahendi kasutamiseks.[156] Seega identifitseerimisvahendite puhul on lisaks tehnoloogilistele vahenditele oluline ka identifitseerimisvahendi kasutamist otseselt võimaldav tunnuskood, milleks on reeglina kasutajatunnus, salasõna või nende kombinatsioon. Taoline abivahend on oluline isiku tuvastamiseks internetipanga poolt pakutavate teenuste tarbimiseks – väljendamaks oma soovi teenuse kasutamiseks, sisestab isik oma kordumatu kasutajatunnuse ja / või –paroolid ning koodi identifitseerimisvahendilt. Kuivõrd internetipangas kasutatavate identifitseerimisvahendite kujul on tegemist maksevahendi kui sellisega, on nendega seotud abivahenditele peetud lisaks silmas ka erinevaid infotehnoloogilisi süsteeme ning seadmeid.

Isiku tahte korrektseks tuvastamiseks eesmärgiga tagada õigesti autoriseeritud teenuse kasutamine, on oluline, et tuvastamisprotsessis kasutatavate IT-süsteemide ning vastavate – seadmete turvalisus oleks tagatud. Siinkohal tuleb kahel eelnevalt nimetatul teha vahet, kuivõrd makseteenuse pakkuja ei oma kontrolli teenuse kasutaja poolt kasutatavate seadmete üle ning teenuse kasutaja omakorda ei saa mõjutada teenuse pakkuja poolt kasutusele võetud süsteemide turvalisust.

Kuigi maksevahendi olemust ja sellega seonduvaid turvariske arvestades võiks seda eeldada, ei sätesta sellegipoolest direktiiv ega ka siseriiklik regulatsioon otseselt osapoolte kohustust kasutada identifitseerimisprotsessi jaoks turvalisi seadmeid ning süsteemlahendusi. Kuna õigusaktides ei ole nimetatud kohustust reguleeritud, ei ole ka makseteenuse pakkujale pandud VÕS-i tasandil sõnaselget kohustust luua identifitseerimisvahendite kasutamiseks turvaline süsteemlahendus, mis võimaldaks välistada autoriseerimata tehingute tegemist. Kuigi ebakvaliteetse ning –turvalise teenuse osutamine ei ole loodetavasti ühegi makseteenuse pakkuja huviks, võiks makseteenuse osutamisega seonduvaid riske silmas pidades nimetatud kohustuse siiski seadusesse sisse kirjutada. Vastasel korral ei oma piisavalt efektiivset kaitset suhte teine osapool ehk makseteenuse kasutaja, kuivõrd olukorras, kus makseteenuse pakkuja ei ole võimaldanud omalt poolt turvalist IT-süsteemlahendust

[155] RKTKo, p 14.
[156] Seletuskiri, *opt.cit.*, lk 45.

identifitseerimisvahendite kasutamisel, ei ole teenuse kasutajal võimalik end olemasolevate ressurssidega kaitsta.

Siiski ei ole nimetatud abivahendite kasutamine täiesti reguleerimata küsimus. Makseteenuse kasutaja kohustuse kasutada turvalisi elektroonilisi seadmeid identifitseerimisprotsessi jooksul tuleneb kõige üldisemalt võttes lepingulise suhte iseloomust; seaduse tasandil võib selle nõude aga tuletada VÕS § 733[10] punktist 1. Nimelt näeb säte ette, et maksevahendi omaja on kohustatud kasutama maksevahendit selle väljastamise ja kasutamise tingimuste kohaselt, muu hulgas tegema alates maksevahendi saamisest kõik vajaliku, et hoida maksevahend ja selle kasutamist võimaldavad abivahendid, sh isikustatud turvaelemendid, kaitstuna. Ehkki nimetatud sättes on turvaelemendid eraldi välja toodud, kuulub maksevahendi kasutamist võimaldavate abivahendite hulka ka arvuti või mobiiltelefon, mille vahendusel isik internetipanka siseneda soovib.

Tekib küsimus sellest, mis tähendab lausefraas "hoida abivahendid kaitstuna". Tänapäeva infotehnoloogilises ühiskonnas võib erialateadmiseid omamata olla sellele küsimusele vastamine raskendatud. Üldsõnaliselt öelduna on nimetatud fraasiga peetud silmas ilmselt olukorda, kus makseteenuse kasutaja kasutab oma abivahendi – milleks võib näiteks olla arvuti, mobiiltelefon või tahvelarvuti – kaitsmiseks vastavaid viiruse- ning nuhkvaravastaseid tarkvarasid ning tulemüüre[157], mis tegelevad viiruste tuvastamise ja eemaletõrjumisega elektroonilistest sidevahenditest. Samuti võiks teenuse pakkuja huvides kuuluda makseteenuse kasutaja hoolsuskohustuse alla ka kahtlastel internetilehekülgedel mittekäimine või kahtlase sisuga tunduvate e-kirjade mitteavamine, kuivõrd ka eelnimetatud võivad kanda endas mitmeid arvuti tarkvarale ohtlikke viiruseid. Siinkohal lasuks aga raskuspunkt sellel, et kuidas sisustada ning tõlgendada mõistet "kahtlane". Selge on aga see, et ei piisa üksnes viiruste- ning nuhkvaravastaste tarkvarade ning tulemüüride paigaldamisest elektroonilisele sidevahendile, vaid isik peab nimetatud vahendit kasutades ka ise pidevalt hoolsust üles näitama ning mitte avama tundmatutelt aadressidelt saadetud ning kahtlase sisuga tunduvaid e-kirju – hinnangu külastatavate lehtede või avatavate kirjamanuste turvalisusele saab anda üksnes makseteenuse kasutaja ise. Kuigi nimetatud hinnangu annab makseteenuse kasutaja, tuleb ka selles küsimuses hoolsuse hindamisel pöörduda küsimuse juurde, et kuidas oleks sarnases olukorras käitunud tavaline mõistlik isik – kas kõike arvestades tema oleks kõnealust veebilehte külastanud või e-kirja avanud. Lõppastmes peaks ka teenuse kasutaja enda huvides teha kõik võimalik, hoidmaks enda rahakontod turvalisena.

[157] Swedbank. Internetipanga turvalisus. Arvutivõrgus. Kättesaadav: https://www.swedbank.ee/private/home/security/security?language=EST. 13.04.2015.

Sarnastele ohtudele on tähelepanu juhitud ka Euroopa Liidu tarbija nõustamiskeskuse kodulehel, kus tarbijaid hoiatatakse nn phishingu eest.[158] Phishingu puhul on tegemist olukorraga, kus saabunud kiri oleks justkui saadetud isiku enda panga poolt ning mis innustab avama kirjale juurde lisatud linki, nõudes seejuures sisestama pangakonto detailseid andmeid, näiteks paroole.[159] Lingil klikkides avanevad lehed on sageli identsed isiku enda panga internetikeskkonnale, mistõttu inimesed ei panegi tihtipeale tähele, et nad ei viibi tegelikult turvalises internetikeskkonnas.[160] Phishingu jaoks loodud kodulehed on väga kavalalt üles ehitatud ning personaalsete andmete sissetrükkimine sellisel lehel võib halvimal juhul kaasa tuua isiku pangakonto tühjendamise, kuivõrd lingile klikkides võib isik anda nõusoleku sellise programmi installeerimisele arvutisse, mis salvestab kasutaja erinevaid paroole ning saadab need petturitele.[161]

Seega olukorras, kus arvuti ei ole piisaval määral kaitstud või isik ise avab tundmatu sisuga e-kirju, on arvuti kaudu sisestatavad identifitseerimisvahendi koodid või salasõnad selgelt kaitsmata. Makseteenuse kasutaja vastutuse sellises olukorras võib, nagu ülalpool ka mainitud, kaudselt tuletada VÕS § 733[10] punktist 1, ent sama säte jätab oma sõnastuse poolest võimaluse ka makseteenuse pakkujal nimetatud vastutust reguleerida.

Nii mõnigi makseteenuse pakkuja on lepingus, mille ta makseteenuse kasutajaga sõlmib, näinud viimasele eraldi ette kohustuse identifitseerimisvahendite kasutamisel olla hoolas ka abivahendite kasutamisel. Näiteks on Swedbank'i teleteenuste lepingu tingimustes ette nähtud, et makseteenuse kasutaja vastutab teleteenuste, sh internetipanga teenuste kasutamiseks kasutatavate sidevahendite (sh arvuti, interneti- ja telefoniühenduse) turvalisuse ja toimimise eest.[162] Nõutud turvalisust ning sidevahendite toimimist saabki teleteenuse kasutaja saavutada eelkõige seeläbi, et paigaldab oma sidevahenditele vajalikud viiruse- ning nuhkvaravastased tarkvaralahendused, mis takistavad sidevahendi nakatumist mõnda viirusesse, mis omakorda võimaldaks takistada tema sidevahendi abil sisestatud paroole petturitele edastamast. Sarnased nõuded sidevahendite turvalisuse tagamiseks on ette näinud ka Danske Bank.[163] Nordea panga telefoni- ja internetipanga lepingus[164] nimetatud kohustust reguleeritud pole ning ka SEB panga internetipanga kasutustingimustes ei ole selgesõnaliselt

[158] Euroopa Liidu tarbija nõustamiskeskus. Ettevaatust pettusskeemidega! Arvutivõrgus. Kättesaadav: http://www.consumer.ee/scam/. 13.04.2015.
[159] *Ibid.*
[160] *Ibid.*
[161] *Ibid.*
[162] Swedbanki lepingu tingimused, *opt.cit.*, p 3.2.
[163] Danske Bank'i teleteenuste tingimused, *opt.cit.*, p 2.
[164] Nordea panga leping, *opt.cit*.

määratud teenuse kasutaja kohustust kasutada identifitseerimisprotsessi ja internetipanga teenuste tarbimisel panga poolt kehtestatud turvanõuetele vastavaid sidevahendeid.[165]

Arvestades tänapäeva infotehnoloogia arengut ja küberkuritegevuse kiiret kasvutrendi ning kurjategijate nutikust andmete kopeerimisel, ei ole autori hinnangul makseteenuste pakkujate poolt kehtestatud turvanõuete järgimise kohustus põhjendamatu. Kujuneks üsnagi ebaõiglane olukord, kui makseteenuste pakkujatel puuduks võimalus kasutajate poolt kasutatavatele sidevahenditele turvanõuete ettekirjutamiseks, ent teiselt poolt jäetakse vastutus varalise kahju eest, mis ületab teenuse kasutaja omavastutuse piirmäära, makseteenuse pakkuja kanda.

Seejuures ei saa aga makseteenuse pakkujate poolt sätestatud tingimused turvameetmete rakendamiseks olla põhjendamatult ranged ning jätta kõik turvameetmete kasutamisega seotud riskid täies ulatuses maksevahendi kasutaja kanda. Swedbank'i teleteenuste lepingu kohaselt peavad teenuse kasutaja sidevahendid ja –ühendused vastama tehnilistele nõuetele, mille pank on kehtestanud. Nimetatud nõudeid aga lepingus eraldi ei ole välja toodud ning teenuse kasutaja peab selleks minema eraldi panga kodulehele. Selliselt on pank soovinud tõenäoliselt ennetada olukorda, kus ta peab turvanõuete muutmiseks hakkama eraldi muutma ka iga kliendiga sõlmitud lepinguid. Panga kodulehelt leitavad, pangapoolt kehtestatud nõuded näevad ette, et makseteenuse kasutaja peab turvalisuse tagamiseks tegutsema järgmiselt:

1) kasutama võimalikult uut brauserit ning operatsioonisüsteemi;
2) seadma brauseri ning operatsioonisüsteemi turvalisse režiimi ning tegema korrapäraseid uuendusi;
3) installeerima viirustõrjetarkvara;
4) kontrollima arvutit ning uuendama tarkvara regulaarselt;
5) mitte avama kahtlaseid faile.[166]

Eeltoodud nõudeid ei ole objektiivselt vaadatuna küll põhjendamatud ning tegemist ei ole ka makseteenuse kasutajat liigselt koormavate tingimustega, ent tavatarbijal võib sellele vaatamata tekkida olukord, kus tema teadmised operatsioonisüsteemide valimisel ning viirustõrjetarkvara installeerimisel jäävad puudulikuks. Kui identifitseerimisvahendite ja sidevahendite kasutamise järgselt tekib kahju ning makseteenuse pakkujal on võimalik tõendada, et makseteenuse kasutaja ei olnud järginud panga poolt esitatud turvanõudeid, rikkudes seejuures lepingut raskelt hooletuna, on makseteenuse pakkujal seetõttu õigus jätta

[165] SEB internetipanga tingimused, *opt.cit*.
[166] Swedbank. Kaitske oma arvutit. Arvutivõrgus. Kättesaadav: https://www.swedbank.ee/private/home/security/security?language=EST. 13.04.2015.

omavastutuse piirmäär kohaldamata ning nõuda teenuse kasutajalt kahju hüvitamist täies ulatuses. Küsimus on aga nimetatud tingimuste kehtivusest VÕS § 42 lg 1 tähenduses. Kuigi autor tõi eelnevalt miinuskohana välja, et makseteenuse kasutajate teadmised võivad operatsioonisüsteemide ja viirustõrjetarkvara valdkondades puudulikud olla, ei ole nimetatud tingimused tõenäoliselt § 42 lg 1 regulatsiooni mõttes tühised. Kuna maksevahendi ja selle kasutamiseks vajalike elektrooniliste maksevahendite valdamine on täielikult ning ainuisikuliselt makseteenuse kasutaja valduses, ei saa pidada ebamõistlikuks seda, et makseteenuse pakkuja on eelnevalt väljatoodud kujul proovinud teenuse kasutaja käitumisele kohalduvat hoolsuskohustust konkretiseerida, nähes ette kohustuse uuendada veebibrauserit, kasutada viirustõrjetarkvara ning mitte avama kahtlaseid faile. Nimetatud kohustusi täidaks ka tavaline mõistlik isik antud olukorras, milleks oleks tema enese rahaliste vahendite kaitsmine internetipangas.

Selliste maksevahendite puhul, mis ei eksisteeri füüsiliselt – ning nende hulka kuulub ka internetipangandus – on hoolas käitumine keerulisem ja võib eeldada, et paljudel tarbijatel on selles küsimuses vähe vajalikke teadmisi.[167] Seetõttu võib tõusetuda küsimus sellest, kas seadusandja peaks seaduse tasandil sätestama miinimumnõuded, mis reguleeriks maksevahendi abil toimingute tegemiseks kasutatavate sidevahendite ning nendega koos kasutatavate viirus- ning nuhkvaravastaste tarkvaradele esitatavaid nõudeid. Sellesisulise sätte formuleerimine seaduses oleks tänapäeva kiirelt arenevat infotehnoloogia valdkonda arvestades kahtlemata keeruline ülesanne – see, mida konkreetsel ajahetkel peetakse antud valdkonnas mõistlikuks ning asjakohaseks nt arvuti hoidmisel viirustest vabana, võib juba järgmisel hetkel olla kardinaalselt muutunud ning ei oleks enam asjakohane. Seega oleks hoolsuskohustuse spetsiifilisem reguleerimine seaduse tasandil (st pooltevahelise lepingu asemel) pigem välistatud. Hoolsuskohustuse kriteeriumite sätestamine pooltevahelises lepingus on seega põhjendatud, kuna lepingutingimuste uuendamine ning kaasajastamine on tunduvalt kergem protsess kui pidev seaduste muutmine – viimase puhul saaks tugevalt kannatada ka õigusselguse põhimõte. Nagu eelnevalt mainitud, on makseteenuse kasutaja kaitseks sellises olukorras VÕS § 42 lg 1 – makseteenuse pakkuja poolt sätestatud kriteeriumid peavad siiski järgima seaduses ette nähtud standardeid käibes vajaliku hoole järgimise osas.

Seega kui makseteenuse pakkuja soovib, et teenuse kasutaja suhtes rakenduks spetsiifilisem hoolsuskohustus, kui seda näeb ette seadus, peab ta vastavad kriteeriumid ka tüüptingimustes

[167] T. Runnel, *opt.cit.*, lk 367.

sätestama. Kui ta seda ei tee, peab ta arvestama sellega, et lepingulisele suhtele rakendub üldine, seadusest tulenev hoolsuskohustus, mille kriteeriumid on aga suhteliselt madalad.

Nagu mainitud, peavad makseteenuse pakkujad hoolsuskohustuse sisustamisel siiski lähtuma ka seaduses toodud piirangutest – sätestatavad kohustused ei tohi vastuollu minna sellega, mida võiks nõuda sarnases olukorras tavaliselt mõistlikult isikult; vastasel korral on tingimus tühine. Kui makseteenuse pakkuja sätestab näiteks sedavõrd kõrged turvaohutusnõuded – kohustus kasutada igal ajal ainult kõige uuemat ning parimat viirustõrjeprogrammi, mis juhtumisi on ka tasuline – ja mille igasugune ning väiksemgi eiramine või rikkumine tooks kaasa makseteenuse pakkuja vastutusest vabanemise ning paneb vastutuse omakorda makseteenuse kasutajale, oleks tingimus VÕS § 42 lg 1 alusel tühine. Ehkki makseteenuse pakkujad (nt Swedbank) pakuvad võimalust osta nende poolt aktsepteeritavat turvalahendust oma koostööpartneritelt, ei saa olla õiguspärane olukord, kus makseteenuse kasutaja pannakse sundolukorda sõlmida lisatasu eest koostööleping makseteenuse pakkuja turvalahenduste saamiseks, kui kasutaja enda teadmised lepingus nõutud turvalisuse saavutamiseks ei ole piisavad.

Analoogia korras saab hooletu käitumisena käsitleda ka maksevahendi kasutamist sellise sidevahendi abil, millisel pole turvanõudeid järgitud, see on viirusega nakatanud ning maksevahendi kasutaja jätkab sellele vaatamata teenuse kasutamisega. Ehkki eelpool nägi autor ebaõiglust olukorras, kus makseteenuse kasutaja pannakse tekkinud kahjude eest vastutama situatsioonis, kus kahju tekkis turvanõuetele mittevastavat sidevahendit kasutades, on vastutuse tekkimise aluseks kehtiva VÕS regulatsiooni kohaselt nõue, et kasutaja käitus seejuures raskelt hooletult. Seetõttu kannab riisikot makseteenuse pakkuja seni, kuni tal õnnestub tõendada, et makseteenuse kasutaja oli viirusega nakatunud sidevahendi kasutamisel rakselt hooletu, kuivõrd üksnes kergest hooletusest selleks ei piisa. Autori hinnangul ei ole sellist piiri hooletuse astmete vahel kerge tõmmata, ent olukorras, kus sidevahendi kasutamisel esines mitmeid ohumärke (nt teavitas arvuti selle kasutajat, et arvutil olevad ohutust tagavad tarkvarad on aegunud), kuid kasutaja logis sellele vaatamata identifitseerimisvahendite abil internetipanka, tuleks kasutaja rasket hooletust jaatada – ohumärgid olid talle nähtavad, ent ta otsustas neid sellele vaatamata ignoreerida.

Kahetsusväärselt puudub Eestis kohtupraktika sellel teemal, kus sidevahendi omanik on pandud vastutama oma kaitsmata arvutist lähtuva ründe eest. Seega Eesti kohtupraktikas on sisuliselt antud küberprobleemi korral lahendamata küsimus, kust jookseb piir hooletuse ning raske hooletuse vahel.

Arvutis kõige uuema ning kaasaegsema turvalahenduse kasutamine on seotud mitmete kulutustega, kuivõrd reeglina ei ole väga heal tasemel viirustõrjeprogrammid vabavarana tasuta saadaval. Tuvastamaks makseteenuse kasutaja rasket hooletust abivahendi valdamisel, ei piisa üksnes väitest, et isik on käitunud raskelt hooletult seetõttu, et ei ole oma sidevahendis kasutanud kõige uuemat saadaolevat tarkvara või ei ole tähele pannud, et tema poolt kasutataval arvutil nimetatud tarkvara puudub / on aegunud. Makseteenuse pakkuja ei saa panna makseteenuse kasutajale kohustust kasutada vaid kõige uuemat ning kallimat turvalahendust. Samas on mõistetav ka see, et mitte iga turvalahendus ei paku kaitset nende ohtude eest, mis internetipanganduse kasutamisega kaasnevad. Kuigi makseteenuse kasutaja usaldab makseteenuse pakkuja valdusesse oma vara ning usaldab, et teenuse pakkuja teeb kõik, et vara oleks kaitstud, ei tähenda see seda, et makseteenuse kasutaja ise ei pea oma vara säilimise nimel enam pingutama. Makseteenuse pakkujate poolt sätestatavates tüüptingimuste regulatsioonis võiks VÕS § 42 lg-st 1 tulenevaid piiranguid silmas pidades kehtestada sellised miinimumnõuded, mis oleksid asjakohased ja mõistlikud ning mida makseteenuse kasutajalt oodata saab, kuivõrd siis oleks üheselt pandud paika need piirid, millest nõrgemaid turvalahendusi maksevahendi omaja kasutada ei või. Nimetatud nõuded ei saa oma sisult aga olla kuigi konkreetsed, vaid need üksnes sätestaksid üldkriteeriumid sidevahendite kasutamisele, kuivõrd tänapäeva pidevalt muutuvas tehnoloogilises ühiskonnas ei ole rangete kriteeriumite sätestamine ratsionaalne. Taoliste kriteeriumite sätestamist kergendaks ka piisava kohtupraktika olemasolu, ent antud hetkel see Eestis puudub.

Võttes arvesse tehnoloogiliste seadmete ja sidevahendite osatähtsust identifitseerimisvahendite kui maksevahendite realiseerimisel, jätavad nii VÕS-i kui direktiivi 2007/64/EÜ regulatsioonid nii makseteenuse pakkujale, aga ka makseteenuse kasutajale suure riski. Kuigi seadusandja on põhjendatult pidanud vajalikuks anda makseteenuse pakkujatele võimalus hoolsuskohustuse sisustamiseks makseteenuse lepingutes, ei oma nad seejuures täiesti vaba voli tingimuste kehtestamisel. Nimetatud kohustuste sätestamisel peavad nad järgima VÕS-i üldosas kehtestatud tüüptingimuste regulatsiooni, kuivõrd hoolsuskohustused kehtestatakse kõige tõenäolisemalt just tüüptingimuste vormis. Seega on oluline, et kohustuste sätestamisel ei tohi oluliselt kõrvale kalduda seaduse nõuetest ehk käibekohustuse sisust – kehtestatavad kohustused peavad mõistlikuna tunduma ka tavalisele kõrvalisele mõistlikule isikule. Kui makseteenuse pakkujad nimetatud kriteeriume ületavad ning kehtestavad oluliselt rangemad hoolsuskohustused, kui seda seadus lubab, on need VÕS § 42 lg 1 alusel tühised ning tagajärjena kuulub kohaldamisele seadusest tulenev hoolsuskohustuse standard. Võrreldes aga nende kohustustega, mis makseteenuse pakkujatel on võimalik kehtestada, on seadusest tulenev standard oluliselt madalam, st makseteenuse kasutaja kasuks.

Kokkuvõte

Magistritöö sissejuhatuses püstitatud uurimiseesmärkideks oli käesolevas töös analüüsida, kas 2010. aastal VÕS-i sisse viidud muudatused parandasid regulatsiooni lisaks vormilistele muudatustele ka sisuliselt ja aitasid seda täiustada ning seda, kas uuenenud normide alusel on osapoolte vahel jagunenud vastutuse ulatus õiglane ja poolte huvid piisavalt kaitstud. Seda tehes soovis autor samuti leida vastuse küsimusele, kas makseteenuse lepingute kontekstis saab teenuse kasutajat pidada lepingupoole nõrgemaks pooleks ning kui saab, siis kas seadusandja on arvestastanud tema huvidega vastutuse regulatsiooni sätestamisel. Nimetatud VÕS-i normide muutmine on kindlasti oluline Euroopa Liidu lepinguõiguse ühtlustamise seisukohalt, samas tuleks seejuures hinnata regulatsiooni muudatusest tulenevat mõju siseriiklikule õiguskorrale selle iseärasusi arvesse võttes. Arvestades eelnevat, oli töö eesmärkide seadmisel autori hinnangul küsitav, kas Eesti seadusandja tegutses nimetatud VÕS-i muudatuse sisseviimisel mõlema osapoole parimaid huvisid silmas pidades.

Vastavalt töö sissejuhatuses märgitule, jõustus muudetud kujul VÕS 22. jaanuaril 2010. aastal. Nimetatud muutmise vajaduse tingis eelkõige makseteenuste direktiivi 2007/64/EÜ ülevõtmise kohustus Eesti siseriiklikusse õigusesse, millise kujul oli tegemist Euroopa Liidu tasemel senikehtinud õiguse uuendamise ning kaasajastamisega. Makseteenuste direktiivi rakendamine liikmesriikide siseriiklikku õigusesse oli kohustuslik kõikidele liikmetele. Nimetatud direktiivi vastuvõtmise peamised eesmärgid võib välja tuua järgnevalt:

1) EL tasandil ühtse makseturu loomine ehk ühendada liikmesriikide erinevad rahvuslikud maksete teostamise süsteemid;
2) ühtse makseturu loomise kaudu luua EL-i ülene makseteenuste õiguslik raamistik, mis tagaks võrdsed võimalused kõikidele maksesüsteemidele;
3) suurendada tarbijate usaldust ja tõhustada nende kaitset läbi ühtsete makseteenuse pakkumise ja maksete teostamist puudutavate nõuete ning osapoolte õiguste ja kohustuste reguleerimise.

Nimetatud muudatustega küll loodi EL tasandil ühine makseturg, mille raames on kõikide liikmesriikidele ette nähtud ühtne õiguskord, ent nendega ei kaasnenud VÕS-s kehtinud põhimõtete kardinaalne muutmine. Kuivõrd VÕS-i varem kehtinud regulatsiooni loomisel järgiti Euroopa Komisjoni soovituses nr 97/489/EÜ toodut, mis oli ühtlasi ka direktiivi 2007/64/EÜ koostamisel üheks oluliseks alusdokumendiks, ei muudetud oluliselt senikehtinud põhimõtteid makseteenuste valdkonnas. Siiski lisandus VÕS-i muudatuste tagajärjel Eesti siseriiklikku regulatsiooni mitmeid uusi sätteid, mis seni kehtinud seadust

märkimisväärselt täiendasid. Asjaomaste normide põhjendatavuse ning efektiivsuse hindamiseks tõstatas autor töö sissejuhatuses probleemküsimused, millele vastuse saamine oli immanentselt seotud uurimiseesmärgi täitmisega.

Esimese probleemina tõi autor välja vajaduse leida vastus küsimusele, milles seisnes VÕS-i muudatustega kaasnenud seaduses kasutatava mõisteaparaadi, eelkõige maksevahendi mõistega seonduva uuendamine ning kas nimetatud uuendused aitasid kaasa regulatsiooni kaasjastamisele. Maksevahend oli ja on jätkuvalt defineeritud VÕS-s, ent kui varem kehtinud VÕS-s eristati elektroonilise maksevahendi alaliikidena kaugjuurdepääsuga maksevahendit ning e-raha, siis kehtivas regulatsioonis on nimetatud erisused kaotatud ning maksevahendi mõiste on ühtse definitsioonina avatud VÕS § 709 lg-s 8: maksevahend on teenuse pakkuja ja tema kliendi vahel kokkulepitud isikustatud seade või ka toimingute kogum, mida makseteenuse pakkuja klient kasutab maksejuhise algatamiseks. Autori hinnangul on VÕS-i muudatustega kaasnenud maksevahendi mõiste korrigeerimine põhjendatud eelkõige seetõttu, et elektrooniliste maksevõimaluste kiiret arengut ning kasvutendentsi silmas pidades ei saa legaaldefinitsioon koosneda jäigast sõnastusest, mis ajale peagi jalgu jääks ning pidevat muutmist vajaks. Tänu pidevalt arenevale tehnoloogia valdkonnale on käesolevaks hetkeks töötatud välja ka mitmeid selliseid alternatiivseid lahendusi, mida õiguslikult küll maksekaartidena ei kvalifitseerita, ent mis oma olemuselt siiski maksevahendite definitsiooni alla kuuluvad. Nimetatud alternatiividena tõi autor käesolevas töös välja mobiilimaksed ehk m-maksed, *PayPal*'i laadsed tehnoloogilised lahendused maksete vahendamiseks ning loojalsusprogrammi raames kaupmeeste poolt väljastatud boonuspunktid, mida saab kasutada järgnevate ostude eest tasumisel. Et nimetatud maksekaardi tüüpi maksevahendite kasutamine oleks ka õiguslikult reguleeritud, andis selleks autori hinnangul omalt poolt märkimisväärse panuse ka VÕS-i mõisteaparaadi muutmine. Sellele vaatamata on autor kriitiline mõistete "autoriseerimine" ning "vastutus" kasutamine makseteenuste kontekstis. Kuivõrd nagu autor ka oma analüüsi käigus leidis, tähendab autoriseerimine sisuliselt nõusoleku sünonüümi, mistõttu jääb siinkohal arusaamatuks mõistete dubleerimise vajadus. Seadusandja on mõisteaparaadi kujundamisel lähtunud makseteenuste direktiivi mõistete otsetõlkest, ent jätnud seejuures tegemata mõjuanalüüsi seaduse selgusele. Samal põhjusel on arusaamatu ka VÕS 40. peatüki 2. jao 3. jaotise kontekstis mõiste vastutus kasutamine, kuivõrd selle all ei mõeldud klassikalist vastutust lepingu rikkumise eest võlaõiguses, vaid eelkõige autoriseerimata maksetehingu tulemusel kujunenud olukorda. Võttes arvesse, et seadused peavad olema arusaadavad ja selged ka õigusteadmisteta isikule, on hetkel kehtivas regulatsioonis nimetatud nõudest kõrvale kaldutud.

Teine küsimus, mille autor töö sissejuhatuses välja tõi, seondub maksevahendi omaja omavastutuse kohaldamise alustega. Kompaktse teemakäsitluse huvides esitas autor ka küsimuse sellest, et millistest asjaoludest sõltub riisiko kandmine osapoolte vahel. Selleks, et rääkida osapoolte vahel kehtivast vastutuse jaotusest, on esmalt vajalik välja tuua üldised maksevahendi kasutamisega seonduvad riskid. Seetõttu analüüsis autor alapeatükis 2.1 identifitseerimisvahendite kui maksevahendite kasutamisega seotud kõige tüüpilisemaid turvariske. Ehkki makseteenuste pakkujad peavad äärmiselt oluliseks oma mainet, mis tagab neile teiste teenuse pakkujate ees tugeva konkurentsieelise ning mille kujunemise üheks olulisemaks komponendiks on nende poolt pakutavate teenustega kaasnev turvalisus, ei ole tänapäeva üsna tehnoloogiliseks kujunenud pangandusmaailmas võimalik luua absoluutselt riskivaba internetipanganduse keskkonda. Hinnates identifitseerimisvahenditega kaasnevaid turvariske, saab neid eelkõige jagada kahel alusel – kas tegemist on riskidega makseteenuse pakkuja või kasutaja jaoks. Makseteenuse pakkuja jaoks saab peamiste turvariskidena välja tuua 1) olukorra, kus internetipangateenust proovib kasutada selleks õigustamata isik, kelle valdusesse on sattunud makseteenuse kasutaja identifitseerimisvahendid, ning 2) situatsiooni, kus identifitseerimisprotsess jääb mõne tarkvaralahendustes esineva vea tõttu poolikuks või süsteemiviga lubab identifitseerimisprotsessi tulemuslikult lõpetada, ehkki sisselogimisel esitati ebaõiged identifitseerimisvahendid või sellel lasunud andmed. Samas ei ole makseteenuse pakkuja jaoks vähemolulisem ka risk, mis on seotud sellega, et makseteenuse kasutaja ees kannab just pakkuja vastutust selle eest, et identifitseerimisel tekib tõrge mõnes tehnilises lahenduses, mida pakkuja vahendab – m-maksete või ID-kaardi abil identifitseerimise võimaluse puhul on makseteenuse pakkuja sageli üksnes vahendaja rollis. Rääkides aga turvariskidest, mis on eelkõige iseloomulikud just makseteenuse kasutajale, tuleb peatuda identifitseerimisvahendi kopeerimisvõimalusel ning hoolsuskohustusel. Hoolsuskohustuse täitmisega, millel autor peatus põhjalikumalt töö 3. peatükis, on tihedalt seotud ka riisiko küsimus.

Kehtiva regulatsiooni kohaselt kannab autoriseerimata makse korral, mis on tehtud kadunud või varastatud maksevahendiga, tekkida võivate kahjude riisikot maksja. Olulise täiendusena, mis tagab eelkõige regulatsioonile õigusselguse, on kehtivasse regulatsiooni lisatud klausel, mille kohaselt kannab maksja riisikot ka siis, kui maksevahendit on kasutatud muul õigustamatul viisil ja kui maksja ei ole isikustatud turvaelemente nõuetekohaselt hoidnud. Toodud täienduse kujul on otsesõnu lisatud seadusesse klausel, millega on hõlmatud ka internetipangas kasutatavad identifitseerimisvahendid, mis oma olemuselt – olles salasõna ning kasutajatunnuse kujul – ei saa olla füüsiliselt kaotatavad või varastatavad; nende vahendite valduse võib omaja kaotada ka enesele teadmata. Toodud reegel ei kuulu aga

kohaldamisele olukorras, mil maksevahendi kaotamisel või varastamisel on maksevahendi omaja käitunud tahtlikult või raskelt hooletult või pettusega. Sellest sõltuvad ka omavastutuse kohaldamise alused – maksevahendi kaotamisel või varastamisel ei tohi olla tegemist olukorraga, kus maksevahendi omaja käitus tahtlikult, raskelt hooletult või pettusega. Riisiko kandmine olukorras, kus maksevahend on kaotatud või varastatud ning makseteenuse kasutaja ei ole seejuures käitunud tahtlikult ega raske hooletusega, on autori hinnangul õiglaselt jaotatud. Kuivõrd maksevahendi väljastamise järgselt on just maksevahendi kasutaja see, kes omab maksevahendi üle otsest valdust ja kontrolli, makseteenuse pakkuja valdus seejuures maksevahendile täiesti puudub, on loomulik, et maksevahendiga toimuva eest kannab riisikot selle omaja. Eeltoodule vaatamata võib praktikas aga probleeme tekitada seadusandja poolt määratlemata õigusmõiste ehk raske hooletuse kasutamine makseteenuste regulatsioonis, millega on seotud ka töö sissejuhatuses neljandana püstitatud küsimus.

Samuti saab seaduse negatiivse uuendusena välja tuua seadusandja soovi jätta kehtivast regulatsioonist välja endises VÕS § 742 lõigetes 4 ja 5 sätestatud reeglid, mille kohaselt ei kanna maksevahendi omaja maksevahendi abil tehtud toimingust tulenevat riisikot, kui maksevahendit kasutati maksevahendi füüsilise esitamiseta või maksevahendi elektroonilise kindlaks tegemiseta (säte ei kuulu kohaldamisele telefoni- või võrgupanga vahendusel tehtud toimingutele). Kuivõrd nimetatud ohud, et internetikeskkonnas kasutatakse maksevahendit elektrooniliselt kindlaks tegemiseta (nt ostude eest krediitkaardiga tasumisel küsitakse tihtipeale üksnes kaardil olevat numbrit ning kehtivusaja pikkust), eksisteerivad ka tänapäeval, jääb mõistmatuks, miks pidas seadusandja ülaltoodud regulatsiooni väljaarvamist kehtivast regulatsioonist vajalikuks. Olukorras, kus makseteenuse pakkuja on makseteenuse kasutajast tugevamal positsioonil ning omab lisaks sellele ka nimetatud juhtumil rahvusvaheliste kaardiorganisatsioonide reeglitest tulenevalt regressiõigust kaupmehe vastu, on põhjendamatu vähendada tarbijate kaitset võrreldes varem kehtinud regulatsiooniga ning jätta riisiko nende kanda.

Kolmanda probleemina tõstatas autor küsimuse sellest, kas on õigustatud seadusandja otsus näha maksevahendi kasutaja omavastutuse piirmäära maksimaalse summana 150 euro suurust omavastutust. Autoriseerimata maksetehinguga kaasneda võivate riskide ning võimalike kahjulike tagajärgede vältimiseks või vähendamiseks peaks makseteenuse kasutaja olema motiveeritud teatama makseteenuse pakkujat maksevahendi väärkasutamisest esimesel võimalusel. Nimetatud motivatsiooni tekkimiseks on aga teatava vajaliku stiimuli olemasolu, milleks antud juhul ongi ette nähtud omavastutuse piirmäär. Maksja kannab küll seadusest tulenevalt riisikot olukorras, kus maksevahend on kaotatud või varastatud, ent mitte rohkem

kui maksevahendi väljajaga kokkulepitud piirsumma ulatuses, kõige rohkem aga summa ulatuses, mis vastab 150 eurole. Nimetatud piirmäär tuleneb makseteenuste direktiivist 2007/64/EÜ, milline näeb liikmesriikidele ette võimaluse juba saavutatud tarbijakaitse taseme säilitamiseks nimetatud summa piiri alandada. Kuigi Ühendkuningriikide õiguses on sellel põhjusel peetud vajalikuks ka nimetatud summa piiri alandada kuni ekvivalendini, mis eurodesse ümberarvutatult vastab ligikaudu 70 eurole, ei ole Eesti seadusandja pidanud vähendamist mõistlikuks. Arvestades mõne teise EL liikmesriigi lähenemist antud küsimusele, sh ka Ühendkuningriikide ning Rootsi lähenemist, jääb autorile mõnevõrra mõistatuks Eesti seadusandja eesmärgid direktiivis ettenähtud maksimaalse piirsumma rakendamise vajalikkuse osas siseriiklikku õigusesse. Kuivõrd antud teemal puudub ülevaatlik siseriiklik kohtupraktika, võib autori hinnangul sellest omakorda järeldada, et reeglina ei viivita makseteenuse kasutajad maksevahendi kaotamisest või varastamisest makseteenuse pakkujale teatamisega. Seetõttu on mõistmatu, miks seadusandja on pidanud stiimuli, mis peaks makseteenuse kasutajaid motiveerima teenuse pakkujaid maksevahendiga seonduvast teavitama, sätestamist keskmiseid brutosissetulekuid arvestades sedavõrd kõrgena vajalikuks.

Töö sissejuhatuses tõstatatud neljas probleemküsimus seisnes eelkõige selles, et kuidas tuleb makseteenuse osutamise valdkonnas sisustada raske hooletuse mõiste, millise täitmise tingimus on üheks omavastutuse kohaldamata jätmise aluseks. Nimetatud küsimus on oluline eelkõige seetõttu, et VÕS-s toodud regulatsioon antud mõiste legaaldefinitsiooni ette ei näe. Direktiivi kohaselt tuleb makseteenuste valdkonnas raske hooletuse mõiste sisustada siseriiklikul tasandil. Ka Ühendkuningriikide õiguses makseteenuste direktiivi rakendamiseks vastu võetud *the Payment Services Regulation* ei sisalda sarnaselt VÕS-le raske hooletuse mõistet, ent seal on probleem lahendatud kohtupraktikaga. Kuivõrd identifitseerimisvahendi heauskne ning korrektne valdamine selle väljastamise järgselt on makseteenuse kasutaja peamiseks kohustuseks, sõltub maksevahendi kaotamise või varastamise järgselt maksevahendi omaja vastutus paljuski sellest, kas makseteenuse pakkujal õnnestub tõendada, et maksevahendi omaja oli maksevahendi kaotamisel või varastamisel raskelt hooletu. Sama on olukord ka infotehnoloogiliste vahendite valdamisel, mis on sidevahendina vajalikud internetipanga keskkonnas isiku identifitseerimiseks. Kuivõrd raske hooletuse mõistet ei ole seaduse tasandil defineeritud, on see võimalus jäetud makseteenuste pakkujale. Autor jõudis seisukohale, et hoolsuskohustuse täpsem defineerimine seaduse tasandil ei oleks valdkonna kiiret arengut silmas pidades kuigi otstarbekas ega mõistlik – seadusandja ei jõuaks vajalike muudatustega sammu pidada. Seetõttu on põhjendatud, et makseteenuse pakkujatele on tagatud võimalus lisaks seadusest tulenevale hoolsuskohustusele sätestada lepingutes ka täiendavad kriteeriumid hoolsuskohustuse sisustamiseks. Seejuures peavad teenuse pakkujad

aga pidama silmas, et kehtestatavad kriteeriumid ei oleks makseteenuse kasutajaid üleliia koormavad ega läheks vastuollu seaduses sätestatud üldise hoolsuskohustusega – nimelt peavad kriteeriumid selleks, et nad kehtiksid, olema mõistlikud ka tavalisele mõistlikule isikule. Kuivõrd nimetatud hoolsuskohustuse sätestavad makseteenuse pakkujad kõige tõenäolisemalt tüüptingimuste vormis, peavad nad jälgima VÕS § 42 lg-st 1 tulenevat regulatsiooni tingimuste kehtivuse tagamiseks.

Töö sissejuhatuses esitas autor esmalt hüpoteesi, et 22. jaaanuaril 2010. aastal jõustunud VÕS-i muudatused olid regulatsiooni kaasajastamise huvides hädavajalikud ning tagavad regulatsiooni selguse. Eelnimetatut arvestades on selge, et nii see siiski päris üheselt ei ole. Kindlasti tuleb jaatada direktiivi 2007/64/EÜ positiivset mõju identifitseerimisprotsessi reguleerivate sätete täpsustamisel ning laiendamisel, ent samal ajal on regulatsioonist kaotatud ka sätteid, mis seal regulatsiooni terviklikkuse huvides jätkuvalt peaks olema.

Teiseks hüpoteesiks võttis autor selle, et VÕS-i muudatused on küll kooskõlas direktiivis 2007/64/EÜ sätestatuga, ent sellele vaatamata ei ole siseriikliku õiguse aspektist vaadatuna makseteenuse lepingu poolte huvid kaitstud parimal võimalikul viisil. See hüpotees leidis töös osaliselt kinnitust – kui autori hinnangul on regulatsioon makseteenuse pakkuja huvide aspektist vaadatuna õiglane, siis makseteenuse kasutaja puhul esineb autori hinnangul mitmeid kitsaskohti, millele seadusandja võiks tähelepanu pöörata. Selliselt ei ole näiteks põhjendatud omavastutuse piirmäära sätestamine 150 eurona.

Käesoleva töö analüüsi tulemusel võib seega leida, et direktiivi 2007/64/EÜ rakendamiseks siseriiklikkusse õigusesse vastu võetud VÕS-i muudatused ei kõrvaldanud muudatustele vaatamata kõiki regulatsiooniga kaasnevaid probleemkohti. Lahendamata probleemkohtadena võib eelkõige välja tuua eelnevalt nimetatud liialt kõrge omavastutuse piirmäära, mis autori hinnangul on põhjendamatult kõrge ning ebaõnnestunud mõisteaparaadi uuendamist, mis ei taganud loodetud õigusselgust.

Katri Kitsing

04.05.2015

The scope and nature of the liability of security risks arising from the usage of authentication instruments of Internet banking

Summary

On the 22nd of January 2010, the improved 40th chapter of the Law of Obligations Act (LOA) entered into force, which was dedicated to amending the inner structure and also the legal provisions of the law. Main reason for the need of the above-mentioned amendments was the adoption of the Payment Institutions and E-money Institutions Act, which main purpose was to harmonise the directive 2007/64/EC on payment services into national law and also to make amendments to the valid regulation of E-money Institutions Act. The need to adopt the directive 2007/64/EC on the level of European Union was caused by the fact, that it's purpose – to create unified payments market – could not have been achieved on the national level of the Member States, because it would have demanded unification of the already developed legal systems of the Member States, which would have been a difficult task to achieve locally. Although amending the legal provisions of the LOA was certainly important in terms of harmonising the European Union's Contract Law, it is also important to evaluate the effect of the changes to the national law and also to take into account its specifications. Considering this fact, it is questionable, whether the Estonian legislator was acting on behalf of both parties' interests when enforcing the amendments of the LOA.

This master's thesis (paper) aims to give an opinion on whether or not the directive 2007/64/EC has been successfully transposed and whether the amendments made into the LOA in 2010 amendended the regulation into a better one by helping to improve it. The author also wishes to answer the questions whether the contractual liability between the payment service provider and the payer has been divided adequately in case when the security risks have occurred using the means of identification in internet banking and if the interests of the parties are protected well enough. In addition, the purpose of this paper is also to collect the relevant materials and literature regarding its subject field. Besides giving comparative assessments, this paper also focuses on giving suggestions for amendments there, where the regulation in force is insufficient or unclear.

In order to analyse the aforementioned amendments and their effectiveness, the author posed the following questions:

1) what was the substance of renewing the definitions of the LOA and did the amendments help to bring the definitions up-to-date;

2) which circumstances affect carrying the risk between parties and how are the bases for applying the payer's liability regulated;
3) how should gross negligence be interpreted in the context of payment services as the cause of not implementing payer's liability;
4) is it justified to set the payer's liability up to 150 euros, which is the maximum sum allowed by the directive 2007/64/EC.

Internet banking is a subject that is constantly developing through time and is also continue to develop in the future. Since the majority of people are using services provided by the internet banking almost on a daily basis, it is important that the contractual relations between the payment service provider and the payer are comprehensible also to the consumer, who presumably has no legal knowledge. This paper's actuality is therefore mainly related to the fact that, since internet banking services and with it the identification process is being used by majority of people, it is required that the liability arising from the relation between the payment service provider and the payer is clearly and understandably regulated on the level of national law. The topic of this paper is also actual due to the reason that there have not been any writings or articles covering the matters of this paper prior to this master's thesis. Amendments to the LOA that came into effect on 22nd of January 2010 have been partially covered in the master's thesis written by Raido Rink ("Unauthorized payment transaction with the electronic payment instrument"). Differently from this paper, the above-mentioned paper is mainly focusing on the unauthorised payments and does not cover the subject of internet banking and the liability arising from using the services of internet banking and in addition is partially focused on German legislation.

Although the unified payments market on EU level was created by adopting the amendments of the LOA on the basis of the directive 2007/64/EC, it did not result in the need to change the principles valid in the LOA extensively. But even though the regulation of the LOA that was valid prior to 2010 adoption was mainly based on the European Commission's recommendation 97/489/EC, which was also the main source document for creating the directive 2007/64/EC, there were many additional provisions added to the valid regulation of the LOA that considerably improved the previous regulation regarding the payment services.

Adopting the improved regulation of the LOA gave the legislator the opportunity to renew the definitions used in the regulation and bring them up-to-date. Regardless of the purposes set to the renewal of the definitions, in her analysis the author questions whether the aforementioned renewal has filled its purpose one hundred per cent.

As the payment instrument was and continuously is being defined in the LOA, the definition itself has changed throughout the amendments. While the previous regulation classified the payment instrument as a remote access payment instrument and e-money, in the valid regulation this kind of classification has been lost and the payment instrument is being defined in § 709 subsection 8: payment instrument within the meaning of the LOA is any personalised device or also a set of procedures agreed on between the payment service provider and its client (payer), which are used by the client of the payment service provider for the initiation of a payment order. In the author's opinion, the correction of the payment instrument's definition in the LOA was reasoned. When taking into consideration the vast development of the electronic payment options and potential to develop even more in the future, the legal definition of the payment instrument cannot consist of a rigid formulation that would soon be out-dated and needs changing. Thanks to rapidly growing and developing subject field, there are already many alternative solutions for payment instruments, that are not yet being legally qualified as payment instruments, but still go under the definition by their nature. These kinds of alternatives are mainly mobile payments also known as m-payments, technological solutions to transfer payments such as PayPal and bonus points that merchants give to their loyal clients and that can be used as payment instrument during the next purchase – the bonus points are equivalent to money. In order to classify these aforementioned alternatives as legally regulated payment instruments, the changes of the definitions in the LOA were needed. As a criticism, all the definitions used in the improved the LOA are not justified. For example, the definition of authorisation that is being used throughout the payment service regulation in the LOA. The definition of authorisation emanates from the directive 2007/64/EC, being translated into Estonian word by word. The meaning of authorisation in the LOA by its content is basically an equivalence to the definition of approval, which is also being mentioned in the LOA. Since the definition of athorisation is given in the LOA § 724^1 subsection 1 through the concept of approval, the legislator's opinion about the need to duplicate the definitions remains unclear. Adopting the laws of the EU is in fact mandatory to the Member States. Regardless, it should be done in a manner, which takes into consideration the national law with its specifications and ensures the principle of clarity in law.

Additionally, the adoption of the amended regulation gave the legislator the chance to eliminate the controversis in the regulation of the LOA, but in the author's opinion the legislator did not use this opportunity. The previous regulation of the LOA and also the directive 2007/64/EC use the definition of liability in the context of payment services that regulates the situations where damages arising from the contractual relations between the

payment service provider and the payer have occurred. The usage of definition liability in the context of the 40th chapter 2nd division 3rd section of the LOA remains unclear, as the definition is not meant for regulating the classical liability arising from breaching the contract, but mainly for regulating the situation arising from performing an unauthorised payment. Taking into consideration that the legal regulations needs to be clear and understandable to persons without legal knowledge, the valid regulation of the LOA regarding the field of liability does not measure up to these requirements. In the interest of correctly understanding this paper's subject, the author hereinafter still refers to liability as it is the definition used in the directive 2007/64/EC and in the LOA, even though she does not approve using this definition in that context.

The second question that the author posed in order to analyse the amendments to the LOA regards the bases of implementing the payer's liability. In order to analyse the division of liability between the parties, it is important to bring out the main security risks regarding the usage of payment instruments. Therefore, in the subsection 2.1 of this paper, the author analysed the main security risks involving the usage of payment instruments and concludes, that they may be divided on two bases: security risks for the payment service provider and for the payer. From the aspect of the payer's liability it is relevant to bring out risks for the payer, mainly relating the obligation to show due diligence and the possibility to copy the data on the payment instrument.

According to the valid regulation of the LOA, the payer shall bear the losses relating to any unauthorised payment transactions resulting from the use of a lost or stolen payment instrument. An important addition to the valid regulation, that shall ensure fulfilling the principle of clarity in law, is the reservation according to which the payer bears the liability also when the payment instrument has been used in another unauthorised manner or if the payer has not duly kept the personalised security features. With the aforementioned reservation the legislator has now implemented a regulation, whereby the means of identifications used in internet banking are included in the regulation word by word. That was mainly needed due to the reason that by their nature, the means of identification – being namely in the form of password and username – cannot be physically lost or stolen. Their owner may lose possession over them without even knowing it himself. However, the afore-mentioned does not apply, if the unauthorised payment involves fraud by the payer or if the payer acts deliberately or due to gross negligence. This is in correlation with implementing the bases for payer's liability. In order to implement the payer's liability, the payer must have not been grossly negligent or acted deliberately or with fraud regarding the loss of the

payment instrument. This also applies when the payment instrument has been stolen. In the author's opinion, bearing the losses in situations, where the payment instrument has been stolen or lost and the payer has not been grossly negligent or acted deliberately or with fraud, is divided fairly. Since, after giving out the payment instrument by the payment service provider, the payer owns the possession over the payment instrument, it is only natural, that when speaking about the risks regarding the payment instruments, its owner must bear the risks. Since the payer's liability is in strong connection with the definition of gross negligence, it may be possible that in the practice, regardless to the aforementioned, the legislator's choice to use the definition of gross negligence in the regulation may become problematic due to the fact that there is not a definition in the law.

Before resolving the question about the usage and definition of gross negligence in the valid regulation, it is important to point out the following: with adopting the new regulation of the LOA, the legislator's wish to exclude some relevant provisions from the new regulation stood out. According to the previous regulation of the LOA, the § 742 subsections 4 and 5 pointed the rules that the payer does not bear any losses in the case of unauthorised transaction, if the payment instrument was used without physically presenting it to the merchant or without electronically identifying the payer. This rule did not apply in case where the transactions were made through mobile or internet bank. Since the danger that one's payment instrument may be used on the internet without electronically identifying the user prior to the transaction (e.g. when paying for products with credit card, sometimes the merchant only asks for the number on the card and it's period of validity), also exists nowadays, during the validity of the new regulation of the LOA, it raises the question why the legislator chose to exclude the above-mentioned provisions from the regulation. In case where the payment service provider has a stronger position compared to the payer's resources and additionally, according to the rules of international card's organisation, owns the right of recourse against the merchant, it is not reasoned enough to minimize the protection of the consumers comparing to the regulation that was in force prior to the amendments of the 22nd of January 2010. In the author's opinion, the legislator mustn't have excluded the mentioned rules from the valid regulation.

In the subparagraph 3.2, the author analysed the question, how the definition of gross negligence should be defined in the context of payment services. This definition is important since it coheres with implementing the payer's liability. This liability, which may be up to 150 euros maximum, may not be applied on the proposal of the payment service provider, if the payer's actions were grossly negligent and caused the possibility for unauthorised transaction. The question about the definition of gross negligence is actual mainly because

according to the directive 2007/64/EC, it should be stated in the national law and the regulation of the LOA does not give the legal definition. Implementing the directive 2007/64/EC into United Kingdom's law, the legislator has adopted the Payment Services Regulation that, similarly to the LOA, does not define the term 'gross negligence'. But, differently from Estonia, gross negligence in the context of payment services has been defined by the judicial practice. In Estonia, that kind of judicial practice in the context of payment services is absent.

Since the *bona fide* possession and possessing the payment instrument correctly after it's issuance are the main obligations of the payer, the liability that follows after losing the payment instrument or it being stolen depends largely on the fact whether the payment service provider manages to prove that the payer was guilty of gross negligence during losing or stealing the payment instrument. The situation is the same when it comes to the possession of the technological devices that are necessary as a means of communication in order to identify a person in the internet banking environment (e.g. mobile phones or computers). Since there is no legal definition given to the gross negligence, the payment service providers are given the opportunity to define it themselves in the matter of the contract between the parties – mainly they do it in the form of standard terms. Even though the first opinion may be that the aforementioned solution may consequence in payment service providers using their stronger position, because they have the opportunity to stipulate the terms regarding the possession of the payment instrument and the technological devices that may unreasonably burden the payer, when he or she can be held liable for not following these stipulations carefully, it is not quite the case. In order to stipulate the valid definition of gross negligence, the payment service providers are binded to the definition of gross negligence by law – they cannot state the stipulations not much higher as they are stated in the law or they will risk with a chance them being invalid according to art 42 (1) of LOA.

Fourthly, the author raised the question, whether the legislator's decision to set the payer's liability up to 150 euros is justified. In order to minimize the risks and possible damages that may be caused due to the unauthorised transactions, the payer must be motivated to notify the payment service provider about the exploitative abuse of the payment instrument as soon as possible. For this kind of motivation, some kind of incentive must be in order – for example, the limit of the payer's liability. It is stipulated in the LOA, that, if an unauthorised payment has been executed using a lost or stolen payment instrument, the payer shall bear the risk, but not more than to the extent of the limit amount agreed on with the issuer of the payment instrument, and at most to the extent of the amount equaling 150 euros. This limit has been

stipulated as the maximum sum that payment service provider may ask in the directive 2007/64/EC. Even so, the directive's preamble states clearly, that the Member States have the possibility to reduce this maximum sum in order to retain the state's consumer protection level. The legislator of the United Kingdom has used this privilege and thought it was necessary to reduce the payer's liability down to an equivalence, which converted into euros corresponds to 60 euros. The Estonian legislator did not think that reducing this limit was necessary, and therefore it is stipulated in the LOA that the payer may be held responsible for up to 150 euros. Considering the approaches of other Member States, including the UK in this matter, it remains unclear why the Estonian legislator did not consider lowering the payer's liability limit. Since there is no Estonian judicial practice on this matter, one may conclude that the payers do not usually delay notifying the payment service provider about the loss of a payment instrument or about it getting stolen, and that the damages that may occur afterwards are not big. Therefore, and also considering the average gross wages in Estonia, the legislator's decision to set the payer's liability up to a maximum 150 euros, is unclear. In the author's opinion, it is not fair to set the liability this high in circumstances, where the payment service provider has obviously better resources of minimizing the damages that may arise from the loss of a payment instrument.

Taking into account the aforementioned explanations, it can be concluded that the transposition of directive 2007/64/EC was needed in order to harmonise the national law with the EU law and that the transposition has had a big effect on the national legislation of Estonia. Sure, not all of the amendments have been as successful, but it still can be seen as a positive step forward. However, the author is under the impression that the need to harmonise the payment service market is also in the interest of the payment service providers themselves. With clear provisions and unified regulations on the EU level they could operate much more easily, also providing their services abroad. When coming back to the specific amendments of the LOA, it can however be said that, at the moment, there is more room to develop and stipulate a regulation without contradictions.

Katri Kitsing

04.05.2015

Kasutatud lühendid

1) direktiiv 2007/64/EÜ – Euroopa Parlamendi ja nõukogu direktiiv 2007/64/EÜ, 13. november 2007, makseteenuste kohta siseturul ning direktiivide 97/7/EÜ, 2002/65/EÜ, 2005/60/EÜ ja 2006/48/EÜ muutmise ning direktiivi 97/5/EÜ kehtetuks tunnistamise kohta
2) EL – Euroopa Liit
3) HMKo – Harju Maakohtu otsus
4) MERAS – Makseasutuste ja e-raha asutuste seadus
5) *opt.cit.* ehk *opere citatio* – varasemalt viidatud töö
6) *per se* – iseenesest
7) RKTKo – Riigikohtu tsiviilkolleegiumi otsus
8) TsÜS – Tsiviilseadustiku üldosa seadus
9) VÕS – Võlaõigusseadus

Kasutatud kirjandus

1) Cheney, J. S. An Examination of Mobile Banking and Mobile Payments: Building Adoption as Experience Goods? 2008.
2) Kull, I., Käerdi, M., Kõve, V. Võlaõigus I. Üldosa. Tallinn: Juura, 2004.
3) Kull, I., Parrest, I. Teatamiskohustus võlaõigusseaduse kontekstis – Juridica 2003/IV.
4) Lahe, J. Doktoritöö: Süü deliktiõiguses. Juura, 2005.
5) Research Group on the on the Existing EC Private Law (Acquis Group). Principles of the Existing EC Contract Law (Acquis Principles) – Contract II: General Provisions, Delivery of Goods, Package Travel and Payment Services. Munich: Sellier, 2009.
6) Runnel, T. Elektroonilise maksevahendi abil omaja tahteta tehtud tehing – Juridica 2005/VI.
7) Schlechtriem, P. Võlaõigus. Eriosa. Tallinn, 2000.
8) Schlechtriem, P. Võlaõigus. Üldosa. Tallinn, 1999.
9) Sootak, J. Üliõpilastöö kirjutamine ja vormistamine. Juhend õigusteaduskonna üliõpilastele. Tallinn, 2011.
10) Tampuu, T. Deliktiõigus võlaõigusseaduses. Üldprobleemid ja delikti üldkoosseisul põhinev vastutus – Juridica 2003/II.
11) The Payment System: Payments, Securities and Derivatives, and the Role of the Eurosystem. European Central Bank.
12) Trautman, J. E-commerce and electronic payment system risks: lessons from PayPal.
13) Varul, P. jt (koost). Võlaõigusseadus I, kommenteeritud väljaanne. Tallinn: Juura, 2006.
14) Varul, P. jt (koost). Võlaõigusseadus III, kommenteeritud väljaanne. Tallinn: Juura, 2009.
15) Wilhelmsson, T. Good Faith and the Duty of Disclosure in Commercial Contracting – Good Faith in Contract: Concept and Context. Brownsword, R., Hird, N.J., Howells, G. Publisher: Dartmouth, Aldershot, 1998

Kasutatud õigusaktid

16) Euroopa Parlamendi ja nõukogu direktiiv 2007/64/EÜ, 13. november 2007, makseteenuste kohta siseturul ning direktiivide 97/7/EÜ, 2002/65/EÜ, 2005/60/EÜ ja

2006/48/EÜ muutmise ning direktiivi 97/5/EÜ kehtetuks tunnistamise kohta– ELT L 319, 5/12/2007.
17) Hea õigusloome ja normitehnika eeskiri – RT I, 29.12.2011, 228.
18) Makseasutuste ja e-raha asutuste seadus – RT I 2010, 2, 3.
19) The Payment Services Regulation, 2009. Arvutivõrgus: http://www.legislation.gov.uk/uksi/2009/209/pdfs/uksi_20090209_en.pdf. 13.04.2015.
20) Tsiviilseadustiku üldosa seadus – RT I 2002, 35, 216.
21) Võlaõigusseadus – RT I 2001, 81, 487.

Kasutatud kohtupraktika

22) HMKo nr 1-12-7896
23) RKTKo tsiviilasjas 3-2-1-92-05.
24) RKTKo tsiviilasjas 3-2-1-73-02.
25) RKTKo tsiviilasjas 3-2-1-125-08.
26) RKTKo tsiviilasjas 3-2-1-161-12.
27) RKTKo tsiviilasjas 3-2-1-73-13.
28) Tallinna Ringkonnakohtu otsus asjas 2-10-55812/27.

Kasutatud muud allikad

29) Acquis Group. European Research Group on Existing EC Private Law. Arvutivõrgus: http://www.acquis-group.org, 13.04.2015.
30) Arvutikaitse. Nuhkvara. Arvutivõrgus: http://www.arvutikaitse.ee/arvutikaitse-algtoed/nuhkvara/, 13.04.2015.
31) CNET. Everything you need to know about NFC and mobile payments. Arvutivõrgus: http://www.cnet.com/how-to/how-nfc-works-and-mobile-payments/. 15.04.2015.
32) Danske Bank. Teleteenuste tingimused. Arvutivõrgus: http://www.danskebank.ee/public/terms/Teleteenused_tingimused_EST.pdf, 13.04.2015.
33) Eesti Panga koduleht. Naelsterlingi vahetuskurss 14.04.2015.a seisuga. Arvutivõrgus: http://www.eestipank.ee, 15.04.2015.

34) Eesti Panga koduleht. Rootsi krooni vahetuskurss 14.04.2015.a seisuga. Arvutivõrgus: http://www.eestipank.ee, 15.04.2015.
35) Eesti Õigustõlke Keskus. Riisiko definitsioon. Arvutivõrgus: http://mt.legaltext.ee/esterm/concept.asp?conceptID=2855&term=riisiko, 13.04.2015.
36) Euroopa Komisjoni soovitus nr 97/489/EÜ. Arvutivõrgus: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1396256154001&uri=CELEX:31997H0489, 13.04.2015.
37) Euroopa Liidu tarbija nõustamiskeskus. Ettevaatust pettusskeemidega! Arvutivõrgus: http://www.consumer.ee/scam/, 13.04.2015.
38) Euroopa Majandus- ja Sotsiaalkomitee arvamus 2009/C 100/04 teemal „Mittesularahaliste maksevahenditega seotud pettuste ja võltsimiste vastane võitlus". Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:100:0022:0027:ET:PDF, 13.04.2015.
39) European Central Bank. Assessment Guide for the Security of Internet Payments. February 2014. Arvutivõrgus: https://www.ecb.europa.eu/pub/pdf/other/assessmentguidesecurityinternetpayments201402en.pdf. 16.04.2015.
40) European Central Bank. Payments and Markets Glossary. Arvutivõrgus: http://www.ecb.eu/home/glossary/html/glossp.en.html, 13.04.2015.
41) Eversheds. The Meaning of Gross Negligence under the Payment Services Regulation. Arvutivõrgus: http://www.eversheds.com/global/en/what/publications/shownews.page?News=en/ireland/the-meaning-of-gross-negligence-under-the-payment-services-regulations-march-2014, 13.04.2015.
42) Finextra, Gemalto releases mini online banking authentication device, *News Release,* October 30, 2008. Arvutivõrgus: http://www.finextra.com/fullstory.asp?id=19204, 13.04.2015.
43) Interpretation of gross negligence in commercial contracts. Arvutivõrgus: http://www.walkermorris.co.uk/interpretation-gross-negligence-commercial-contracts. 13.04.2015.
44) Kamps, M. Nigeeria petukirjadega petetakse Soomest sadu tuhendaid eurosid. Arvutivõrgus: http://www.postimees.ee/1132430/ajaleht-nigeeria-petukirjadega-petetakse-soomest-sadu-tuhandeid-eurosid, 13.04.2015.

45) LHV Partner Krediitkaart. Arvutivõrgus: https://www.partnerkaart.ee/et/lhv-partner-krediitkaart-ainus-pangakaart-mida-sa-vajad_archived. 15.04.2015.
46) Linkgreim, I-G. Eestlased ei raatsi panga paroolikaartidest loobuda. Arvutivõrgus: http://uudised.err.ee/v/majandus/14b8cbb6-f1cb-4902-ade4-1c958ae1a72a, 13.04.2015.
47) Maksed mobiiliga. AS EMT. Arvutivõrgus: https://www.emt.ee/era/teenused/maksed-mobiiliga, 13.04.2015.
48) Mis on PayPal? PayPal Eesti kogukond. Arvutivõrgus: http://www.paypal-eesti.maksed.net, 13.04.2015.
49) Nordea pank. Telefoni- ja internetipanga tingimused eraisikule. Arvutivõrgus: http://www.nordea.ee/sitemod/upload/root/content/nordea_ee_ee/eeee_private/eeee_pr_igapaevapangandus_pr/e-pangandus/TIP_tingimused.pdf, 13.04.2015.
50) Payments Council. The Payment Service Directive. Arvutivõrgus: http://www.paymentscouncil.org.uk/what_do_we_do/european_payments/the_payment_services_directive/, 13.04.2015.
51) PIN kood pangakaardi juures: varas sai saagiks üle 1600 krooni. Arvutivõrgus: http://www.ohtuleht.ee/383105/pin-kood-pangakaardi-juures-varas-sai-saagiks-1600-krooni, 13.04.2015.
52) Reserve Bank of India. Report on Internet Banking. Arvutivõrgus: http://www.rbi.org.in/scripts/PublicationReportDetails.aspx?ID=243#ch5, 13.04.2015.
53) Roheline raamat: Euroopa integreerituma kaardi-, interneti- ja mobiilimaksete turu saavutamine. Brüssel, 11.1.2012. KOM (2011) 941 lõplik. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0941:FIN:ET:PDF, 13.04.2015.
54) Roonemaa, H. Koodikaartide kaotamist alustab Eestis Sampo pank. Arvutivõrgus: http://epl.delfi.ee/news/eesti/koodikaartide-kaotamist-alustab-eestis-sampo-pank.d?id=51274617, 13.04.2015.
55) SEB. Erakliendi internetipank. Arvutivõrgus: http://www.seb.ee/igapaevapangandus/teeninduskanalid/erakliendi-internetipank, 29.04.2015.
56) SEB. Internetipanga kasutamistingimused. Arvutivõrgus: http://www.seb.ee/files/tingimused/u-neti_lepingu_tingimused_est.pdf, 13.04.2015.
57) SEB Rahvusvahelise Debetkaardi Lepingu Tingimused 01.01.2012. Arvutivõrgus: http://www.seb.ee/files/tingimused/rahvusvahelise_deebetkaardi_tingimused_est.pdf, 13.04.2015.

58) Seletuskiri makseasutuste ja e-raha asutuste seaduse eelnõu juurde. Arvutivõrgus: http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=2f4e7aa2-6a42-2e32-4295-c1ca7778230f&, 13.04.2015.
59) Smart card'i definitsioon. Arvutivõrgus: http://computer.howstuffworks.com/question332.htm, 13.04.2015.
60) Statiskaameti aruanne 2012. aasta I kvartalis interneti kasutamise kohta. Arvutivõrgus: www.stat.ee/dokumendid/68622, 13.04.2015.
61) Statistikaameti koduleht. Keskmine palk 2014. aasta IV kvartalis. Arvutivõrgus: http://www.stat.ee/13105, 13.04.2015.
62) Swedbank. Internetipanga turvalisus. Arvutivõrgus: https://www.swedbank.ee/private/home/security/security?language=EST, 13.04.2015.
63) Swedbank. Kaitske oma arvutit. Arvutivõrgus: https://www.swedbank.ee/private/home/security/security?language=EST, 13.04.2015.
64) Swedbank. Muudatused hinnakirjas alates 31.03.2014. Arvutivõrgus: https://www.swedbank.ee/static/pdf/private/home/useful/pricelist_changes_est.pdf, 13.04.2015.
65) Swedbank. Paroolikaart. Arvutivõrgus: https://www.swedbank.ee/private/home/more/channels/internet/password, 29.04.2015.
66) Swedbank. Teleteenuste lepingu tingimused. Arvutivõrgus: https://www.swedbank.ee/static/pdf/private/home/useful/cond_teleservices_2012_12_01_est.pdf, 13.04.2015.
67) Tipik Communications Agency. Conformity Assessment of Directive 2007/64/EC. Estonia. July 2011. Arvutivõrgus: http://ec.europa.eu/internal_market/payments/docs/framework/transposition/estonia_en.pdf. 16.04.2015.
68) Tipik Communications Agency. Conformity Assessment of Directive 2007/64/EC. Latvia. August 2011. Arvutivõrgus: http://ec.europa.eu/internal_market/payments/docs/framework/transposition/latvia_en.pdf. 16.04.2015.
69) Tipik Communications Agency. Conformity Assessment of Directive 2007/64/EC. Sweden. August 2011. Arvutivõrgus: http://ec.europa.eu/internal_market/payments/docs/framework/transposition/sweden_en.pdf. 16.04.2015.
70) Tipik Communications Agency. Conformity Assessment of Directive 2007/64/EC. United Kingdom. August 2011. Arvutivõrgus:

http://ec.europa.eu/internal_market/payments/docs/framework/transposition/united_kingdom_en.pdf. 16.04.2015.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, **Katri Kitsing** (sünd. 13.11.1989),

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

"Internetipanga identifitseerimisvahendite kasutamisel realiseerunud turvariskidest tekkiva vastutuse olemus ja ulatus",

mille juhendaja on dr. iur **Martin Käerdi**,

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, **04.05.2015**