

TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Karistusõiguse osakond

Elizabeth Kirss

**FINANTSASUTUSE KARISTUSÕIGUSLIKU VASTUTUSE VÕIMALIKKUS
PETTUSE MÕJUL SOORITATUD TEHINGU EEST**

Magistritöö

Juhendaja PhD Priit Pikamäe

Tallinn

2026

Sisukord

SISSEJUHATUS	3
1. LÜHIÜLEVAADE FINANTSSEKTORIS ENAMKASUTATAVATEST PETTUSTEST	8
2. FINANTSASUTUSTE HOOLSUSNÕUETE ÕIGUSLIK RAAMISTIK	12
2.1. Finantsasutuste hoolsusnõuded Euroopa Liidu õiguses	12
2.1.1. Makseteenuse kasutaja autentimise kohustus	14
2.1.2. Makseteenuse kasutaja autentimise kohustus kohtupraktikas	21
2.1.3. Operatsiooniriski juhtimine ja turvameetmete kohustus normatiivses raamistikus	26
2.1.4. Operatsiooniriski juhtimine ja turvameetmete kohustus kohtupraktikas	27
2.2. Finantsasutuste hoolsusnõuete regulatsioon Eesti õiguses	30
2.2.1. Makseteenuse kasutaja autentimise kohustus Eesti õiguses	33
2.2.2. Operatsiooniriski juhtimine ja turvameetmete kohustus Eesti õiguses	34
2.2.3. Eesti kohtupraktika	38
3. FINANTSASUTUSTE KARISTUSÕIGUSLIK VASTUTUS KARS § 2172 ALUSEL	42
3.1. Usalduse kuritarvitamise koosseisu eeldused	42
3.2. Finantsasutuste hoolsusnõuete täitmata jätmise/rikkumise ja KarS § 2172 seos	46
4. DE LEGE LATA JA DE LEGE FERENDA HINNANGUD	51
4.1. De lege lata hinnang: kehtiva õiguskorra analüüs Eestis	51
4.2. De lege ferenda hinnang: normatiivsed kaalutlused ja võimalikud arengusuunad	53
Kokkuvõte	58
SUMMARY: The Possibility of Criminal Liability of a Financial Institution for a Transaction Executed Through Fraud	61
KASUTATUD MATERJALIDE LOETELU	67
Kasutatud normatiivmaterjalid ja kommenteeritud väljaanded	67
Kasutatud välisriigi normatiivmaterjalid	67
Kasutatud kirjandus	67
Kasutatud võõrkeelne kirjandus	69
Kasutatud kohtupraktika	70
Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks	72

SISSEJUHATUS

Viimastel aastatel on finantssektoris märgatavalt kasvanud pettuse mõjul sooritatud tehingute arv, mis on otseselt seotud elektrooniliste maksete ja digitaalse panganduse laialdase kasutuselevõtuga. Justiits- ja Digiministeeriumi koostatud ülevaate kohaselt registreeriti Eestis aastatel 2020-2024 kokku 8 081 kelmuskuritegu, kusjuures oluline osa neist oli seotud finantsteenuste ja maksete väärkasutamisega, sealhulgas pettuse mõjul tehtud pangatehingutega¹. Ülevaates esitatud andmed näitavad, et kelmuskuritegude arv on olnud kasvutrendis, suurenedes aastast aastasse. Kelmuste arvu kasvu võib selgitada mitmete teguritega. Ühelt poolt on makselahenduste kiire areng ja kasutusmugavuse suurenemine toonud kaasa olukorra, kus raha liikumine toimub senisest kiiremini ja väiksema kontrolliga. Teiselt poolt on paralleelselt arenenud ka tehnoloogilised lahendused, mida kasutatakse pettuseskeemide elluviimiseks, sealhulgas automatiseeritud manipulatsioonivõtted ja tehisintellekti kasutamine. Justiits- ja Digiministeeriumi ülevaates rõhutatakse, et pettuse eesmärk on inimestelt välja petta andmeid või raha ja nendega puutuvad varem või hiljem kokku kõik internetis toimetavad inimesed.² Sisuliselt tähendab maksepettus sageli olukorda, kus klient edastab oma autentimisandmed petturile või sooritab petturi juhendamisel ise tehingu, teadmata selle tegelikku olemust. Panga vaatenurgast on selliste juhtumite puhul tegemist kliendi enda algatatud ja nõuetekohaselt autentitud tehinguga, kuna makse kinnitamiseks on kasutatud kliendi isiklikke autentimisvahendeid. Selline käsitlus, kus pettuse mõjul sooritatud tehingute vastutus jääks täielikult kliendi kanda, võib kahjustada klientide usaldust finantsasutuse³ vastu ning muuta pettuse ohvriks langenud isikute õiguste kaitse praktikas keeruliseks. Enamasti jääb kannatanule võimalus nõuda kahju hüvitamist üksnes kuriteo toimepanijalt, kuid arvestades, et pettuse toimepanija jääb sageli tuvastamata, nagu nähtub Justiits- ja Digiministeeriumi ülevaates leheküljel 8 esitatud joonisest 2, siis muutub keskseks küsimuseks finantsasutuse roll maksepettuste ärahoidmisel ja pettusega võitlemisel. Sellest tulenevalt tekib küsimus, kas ja millises ulatuses saab finantsasutus vastutada pettuse mõjul sooritatud tehingu eest olukorras, kus klient on tehingu formaalselt ise kinnitanud.

¹ Saarepuu, I., Leps, A. Ülevaade enamlevinud kelmuskuritegudest perioodil 2021-2024. Tallinn: Justiits- ja Digiministeeriumi kriminaalpoliitika osakond 2025. -

<https://www.justdigi.ee/sites/default/files/documents/2025-06/%C3%9Clevaade%20enamlevinud%20kelmuskuritegudest%20perioodil%202021%E2%80%932024.pdf> (02.02.2026).

² *Ibid.*

³ Magistritöö autor täpsustab, et käesolevas magistritöös kasutatakse termineid “finantsasutus” ja “makseteenuse pakkuja” kattuva tähendusega, kuna finantsasutuse mõiste, mis hõlmab laialdast tegevusvaldkonda, sisaldab endas ka makseteenuse osutamist. Seetõttu rakendatakse finantsasutuse suhtes sama regulatiivset raamistikku, mis reguleerib makseteenuse pakkujaid. Selle terminoloogia valiku ja regulatiivset analüüsi põhjendab autor töö teises peatükis.

Maksepettuste ulatuslikku kasvu kinnitab ka Eesti Panga 2025. aasta ülevaade. Selle kohaselt tehti 2024. aastal 25 100 kaardipettust, mis on 16% rohkem kui aasta varem ning kaardipettuste tagajärjel kaotasid inimesed kokku 3,1 miljonit eurot, mis tähistab 24% kasvu võrreldes 2023. aastaga. Kuigi maksekorralduspettuste arv vähenes samal perioodil 5%, püsis nende keskmine kahjusumma kõrgel tasemel - 2024. aastal oli see 1 893 eurot, mis on ligi üheksa korda suurem kui tavapärase maksekorraldustehingu väärtus. Pettustest põhjustatud kogukahju ulatus 2024. aastal 13,5 miljoni euroni, mõjutades nii eraisikuid kui ka ettevõtteid ning kujutades endast märkimisväärt riskitegurit kogu finantssektorile.⁴ Lisaks on küberkuritegevuse ja finantspettuste kasv ning nendega seotud regulatiivsed ja institutsionaalsed väljakutsed olnud käsitle all ka Riigikogus, kus 19.02.2026 arutati olulise tähtsusega riikliku küsimusena küberkuritegevuse ohjeldamist finantsvaldkonnas, rõhutades nii probleemide ulatust kui ka vajadust tõhustada ennetus- ja sekkumismehhanisme finantssektoris.⁵ Eeltoodud statistika näitab selgelt, et maksepettused ei ole üksikjuhtumid, vaid süsteemne probleem, millel on oluline mõju tarbijate varalistele huvidele ja usaldusele finantssüsteemi vastu. Siin omakorda tekib küsimus, kas kehtivad õiguslikud raamistikud vastutuse osas on piisavad ning kas finantsasutuste roll pettuste ennetamisel on õigusselgelt määratletud.

Sarnased arengud on täheldatavad ka Euroopa Liidu tasandil. Liikmesriikides kehtiv aruandluskohustus maksepettuste kohta võimaldab koguda võrreldavaid andmeid ning hinnata pettuste levikut kogu liidus. Euroopa Liidu statistika kohaselt ulatusid 2024. aastal maksepettustest põhjustatud kogukahjud krediitülekannete puhul ligikaudu 2,2 miljardi euroni ja kaardimaksete puhul 1,329 miljardi euroni, mis tähendab vastavalt 16% ja 29% kasvu võrreldes eelneva aastaga. Lisaks põhjustasid pettused muude maksevahendite - näiteks otsedebiteerimiste (ingl. *direct debits*), sularahaautomaatide ja e-raha tehingute (ingl. *e-money transactions*) - puhul veel ligikaudu 239 miljoni euro suuruse kahju. Kokku kasvas pettustest tingitud finantskahju Euroopa Liidus aastaga ligikaudu 23%, ületades pettustega seotud tehingute väärtuse kasvu.⁶

Eriti probleemne on asjaolu, et suurem osa maksepettustest tulenevast kahjust jääb tarbijate ehk makseteenuse kasutajate kanda. 2024. aastal ulatus tarbijate kanda jäänud kahju Euroopa

⁴ Maksepettuste ülevaade 2025. Eesti Pank; Eesti Pangaliit; Politsei- ja Piirivalveamet 2025. - https://haldus.eestipank.ee/sites/default/files/2025-12/ep_maksepettuste-ulevaade-2025_0.pdf (06.02.2026).

⁵ Riigikogu. (2026). Küberkuritegevuse ohjeldamine finantsvaldkonnas - olulise tähtsusega riikliku küsimuse arutelu 19.02.2026. Istungi ülevaade. - <https://www.riigikogu.ee/istungi-ulevaated/riigikogu-arutas-olulise-riikliku-k-simusena-k-berkuritegevuse-ohjeldamist-finantsvaldkonnas/> (03.04.2026).

⁶ Report on payment fraud 2025 (EBA/REP/2025/40). European Banking Authority; European Central Bank 2025. - <https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202512.en.pdf> (09.02.2026).

Liidus ligikaudu 2,485 miljardi euron. ⁷ See viitab sellele, et kehtivad õiguslikud raamistikud ja finantsasutustele kohaldatud nõuded maksepettuste ärahoidmiseks ei pruugi siiski tõhusalt ennetada kuritegelikke skeeme.

Maksepettuste tõkestamise vajadust rõhutati ka 2025. aasta jaanuaris toimunud Maksekeskkonna Foorumi kohtumisel, kus otsiti lahendusi pettuste ennetamiseks ja nendest tulenevate kahjude vähendamiseks. Aruteludes toodi esile, et Euroopa Komisjon on juba 2023. aastal teinud ettepanekuid makseteenuste osutamise reeglite muutmiseks, mille eesmärk on suurendada tarbijakaitset ja parandada maksesüsteemide turvalisust. Muudatuste keskmes on muu hulgas pettustega seotud teabe parem jagamine makseteenuse pakkujate vahel, tarbijate teadlikkuse suurendamine ning maksete autoriseerimise nõuete täpsustamine, et vähendada pettuse mõjul tehtavate tehingute riski ⁸. Seni on pettuse mõjul sooritatud tehingute puhul vastutus finantsasutuse tasandil piirdunud peamiselt võlaõigusliku vastutusega, eelkõige makseteenuste regulatsioonist tuleneva kohustusega hüvitada teatud juhtudel kliendile tekitatud kahju. Euroopa Liidu makseteenuste määruse (The Payment Services Regulation, lühidalt PSR) ja kolmanda makseteenuste direktiivi (PSD3) kohaselt suureneb finantsasutuste hoolsuskohustus siiski märkimisväärselt. Nimetatud õigusaktid näevad ette, et makseteenuse pakkujad peavad rakendama tõhusaid pettuse ennetamise mehhanisme, kontrollima makse saaja nime ja unikaalse tunnuse vastavust, tagama tugeva kliendituvastuse ning viima läbi riskihindamisi. Samuti on nad kohustatud rakendama meetmeid pettuse riskide vähendamiseks, näiteks kululimiite ja tehingute blokeerimist, ning kandma vastutust kliendile tekkinud kahju hüvitamise eest juhul, kui nad ei ole oma kohustusi nõuetekohaselt täitnud. Arvestades hoolsuskohustuse selget laienemist, tekib õigustatud küsimus, kas ja millistel tingimustel võib hoolsusnõuete rikkumine tuua kaasa ka finantsasutuse karistusõigusliku vastutuse. ⁹ Kuigi PSD3 ja PSR keskenduvad eelkõige tsiviil- ja haldusvastutusele, ei ole välistatud, et korduvad või raskest hooletusest tingitud rikkumised võivad viia ka karistusõigusliku vastutuse kohaldamiseni, näiteks pettuse hõlbustamise või kliendi vara ohtu seadmise eest.

Käesoleva magistritöö teema valiku tingib vajadus selgitada, kas ja millistel tingimustel võib finantsasutus kanda karistusõiguslikku vastutust pettuse mõjul sooritatud tehingu eest

⁷ Report on payment fraud (viide 6).

⁸ Maksekeskkonna Foorumil otsiti lahendusi maksepettuste tõkestamiseks. - Eesti Pangaliit 16.01.2025 <https://pangaliit.ee/uudised-ja-teated/maksekeskkonna-foorumil-otsiti-lahendusi-maksepettuste-tokestamiseks> (06.02.2026).

⁹ Payment services deal: More protection from online fraud and hidden fees. European Parliament 27.11.2025. - <https://www.europarl.europa.eu/news/en/press-room/20251121IPR31540/payment-services-deal-more-protection-from-online-fraud-and-hidden-fees> (08.02.2026).

olukorras, kus tehing on formaalselt kliendi enda poolt algatatud ja nõuetekohaselt autoriseeritud. Teema aktuaalsus ei tulene üksnes maksepettuste arvu märgatavast kasvust, vaid eelkõige õigusliku ebamäärasuse olemasolust finantsasutuste vastutuse piiride osas. Praktikas tekib küsimus, kas olukordades, kus pank jätab täitmata seadusest või järelevalvepraktikast tulenevad hoolsusnõuded, saab rääkida üksnes võlaõiguslikust vastutusest või võib selline käitumine teatud juhtudel täita ka karistusõigusliku koosseisu tunnused.

Maksepettuste kontekstis võib olukord kujuneda selliseks, kus petturi tegevus realiseerub üksnes tänu sellele, et finantsasutus ei kasuta talle kättesaadavaid kontrolli- või sekkumisvõimalusi kliendi vara kaitsmisel. Sellisel juhul ei ole probleem üksnes petturi käitumises, vaid ka küsimuses, kas finantsasutuse tegevus või tegevusetus usaldussuhte raames on aidanud kaasa kliendi vara kahjustamisele viisil, mis võib olla karistusõiguslikult relevantne.

Karistusõigusliku vastutuse kontekstis on keskseks küsimuseks eeskätt Karistusseadustiku (edaspidi KarS) § 217² kohaldamisala ning selle seos finantsasutuse hoolsusnõuete täitmata jätmise või rikkumisega¹⁰. Nimetatud koosseis eeldab muu hulgas usaldussuhte olemasolu, tahtlikku käitumist ning kliendi vara kahjustamist usalduse kuritarvitamise kaudu. Finantsasutuse ja kliendi vahelise suhte eripära seisneb aga selles, et pank ei ole pelgalt tehingu tehniline vahendaja, vaid professionaalne teenuseosutaja, kellelt oodatakse kõrgendatud hoolsust, riskide hindamist ning pettusekahtluste korral sekkumist. Sellest tulenevalt tekib küsimus, kas ja millistel tingimustel võib finantsasutuse hoolsusnõuete täitmata jätmine või rikkumine kvalifitseeruda mitte üksnes tsiviilõiguslikuks rikkumiseks, vaid ka karistusõiguslikult etteheidetavaks teoks.

Tulenevalt eelnevast püstitab autor käesolevas magistritöös hüpoteesi, mille kohaselt võib finantsasutuse hoolsusnõuete täitmata jätmine või rikkumine teatud tingimustel kaasa tuua karistusõigusliku vastutuse KarS § 217² alusel, kui see võimaldab kliendi vara käsutamist pettuse mõjul. Hüpoteesi keskmes on eeldus, et finantsasutuse vastutus ei sõltu üksnes petturi tahtlusest, vaid ka panga enda käitumise kvaliteedist, sealhulgas riskihindamisest, tehingute monitoorimisest ning pettuse kahtluste korral rakendatud meetmetest.

Püstitatud hüpoteesist tuleneb töö keskne uurimisküsimus, milleks on: millised finantsasutuse hoolsusnõuete rikkumised ja millises ulatuses võivad täita KarS § 217² eeldusi maksepettuse võimaldamisel? Sellele küsimusele vastamiseks tuleb muuhulgas selgitada, millised pettuse

¹⁰ Karistusseadustik. - RT I, 22.12.2025, 2.

vormid KarS § 209 tähenduses võivad praktikas seonduda finantsasutuse tegevuse või tegevusetusega ning kuidas need olukorrad suhestuvad usalduse kuritarvitamise koosseisuga.

Uurimisküsimusele vastamiseks on magistritöös püstitatud mitmed uurimisülesanded. Esiteks analüüsitakse Eesti ja Euroopa Liidu õigusraamistikku, mis reguleerib finantsasutuste vastutust maksepettuste kontekstis, keskendudes kehtivatele hoolsusnõuetele ning KarS § 217² kohaldamisele. Teiseks uuritakse finantsasutuste hoolsusnõuete täitmata jätmise ja rikkumise seoseid karistusõigusliku vastutusega ning selgitatakse välja piir võlaõigusliku ja karistusõigusliku vastutuse vahel. Kolmandaks viiakse läbi võrdlev analüüs Euroopa Liidu liikmesriikide kohtupraktika põhjal, et hinnata, millistel juhtudel tekib finantsasutustel vastutus kliendile pettuse mõjul sooritatud tehingutega tekitatud kahju eest. Neljandaks koondatakse analüüsi tulemused ning esitatakse vajadusel ettepanekuid Eesti õiguse täiustamiseks, lähtudes töö käigus tuvastatud probleemidest ja parimatest praktikatest.

Magistritöö eesmärkide saavutamiseks kasutatakse peamiselt õigusdogmaatilist ja võrdlevat uurimismeetodit, mida täiendavad kohtupraktika analüüs ning normide süstemaatiline ja teleoloogiline tõlgendamine. Õigusdogmaatilist meetodit kasutatakse kehtiva õiguse analüüsimiseks ja süstematiseerimiseks, eeskätt usalduse kuritarvitamise koosseisu (KarS § 217²) sisulise ulatuse ning maksepettuste kontekstis selle koosseisu ja finantsasutuste hoolsusnõuete täitmise ulatuse omavahelise seose välja selgitamiseks. Dogmaatilise analüüsi käigus uuritakse finantsasutustele kehtestatud hoolsusnõudeid, nende eesmärki ning võimalikku seost karistusõigusliku vastutuse tekkimisega olukordades, kus pettuse mõjul sooritatakse kliendi vara kahjustavaid tehinguid. Võrdlevat meetodit rakendatakse Eesti regulatsiooni ja kohtupraktika võrdlemisel Euroopa Liidu regulatsiooni ning teiste liikmesriikide kohtupraktikaga, et hinnata, kas ja millisel määral on finantsasutustele omistatud vastutust pettuse mõjul sooritatud tehingute puhul ning milliseid lahendusi on erinevates õigussüsteemides kasutatud, sh kuidas finantsasutuste hoolsusnõudeid ja vastutuse piire on praktikas mõistetud ja kohaldatud. Võrdleva analüüsi eesmärk on tuvastada võimalikke alternatiivseid lähenemisi ja hinnata Eesti õiguse arenguvõimalusi. Õigusnormide tõlgendamisel kasutatakse süstemaatilist ja objektiivteleoloogilist meetodit, arvestades normide eesmärki, kohta õigussüsteemis ning maksepettuste ennetamise ja tarbijakaitsega seotud kaalutlusi. Vajadusel tuginetakse ka subjektiivteleoloogilisele tõlgendamisele õigusaktide seletuskirjade ja seadusandja eesmärkide analüüsi kaudu.

Tööd iseloomustavad märksõnad: karistusõigus, finantsregulatsioonid, hoolsusnõuded.

1. LÜHIÜLEVADE FINANTSSEKTORIS ENAMKASUTATAVATEST PETTUSTEST

Kaasaegses digitaalses- ja finantskeskkonnas on pettuste ilmnemisviisid muutunud äärmiselt mitmekesiseks ning dünaamiliseks. Pettused võivad avalduda nii traditsiooniliste lepinguliste skeemide, investeerimispettuste, identiteedivarguste kui ka tehnoloogiapõhiste maksepettustena.

Eesti Vabariigis petturi tel on kasutuselt väga palju erinevaid pettuse liike. Pettus on tänapäeval muutunud omaette kõrgetasemeliseks tööstusharuks, mille tööriistadeks on andmepüük, spetsiaalsed tööriistad ja manipuleerimistaktikad. Pettuseid liigitatakse kolme gruppi: 1) autoriseeritud maksed, 2) andmepüük ja identiteedivargus ning 3) kaardipettused.¹¹

Autoriseeritud maksed on sellised, mida ohver algatab ja kinnitab oma tahtel, kuid teeb seda petturite innustamisel. Autoriseeritud maksete hulka kuuluvad ostupettus, investeerimispettus, romantikapettus, ettemaksupettus, äriühingute puhul kasutatavad maksejuhise muutmine ehk arvepettus ning CEO- ehk juhipettus, pangatöötaja, politseiniku või muu ametnikuna esinemise pettus. Ostupettuseks on juhtumid, kus ohver sooritab interneti kaudu ostu ning müüjast pettur kaob pangaülekande laekumise järgselt. Investeerimispettusteks loetakse juhtumeid, mil ohvrile pakutakse näilikult kasumlikku investeerimisvõimalust telefoni või internetireklaami kaudu. Investeerimispettuste näideteks võib pidada ettemaksupettust, erinevaid skeeme nagu näiteks püramiidskeemid, kus skeemi vanemad osalised saavad tulu uute osaliste pealt ning turuga manipuleerimise skeemid¹². Petturid võivad esitleda võltsitud ettevõtete osakud või aktsiad kui uut äri võimalust, pakkuda võimalust osaleda kinnisvara projektides või kindlustuse skeemides¹³. Ettemaksupettuse korral paluvad petturid ohvrit lühiajalist rahalist abi maksu või muu rahalise vajaduse katmiseks ning lubavad rohkem raha tagasi maksta (Nigeeria printsi näide). Ettemaksupettusele sarnaste tunnustega on romantika- ehk armupettused, millede puhul kasutatakse võltsprofili ohvri usalduse saamiseks ja temaga armusuhte loomiseks kohtingukeskonna kaudu. Usalduse saavutamisel palutakse kiiret ja suurt rahalist abi. Turuga manipuleerimise korral luuakse petturite poolt kunstlikult ostusurve teatud väärtpaberile, mis on emiteeritud börsivälisel väärtpaberiturul. Kunstlikult ostusurve loomisel tõstetakse väärtpaberi hinda, millega väärtpaber hiljem müüakse maha ja seekaudu

¹¹ Maksepettuste ülevaade 2025. Eesti Pank; Eesti Pangaliit; Politsei- ja Piirivalveamet 2025. - https://haldus.eestipank.ee/sites/default/files/2025-12/ep_maksepettuste-ulevaade-2025_0.pdf (06.02.2026).

¹² Federal Bureau of Investigation (n.d.) Common frauds and scams. - <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams> (10.02.2026).

¹³ Reurink, A. (2016). Financial Fraud: A Literature Review. MPIfG Discussion Paper 16/5, 47-49. - https://www.researchgate.net/publication/303517861_Financial_Fraud_A_Literature_Review#pf33 (11.02.2026).

tekitatakse investoritele kahju¹⁴. Maksejuhise muutmise ehk äriühingute arvepettuste puhul saadetakse äriklientidele võltsarve või kiri äriühingu kontoandmete muutmise kohta. Juhipettuse korral esinevad petturid äriühingu tippjuhina, kasutades selleks tehisaru (tehes selle kaudu võltsvideoid ja -helifaile, et raamatupidajat eksitades teha kiireloomulised ülekanded) või kompromiteeritud e-posti aadressi. Kõige levinumaks skeemiks on pangatöötajana või politseinikuna esinemise pettus, mille toimepanemisel, hoiatatakse kontohäkkimise eest ja veendakse ohvrit kanda raha turvakontole üle ja uuendada andmeid, saavutades seekaudu ligipääs rahalistele vahenditele turvakontol. Muude ametnikena (tervisekassa, kindlustusettevõtte) esinemise pettuste korral on sarnane eelmisega skeem, kuid makse suunatakse otse oma kontole või rakendatakse kaheastmelised skeemid, millede puhul toimub kaks kõnet - esimesel kogutakse andmeid ohvri kohta ning teisel juba hirmutatakse, et esimene kõne toimus petturite poolt ning on vaja kiireloomuliselt oma andmeid ja tehingud kinnitada, et ärahoida kahju tekkimist.¹⁵

Andmepüügi ja identiteedivarguse alla kuuluvad e-posti andmepüük ehk *phishing*, petusõnumid ehk *smishing*, häälandmepüük ehk *vishing*, Qr-koodi pettus ehk *quishing* ning reklaamipettus. *Phishing* ehk õngitsemine on kõige levinum manipuleerimisründe meetod, mille kaudu saab ohver näiliselt e-kirja kas pangalt või teiselt teenusepakkujalt korraldusega viivitamatult asutuse veebikeskkonda siseneda eesmärgiga ennetada kahju tekkimist. Võltsitud sisselogimislehele autentides, edastab ohver petturitele oma isikuandmeid, sealhulgas kaardiandmeid¹⁶. *Smishing*'u puhul kasutatakse võltsitud numbrit, et saata ohvrile sõnum meelitamaks teda oma kaardiandmeid või elektroonilise identiteedi (lühidalt ja edaspidi e-ID) PIN-koode avaldama selle kaudu, et palutakse maksta paki teenustasu või tollimaks. *Vishing* on Eestis viimastel aastatel üsna levinuks muutunud pettusskeem, mis sarnaneb õngitsemisega, kus pettur esineb telefonikõnes ametnikuna, näiteks kodupanga töötajana, ning petab välja kaardiandmeid või e-ID PIN-koode. QR-koodi pettus ehk *quishing* on uuem pettusevorm, kus petturid kleeбивad enda loodud QR-koodi originaalse QR-koodi peale, lootes, et inimesed sisestavad seda kasutades oma andmeid. Reklaamipettus tavaliselt toimub internetireklaami või bannerina, kus lubatakse mõnest veebikeskkonnast soodsa intressiga kiirlaenu, mille saamiseks on vaja vaid täita vorm, kuid tegelikkuses sellega avaldatakse petturitele oma isikuandmeid.¹⁷

¹⁴ Federal Bureau of Investigation (n.d.) Common frauds and scams. - <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams> (10.02.2026).

¹⁵ Maksepettuste ülevaade 2025. Eesti Pank; Eesti Pangaliit; Politsei- ja Piirivalveamet 2025. - https://haldus.eestipank.ee/sites/default/files/2025-12/ep_maksepettuste-ulevaade-2025_0.pdf (06.02.2026).

¹⁶ Reurink, A. (2016). Financial Fraud: A Literature Review. MPiFG Discussion Paper 16/5, 47-49. - https://www.researchgate.net/publication/303517861_Financial_Fraud_A_Literature_Review#pf33 (11.02.2026)

¹⁷ Maksepettuste ülevaade 2025. Eesti Pank; Eesti Pangaliit; Politsei- ja Piirivalveamet 2025. - https://haldus.eestipank.ee/sites/default/files/2025-12/ep_maksepettuste-ulevaade-2025_0.pdf (06.02.2026).

Kaardipettused hõlmavad kaardi vargust või kaotust, *card-not-present* ehk CNP-pettust, kaardi kopeerimist ehk skimmimist, *point-of-sale* ehk POSi-pettust, ATMi-pettust ehk sularahaautomaadipettust. Kaardi varguse või kaotuse korral satub kaart võõrastesse kätte ja seda kasutatakse võimalikult paljudeks makseteks, enne kui jõutakse konto ära blokeerida. *Card-not-present* pettused moodustuvad Euroopa Keskpanga andmetel ligi 80% kõikidest ühtse euromaksete piirkonnas (SEPA piirkond) tuvastatud kaardipettustest¹⁸. CNP-pettus on kaardipettus, mille toimepanemiseks ei ole petturile vajalik füüsiline pangakaart, vaid piisab pangakaardi andmetest. Kaardi kopeerimine ehk *skimmimine* leiab aset ennekõike siis, kui ohver sisestab kaardi sularahaautomaati või terminali, kuhu on paigaldatud magnetriba kopeeriv seade, mille abil luuakse kaardist ebaseaduslik dublikaat. *Point-of-sale* toimepanemisel makseterminalis mängitakse hinnaga, lootes, et tähelepanematu või joobes ohver maksab suuremat summat. Samuti võidakse kaardilt võtta raha mitu korda või paigaldatakse makseterminali sisse skimmimisseade. Sularahaautomaadipettused võivad esineda mitmel moel, näiteks manipuleerides ohvrit pangaautomaadist sularaha võtmiseks ja petturile andmiseks.¹⁹

Käesolevas töös keskendutakse eelkõige petukõnedele, sealhulgas õngitsuskõnedele (*vishing*), mis on Eestis kiiresti leviv ja majanduslikku kahju põhjustav pettuse vorm. See näide võimaldab selgelt demonstreerida KarS §-i 209 koosseisu elementide praktilist toimimist ning illustreerib, kuidas pettus reaalses elus avaldub. Tavaliselt esitavad petturid end mõne usaldusväärse asutuse, organisatsiooni või panga esindajana, kasutades korrektset eesti keelt ja professionaalset kommunikatsiooni. Kõnede peamine eesmärk on mõjutada ohvrit tegutsema viisil, mis võimaldab kurjategijal ligipääsu ohvri pangakontole või muudele finantsvahenditele. Petukõned toimuvad tavaliselt mitmeastmelise skeemi järgi. Esimeses kõnes esitatakse ohvrile kiireloomuline või ahvatlev teade, näiteks kasutamata hüvitise tagastamine, kahtlased tehingud pangakontol või võimalus kiireks rahateenimiseks. Sellise kõne eesmärgiks on tekitada emotsionaalne surve ja kiirustamise tunne. Kõige levinum meetod on panna ohver Smart-ID või Mobiil-ID abil tehinguid kinnitama, sageli pannes kannatanu uskuma, et tegemist on turvalise või isegi hädaolukorra lahendava tegevusega. Järgmised kõned toimuvad siis, kui ohver ei reageeri esimese kõne peale ning petturite eesmärk jääb saavutamata. Sellistel juhtudel helistatakse uuesti ja väidetakse, et eelmine kõne oli kelmide poolt ja et olukorra lahendamiseks on vaja panka sisse logida ning kinnitada

¹⁸ Seventh report on card fraud. European Central Bank (2021). -

<https://www.ecb.europa.eu/press/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html> (15.02.2026).

¹⁹ Maksepettuste ülevaade 2025. Eesti Pank; Eesti Pangaliit; Politsei- ja Piirivalveamet 2025. - https://haldus.eestipank.ee/sites/default/files/2025-12/ep_maksepettuste-ulevaade-2025_0.pdf (06.02.2026).

tehingud Smart-ID või Mobiil-ID PIN-koodide kaudu. Tegelikult annab ohver sellega kurjategijale juurdepääsu oma rahalistele vahenditele (*vishing*).

Petukõnede skeemi tunnusjooned on emotsionaalne manipuleerimine, kiire tegutsemise surve ning kannatanu veenmine, et tegemist on usaldusväärse või hädavajaliku tegevusega. Petukõnede eripära seisneb ka selles, et need on muutunud väga realistlikuks ja keerukaks, nii et kogenud pangakliendidki võivad ohvriks langeda.²⁰

²⁰ Petukõned. Riigi Infosüsteemi Amet. - <https://www.itvaatlik.ee/levinud-pettused/petukoned/> (10.02.2026).

2. FINANTSASUTUSTE HOOLSUSNÕUETE ÕIGUSLIK RAAMISTIK

Digitaalsete finantsteenuste areng on loonud keskkonda, kus tehinguid tehakse kiiresti ja sageli täielikult kaugteel, sealhulgas välgmaksetena, mille täitmine toimub mõne sekundi jooksul. Sellises keskkonnas suureneb risk, et klient teeb tehingu küll ise ja kasutab nõuetekohaselt oma autentimisvahendeid, kuid teeb seda petturi antud eksitava teabe mõjul. Petukõnede ja muude sotsiaalse manipulatsiooni skeemide puhul ei pruugi finantsasutust eksitada mitte tehniline turvanõrkus, vaid kliendi tahe, mis on kujundatud eksitamise või surve teel. Sellisel juhul on tehing formaalselt autoriseeritud, kuid sisuliselt tehtud pettuse mõjul. Praktikas finantsasutusel ei pruugi olla võimalik tehingusse sekkuda, eriti välgmaksete puhul, mistõttu keskseks küsimuseks on, milline on finantsasutuse hoolsusnõuete ulatus olukorras, kus tehnilised turvameetmed on järgitud, kuid pettus realiseerub kliendi mõjutamise kaudu.

2.1. Finantsasutuste hoolsusnõuded Euroopa Liidu õiguses

Finantsasutuste, sealhulgas makseteenuse pakkujate tegevust Euroopa Liidus reguleerib Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/2366, 25. november 2015, makseteenuste kohta siseturul (Payment Services Directive 2, lühidalt ja edaspidi PSD2), mille eesmärk on tagada ühtse ja turvalise makseteenuste turu toimimine. PSD2 preambulas rõhutatakse, et elektrooniliste maksete kasutamise kasvuga on suurenenud ka turvariskid, mistõttu tuleb makseteenuste kasutajatele tagada piisav kaitse ning makseteenuste turvaline toimimine. Samuti märgitakse, et makseteenuste regulatsiooni eesmärk on parandada makseteenuste turu tõhusust, suurendada konkurentsi ning tugevdada tarbijakaitset.²¹ Sellest tulenevalt on makseteenuste regulatsiooni keskseks eesmärgiks tagada usaldusväärne ja turvaline maksekeskkond, milles makseteenuse kasutajad saavad oma maksetehinguid teha ilma põhjendamatute riskideta.

PSD2 preambulas rõhutatakse ka vajadust kaitsta makseteenuse kasutajate rahalisi vahendeid ning ennetada pettusi ja volitamata juurdepääsu maksekontodele. Eelkõige tuuakse esile isikustatud turvavolituste turvalise hoidmise tähtsus, et vältida maksekontodele loata juurdepääsu ning kaitsta kasutajate vahendeid²². Sellest võib järeldada, et makseteenuse pakkujatel eeldatakse selliste tehniliste ja organisatsiooniliste meetmete rakendamist, mis vähendavad loata juurdepääsu riski ning tagavad makseteenuste turvalise kasutamise.

²¹ 25. novembri 2015. aasta Euroopa Parlamendi ja nõukogu direktiiv 2015/2366 makseteenuste kohta siseturul (PSD2). - ELT L 337, 23.12.2015, lk 2.

²² *Ibid*, lk 12.

Samuti käsitletakse PSD2 preambulas autoriseerimata maksetehingute riski ning vastutuse jaotust makseteenuse kasutaja ja makseteenuse pakkuja vahel. PSD2 kohaselt peab makseteenuse pakkuja üldjuhul autoriseerimata maksetehingu korral viivitamata tagastama maksesumma makseteenuse kasutajale, välja arvatud juhul, kui kasutaja on tegutsenud pettuse eesmärgil või raskest hooletusest²³. PSD2 ei sätesta otseselt kohustust vältida aurotiseerimata maksetehinguid, kuid vastutuse jaotus näitab, et autoriseerimata tehingu korral kannab esmase vastutuse makseteenuse pakkuja. Selline vastutuse jaotus näitab, et seadusandja on pidanud vajalikuks tagada makseteenuse kasutajatele kõrgetasemeline kaitse ning suunata makseteenuse pakkujaid rakendama meetmeid, mis vähendavad või ennetavad autoriseerimata tehingute riski.

PSD2 preambulas rõhutatakse ka makseteenuse pakkujate rolli maksetehingute korrektse täitmise tagamisel. Maksesüsteemi tõhus toimimine sõltub sellest, kas makseteenuse kasutaja saab olla kindel, et makseteenuse pakkuja täidab maksetehingu korrektselt ja kokkulepitud aja jooksul. Sellest tulenevalt nähakse ette, et makseteenuse pakkuja vastutab kasutajalt vastu võetud maksetehingu nõuetekohase täitmise eest, sealhulgas maksesumma õige ülekandmise ja täitmisaja järgimise eest. Samuti vastutab maksja makseteenuse pakkuja makseahelasse kaasatud vahendajate vigade eest kuni makse laekumiseni makse saaja kontole.²⁴ See viitab sellele, et makseteenuse pakkujale on maksetehingu täitmise protsessis antud suurim roll ning kontrolli maksetehingu täitmise üle omab eelkõige makseteenuse pakkuja, mistõttu on makseteenuse pakkuja kohustatud tegutsema nõuetekohase hoolsusega. Makseteenuse pakkuja kohustus ei piirdu üksnes maksekäsundi tehnilise täitmisega, vaid nõuetekohase hoolsusega tegutsemine eeldab eelkõige maksetehingu andmete kontrollimist, et vähendada ekslike või väärte maksetehingute tekkimise riski²⁵.

Makseteenuste turvalisuse tagamiseks nähakse PSD2 direktiivis ette ka makseteenuse pakkujate kohustus rakendada asjakohaseid turvameetmeid ja riskijuhtimise mehhanisme. PSD2 preambula kohaselt vastutavad makseteenuse pakkujad turvameetmete eest ning peavad looma raamistiku turvariskide maandamiseks ja intsidentide tõhusaks juhtimiseks. Samuti peavad nad hindama makseteenustega seotud turvariske ning teavitama pädevaid asutusi olulistest turvaintsidentidest.²⁶ Selline regulatsioon viitab sellele, et makseteenuse pakkujatel lasub aktiivne kohustus hinnata makseteenustega seotud riske ning rakendada meetmeid nende riskide maandamiseks.

²³ PSD2 (viide 21), lk 12-13.

²⁴ *Ibid*, lk 15.

²⁵ *Ibid*, lk 16.

²⁶ *Ibid*, lk 16.

Elektrooniliste maksete turvalisuse olulisust rõhutatakse ka seoses autentimismehhanismidega. PSD2 kohaselt tuleb elektroonilisi makseteenuseid osutada turvaliselt, kasutades tehnoloogiat, mis võimaldab kasutaja turvalist autentimist ning vähendab maksimaalselt pettuse ohtu. Turvameetmed peavad olema kooskõlas makseteenusega seotud riskitasemega ning hõlmama muu hulgas isikustatud turvavolituste konfidentsiaalsuse ja terviklikkuse kaitset, näiteks autentimiskoodide või ühekordsete salasõnade kasutamist.²⁷ Nimetatud sätted viitavad sellele, et makseteenuse pakkujalt oodatakse selliste autentimis- ja turvameetmete rakendamist, mis vähendavad maksepettuste ning autoriseerimata maksetehingute tekkimise võimalust.

Eeltoodust tulenevalt võib järeldada, et Euroopa Liidu seadusandja eesmärk on tagada makseteenuste turvaline toimimine ning makseteenuse kasutajate tõhus kaitse maksepettuste ja autoriseerimata maksetehingute eest. Eelnimetatud põhimõtted loovad aluse konkreetsematele hooleksusnõuetele, mis tulenevad direktiivi sätetest ning mille eesmärk on ennetada pettusi ja tagada makseteenuste turvaline osutamine.

2.1.1. Makseteenuse kasutaja autentimise kohustus

PSD2 direktiivi artikli 4 punkti 29 kohaselt hõlmab autentimine mistahes toimingut, mis võimaldab makseteenuse pakkujal kindlaks teha kasutaja identiteedi või makseinstrumendi kehtivuse, sealhulgas isikustatud turvavolituste kasutamise²⁸. Autentimise kohustus kehtib kõigi maksete puhul ja moodustab PSD2 aluse hooleksusmeetmete rakendamiseks. Autori hinnangul tähendab see, et makseteenuse pakkuja peab igal juhul tagama, et tehingut algatav isik on õiguspärane kasutaja ning et makseinstrumendi volitus on kontrollitud. PSD2 reguleerib tugeva kliendi autentimise (Strong Customer Authentication, lühidalt ja edaspidi SCA) kohaldamist, mis on autentimise eriliik ning kohaldub eelkõige olukordades, kus maksetehingud viiakse läbi elektrooniliselt või kaugjuurdepääsu kaudu ning kus pettuse või kuritarvitamise risk on märkimisväärt. PSD2 defineerib SCA-d selliselt, et autentimine nõuab vähemalt kahte sõltumatu elementi kombinatsiooni kolmest kategooriast: teadmised, omamine ja tunnus - ning nende elementide vastastikune sõltumatus peab tagama, et ühe elemendi rikkumine ei ohustaks teisi elemente. Preambulas rõhutatakse SCA olulisust riskide maandamisel ja turvalisuse tagamisel, millest võib järeldada, et autentimine kujutab üldist hooleksusnõuet, samas kui tugev kliendi autentimine on PSD2 poolt kehtestatud hooleksusnõue kõrge riskiga tehingute turvalisuse tagamiseks. Selline eristamine võimaldab käesoleva magistritöö raames analüüsida finantsasutuse kohustusi ja nende täitmist, sealhulgas

²⁷ PSD2 (viide 21), lk 17.

²⁸ *Ibid*, lk 24.

petukõnede ja autoriseerimata maksete kontekstis, kus SCA rakendamine on võtmetähtsusega pettuse riski maandamiseks.

Käesolevas magistritöös on muuhulgas oluline eristada kahte erinevat olukorda: esiteks juhtumeid, kus makseteenuse kasutaja autoriseerib maksetehingu ise pettuse mõjul, näiteks petukõne kaudu loodud eksitava olukorra tõttu, mille tulemusena klient logib internetipanka ning kinnitab tehingu ning teiseks juhtumeid, kus makseteenuse pakkuja ennast eksitatakse, kui kolmas isik omandab ebaseaduslikult ligipääsu maksekontole ja teeb tehingu ilma tegeliku kasutaja nõusolekuta.

Eeltoodust tulenevalt, kuigi PSD2 sätestab üldise autentimise kohustuse siiski kõigi maksete puhul, keskendub magistritöö autor tugevale kliendi autentimisele, kuna just SCA rakendamine võimaldab hinnata finantsasutuse riskipõhise hoolsusnõude täitmist ning tuvastada olukordi, kus pettuseoht on suurem. SCA on oluline, sest see vähendab autoriseerimata tehingute riski. PSD2 direktiivi artikli 64 kohaselt loetakse maksetehing autoriseerituks ainult siis, kui maksja on andnud nõusoleku tehingu täitmiseks - kui nõusolek puudub, käsitletakse maksetehingut autoriseerimata maksetehinguna. Pettusejuhtumi analüüsimisel ning vastutuse määramisel makseteenuse kasutaja kahju eest on esmalt vajalik tuvastada, kas maksetehing oli autoriseeritud või autoriseerimata. Autor järeldeb, et tehingu iseloomust sõltub, millised õiguslikud kohustused makseteenuse pakkujal tekivad ning milline hoolsusnõuete raamistik on kohaldatav. Alles pärast tehingu iseloomu väljaselgitamist tuleb hinnata, kas makseteenuse pakkuja on täitnud talle PSD2 direktiivist tuleneva kohustuse rakendada tugevat kliendi autentimist ning kas hoolsusnõuded on täidetud. Tugeva kliendi autentimise kohustuse rikkumine kujutab autori hinnangul sellises olukorras olulist alust vastutuse hindamiseks ning võib moodustada eelduse ka võimaliku karistusõigusliku vastutuse kaalumiseks, kuna see võib tähendada, et finantsasutus ei ole täitnud kohustuslikke hoolsusnõudeid.

Artikli 97 lõike 1 kohaselt peavad liikmesriigid tagama, et makseteenuse pakkuja kasutab tugevat kliendi autentimist juhul, kui maksja (a) soovib pääseda ligi oma maksekontole interneti kaudu, (b) algatab elektroonilise maksetehingu või (c) teeb kaugejuurdepääsu teel mis tahes muu toimingut, millega võib kaasneda maksepettuse või muu kuritarvitamise risk²⁹.

Juba lõike 1 sõnastus näitab, et liidu seadusandja on sidunud tugeva kliendi autentimise kohustuse otseselt pettuseriskiga. Petukõnede kontekstis kvalifitseerub kliendi poolt internetipangas või mobiilirakenduses algatatud makse vaieldamatult artikli 97 lõike 1 punktis

²⁹ PSD2 (viide 21), art 97.

b nimetatud elektrooniliseks maksetehinguks. Seega on tugeva kliendi autentimise kohaldamine sellisel juhul õiguslik kohustus. Siiski tuleb rõhutada, et petukõnede kontekstis ei seisne probleem selles, et makseteenuse pakkuja oleks autentimise kohustust rikkunud, vaid probleem on kliendi otsuse ja petturi mõjuga seotud riskides. Autentimise probleem leiaks aset siis, kui kolmas isik esineb kliendina ning omandab ebaseaduslikult ligipääsu maksekontole, kust teeb tehinguid. Sellises olukorras oleks tehing tehniliselt autoriseerimata. Samas, panga vaates loetakse klient õiguspäraselt autendituks ning tehing õiguspäraselt autoriseerituks, kuna see on kinnitatud makseinstrumendi volituse alusel. Sellistes olukordades eeldatakse, et makseteenuse pakkuja võiks rakendada täiendavaid turvameetmeid, mis võimaldaksid tuvastada, et makseinstrumendi volitus ei pruugi olla tegelikult kliendi enda käes ning sekkuda riskide vähendamiseks. Kõik eelnimetatud asjaolud viitavad sellele, et tuleb keskenduda seega pigem makseteenuse pakkuja kehtestatud turvameetmete ja tehingu seire süsteemide olemasolule, mis võivad tuvastada ebatavalisi või kõrge riskiga tehingumustreid ning seeläbi hinnata, kas tegemist on olukorraga, kus tehingu algatab klient petturi eksituse mõjul, või olukorraga, kus tehingu teostab kolmas isik ilma kliendi tegeliku nõusolekuta. Mõlemal juhul on tegemist pettusega, kuid nende õiguslik kvalifikatsioon ja sellest tulenevad tagajärjed makseteenuse pakkuja vastutuse seisukohalt on erinevad.

Digitaalsete maksete turvalisuse tagamiseks ei piirdunud liidu seadusandja siiski üksnes artikli 97 üldise kohustuse sätestamisega. PSD2 direktiivi artikli 98 alusel töötas Euroopa Pangandusjärelevalve (European Banking Authority, lühidalt ja edaspidi EBA) välja tehnilised regulatiivsed standardid tugeva kliendi autentimise ja turvalise kommunikatsiooni kohta, mis on kehtestatud Komisjoni Delegeeritud määruse (EU) 2018/389 (The proposed Regulatory Technical Standards on strong customer authentication and secure communication are key to achieving the objective of the PSD2, lühidalt ja edaspidi RTS). Nimetatud standardid täpsustavad, milliseid tehnilisi ja organisatsioonilisi meetmeid peavad makseteenuse pakkujad rakendama, et artiklis 97 sätestatud autentimisnõuded oleksid praktikas tõhusad.

Tugev kliendi autentimine põhinema vähemalt kahel sõltumatul autentimiselemendil kolmest kategooriast: teadmine (näiteks parool või PIN-kood), omamine (näiteks füüsiline seade või autentimistoken) ning pärilikkus ehk kasutajale omane tunnus, nagu biomeetriline identifikaator. Nende elementide kasutamine peab olema korraldatud viisil, mis tagab nende

vastastikuse sõltumatuse ning välistab olukorra, kus ühe autentimiselemendi rikkumine ohustab teiste elementide turvalisust.³⁰

Lisaks sätestavad EBA standardid, et elektroonilise maksetehingu autentimine peab olema seotud konkreetse tehinguga. See tähendab, et autentimisprotsess peab hõlmama nn dünaamilist linkimist, mille käigus seotakse autentimiskood konkreetse makse summa ja saajaga, nii et nende andmete muutmisel muutub autentimiskood automaatselt kehtetuks.³¹ Sellise mehhanismi eesmärk on vähendada riski, et maksetehingut manipuleeritakse või suunatakse pettuse teel kolmandale isikule. Praktikast tähendab see, et enne tehingu kinnitamist kuvatakse kliendile tehingu põhiaandmed - eelkõige summa ja saaja - ning autentimisvahend (nt mobiilirakendus või muu lahendus) seob kinnituse tehniliselt nende andmetega. Autori hinnangul on selline mehhanism loodud eeskätt kaitsmiseks tehniliste manipulatsioonide või andmete vahelt muutmise eest. Samas ei pruugi see toimida piisava kaitsemeetodina. Paraku maksepettuste kasvutempo näitab, et petturid manipuleerivad inimesi niivõrd oskuslikult, et klient annab kinnituse olukorras, kus ta ei pruugi tehingu ehk kuvatud andmete tegelikke asjaolusid adekvaatselt tajuda ning loetakse paraku formaalselt korrektse kinnituse andmisel tehing õiguspäraselt autoriseerituks. Autori hinnangul peaks kliendi kinnitus sellisel juhul andma makseteenuse pakkuja reaalajas signaali, võimaldades hinnata tehingu riski ning rakendada vajadusel täiendavaid turvameetmeid, näiteks tehingu peatamist ja täiendava kinnituse nõudmist.

EBA regulatsioon rõhutab samas, et makseteenuse pakkujad peavad kasutama tehinguseire mehhanisme, mis võimaldavad tuvastada autoriseerimata või pettuslikke maksetehinguid ning hinnata iga tehingu riski erinevate indikaatorite alusel. Riskihindamisel tuleb arvesse võtta muu hulgas maksetehingu summat, kasutatavat seadet, võimalikku pahavara olemasolu ning ebatavalisi kasutusmustreid.³² Selline riskipõhine lähenemine näitab, et tugev kliendi autentimine ei ole käsitatav üksnes tehnilise autentimisprotseduurina, vaid laiemalt pettuste ennetamise süsteemi osana, mille eesmärk on tuvastada ka ebatavalisi või potentsiaalselt pettuslikke tehinguid enne nende lõplikku täitmist. Autori hinnangul eeltoodu näitab samuti, et kliendi poolt tehingu kinnitamisel peab makseteenuse pakkuja siiski jätma endale võimalust reageerida vajadusel enne, kui tehing rahaliselt realiseerub.

Petukõnede kontekstis omab see erilist tähendust. Kuigi klient võib maksetehingu tehniliselt korrektselt autentida, võivad tehingu asjaolud siiski viidata suurenenud pettuseriskile, näiteks

³⁰ PSD2 (viide 21), art 4 p 30.

³¹ 27. novembri 2017. aasta komisjoni delegeeritud määrus 2018/389, millega täiendatakse EL-i 2015/2366 regulatiivsete tehniliste standarditega, mis käsitlevad kliendi tugevat autentimist ning ühiseid ja turvalisi teabevahetuse avatud standardeid (RTS). - ELT L 69, lk 1.

³² *Ibid*, lk 5,6.

juhul, kui tegemist on ebatavaliselt suure maksega või maksega uuele saajale. Sellistes olukordades võivad EBA standardites ettenähtud riskihindamise ja tehingu seire mehhanismid olla olulised vahendid pettuse avastamiseks või selle riski vähendamiseks. Seejuures on oluline eristada olukordi, kus tehingu algatab formaalselt klient ise petturi eksituse mõjul, ning olukordi, kus tehingu teostab kolmas isik ilma kliendi tegeliku nõusolekuta. Just selliste indikaatorite olemasolu või puudumine võib osutada oluliseks ka käesolevas magistritöös käsitletava vastutuse hindamisel. Esimesel juhul on tegemist küll autoriseeritud tehinguga, kuid pettuse mõjul, samas kui teisel juhul võib tegemist olla autoriseerimata tehinguga, mis võib viidata võimalikele puudustele autentimissüsteemis, kus kolmas isik on saanud ebaseaduslikult ligipääsu maksekontole ja teostab tehinguid kliendi nimel. Samas, praktikas ei ole makseteenuse pakkujal alati võimalik tuvastada, et maksekontole on ligipääsu saanud kolmas isik, eriti olukordades, kus kasutatakse kliendi tegelikke autentimisvahendeid ja tehing ei erine oluliselt kliendi tavapärasest käitumismustrist. Samas võivad teatud objektiivsed indikaatorid, nagu ebatavaline seade, asukoht või tehingumuster, viidata võimalikule ebaseaduslikule ligipääsule ning sellisel juhul eeldatakse makseteenuse pakkujalt täiendavate kontrollimeetmete rakendamist. Kui makseteenuse pakkuja ei ole rakendanud mehhanisme, mis võimaldaksid tuvastada tehingute puhul pettusele viitavaid näitajaid või ei ole loonud süsteemi, mis võimaldaks selliste indikaatorite ilmnemisel tehingut täiendavalt hinnata, võib tekkida küsimus, kas finantsasutus on täitnud talle Euroopa Liidu õigusest tulenevad hoolsusnõuded. Puudulik mehhanismide rakendamine võib samuti olla käsitletav Euroopa Liidu õigusest tulenevate hoolsusnõuete rikkumisena, eelkõige olukordades, kus makseteenuse pakkuja ei ole suutnud eristada pettuse mõjul tehtud tehinguid juhtudest, kus makseinstrument on sattunud kolmanda isiku valdusesse. Sellisel juhul võib kaaluda, kas turvameetmete või tehingu seire süsteemide puudulikkus on loonud olukorda, kus finantsasutus ei ole olnud võimeline reageerima ilmsetele indikaatoritele, mis viitasid võimalikule pettusele. Käesolevas magistritöös analüüsitakse, kas ja millistel tingimustel võiks selline olukord kujutada endast eeltingimust finantsasutuse võimaliku karistusõigusliku vastutuse hindamisel. Samas tuleb rõhutada, et vastutuse tekkimine sõltub alati konkreetsetest asjaoludest, sealhulgas turvameetmete ulatusest, rakendatud kontrollisüsteemide tõhususest ning sellest, kas pettuseriski oli objektiivselt võimalik mõistlikult ette näha ja ennetada.

Artikli 97 lõige 2 täpsustab, et elektrooniliste kaugmaksetehingute puhul peab tugev kliendi autentimine hõlmama elemente, millega seostatakse tehing dünaamiliselt konkreetse summa ja konkreetse makse saajaga. Dünaamilise sidumise nõue tähendab, et autentimisprotsess peab olema tehniliselt üles ehitatud viisil, mis välistab autentimiskinnituse „üldise“ või määratlemata kasutuse. Teisisõnu, peab kliendi antud kinnitus olema seotud just selle

konkreetses maksega, selle konkreetse saaja ja summaga. Sellise regulatsiooni eesmärk on tagada, et kliendi tahteavaldus ei oleks abstraktne või korduvkasutatav, vaid seotud selgelt identifitseeritava tehinguga. Kui makse summa või saaja andmed muutuvad, peab muutuma ka autentimiskinnitus, varasem kinnitus ei tohi jääda kehtima. Seeläbi vähendatakse riski, et kolmas isik muudab makseandmeid kliendi teadmata pärast seda, kui klient on andnud oma autentimiskinnituse. Praktikas tähendab see, et enne kinnitamist kuvatakse kliendile tehingu põhiandmed - eelkõige summa ja saaja - ning autentimisvahend (nt mobiilirakendus või muu lahendus) seob kinnituse tehniliselt nende andmetega. Selline mehhanism kaitseb eeskätt tehniliste manipulatsioonide või andmete vahelt muutmise eest. Petukõnede puhul täidab dünaamiline sidumine kahte erinevat funktsiooni. Ühelt poolt võib see vähendada riski, et klient kinnitab teadmatuses teistsuguse summa või saaja kasuks tehtava makse, kui talle kuvatakse selgelt makseandmed. Teiselt poolt ei kõrvalda see olukorda, kus klient - olles petturi eksitava mõjutuse all - kinnitab teadlikult just selle summa ja saaja, kelle pettur on talle ette andnud. Riigikogu arutelu küberkuritegevuse teemal toob esile, et isegi kui pangatöötajad tuvastavad, et klient on pettuse ohver, ei ole neil õigust keelduda tehingu tegemisest, kui klient on kindel oma tegevuses. Swedbanki finantskuritegude tõkestamise divisjoni direktor Raul Vahtra selgitas, et klient võib jääda oma valikute juurde ning nõuda ülekande tegemist, isegi kui on ilmne, et tegemist on kelmustega.³³ Sellest järeldub, et artikli 97 nõuete formaalne täitmine ei pruugi igas olukorras välistada pettuse realiseerumist, kuid see kujundab siiski kohustuslikku sammu, mille täitmata jätmine võib viidata hoolsuskohustuse rikkumisele. Dünaamilise sidumise nõuet täpsustavad ka EBA välja töötatud tehnilised regulatiivsed standardid, mis sätestavad, et autentimisprotsessi tulemusena genereeritav autentimiskood peab olema seotud konkreetse maksetehingu andmetega ning selle kasutamine peab olema piiratud üksnes selle konkreetse tehinguga. Standardite kohaselt ei tohi autentimiskoodist olla võimalik tuletada autentimise aluseks olnud turvaelemente ega kasutada varasema autentimise andmeid uue tehingu kinnitamiseks. Lisaks peavad makseteenuse pakkujad tagama, et autentimiskoodide loomine, edastamine ja kasutamine toimuks viisil, mis kaitseb nende konfidentsiaalsust ja terviklikkust ning välistab nende võltsimise või korduvkasutamise.³⁴ Sellised tehnilised nõuded täiendavad artikli 97 lõikes 2 sätestatud dünaamilise sidumise põhimõtet, muutes kliendi kinnituse ühekordseks ja tehinguspetsiifiliseks. Autor järeldab eeltoodust, et nende eesmärk on eelkõige vältida

³³ Riigikogu. (2026). Küberkuritegevuse ohjeldamine finantsvaldkonnas - olulise tähtsusega riikliku küsimuse arutelu 19.02.2026. Istungi ülevaade. - <https://www.riigikogu.ee/istungi-ulevaated/riigikogu-arutas-olulise-riikliku-k-simusena-k-berkuritegevuse-ohjeldamist-finantsvaldkonnas/> (03.04.2026).

³⁴ PSD2 (viide 21), lk-d 6-9.

olukordi, kus autentimiskinnitus võiks olla kasutatav mitme tehingu jaoks või kus kolmas isik saaks autentimisandmeid manipuleerida pärast seda, kui klient on oma kinnituse andnud.

Artikli 97 lõige 3 sätestab, et makseteenuse pakkujatel peavad olema piisavad turvameetmed makseteenuse kasutajate isikustatud turvavolituste konfidentsiaalsuse ja tervikluse kaitseks. Sellest võib järeldada, et autentimise kohustus ei piirdu üksnes autentimishetkega, vaid hõlmab autentimisvahendite kaitset tervikuna. Seega peab makseteenuse pakkuja tagama, et kasutaja isikustatud turvaelemendid - näiteks PIN-koodid või autentimisirakendused - oleksid kaitstud nii tehniliste kui ka organisatsiooniliste meetmetega. Praktikas tähendab see, et makseteenuse pakkuja peab kujundama sellise tehnilise ja organisatsioonilise keskkonna, mis vähendab riski, et isikustatud turvaelemendid satuvad kolmandate isikute valdusesse või neid kasutatakse autoriseerimata viisil. See hõlmab muu hulgas turvalist autentimisprotsessi, andmete krüpteerimist, seansside kaitset ning süsteemset riskide monitoorimist. Välmaksete kontekstis tekib aga täiendav probleem. Välmaksete olemus eeldab tehingu täitmist mõne sekundi jooksul, mis tähendab, et makseteenuse pakkujal on ajaliselt väga piiratud võimalus tehingu sisuliseks täiendavaks kontrolliks enne selle lõplikku teostamist. Kui tehniline ja organisatsiooniline keskkond on üles ehitatud eeskätt kiirusele ja kasutusmugavusele, võib see vähendada pankade sekkumisvõimalust olukorras, kus tehing vastab küll formaalsetele autentimisnõuetele, kuid kannab sotsiaalse manipulatsiooni riski. Siiski ei saa üksnes makse kiirust pidada hoolsuskohustuse rikkumiseks. Küsimus on selles, kas makseteenuse pakkuja on loonud sellise süsteemi, mis suudab ka välmaksete puhul tuvastada selgelt ebatavalisi või kõrge riskiga tehingumustreid ning vajadusel rakendada täiendavaid kontrollimeetmeid. Kui süsteem on üles ehitatud viisil, mis sisuliselt välistab igasuguse riskipõhise sekkumise isegi ilmselgelt kahtlaste tehingute korral, võib tekkida küsimus, kas artikli 97 lõikest 3 tulenev piisavate turvameetmete nõue on tegelikult täidetud. Samas tuleb arvestada, et välmaksete kasutamine ei ole täielikult makseteenuse pakkuja kontrolli all, kuna makseteenuse kasutajal on üldjuhul võimalik vastav funktsionaalsus internetipangas ise välja lülitada või piirata, mistõttu ei saa välmaksete kiirust käsitada üksnes makseteenuse pakkuja hoolsuskohustuse rikkumiseks, vaid tegemist on ka kasutaja enda riskivalikuga. Seega ei seisne probleem välmaksete olemasolus iseenesest, vaid selles, kuidas makseteenuse pakkuja on tasakaalustanud kiiruse, kasutusmugavuse ja turvalisuse nõuded. Just see tasakaal võib osutuda määravaks ka hinnangul, kas pank on täitnud Euroopa Liidu õigusest tuleneva hoolsusnõuet või on jätnud selle ebapiisavaks pettuseriskide kontekstis.

Oluline on ka see, et artikli 97 lõigete 4 ja 5 kohaselt kohaldatakse tugeva kliendi autentimise nõudeid ka juhul, kui makse on algatatud makse algatamise teenuse pakkuja poolt ning kontot

haldav makseteenuse pakkuja peab võimaldama teistel teenusepakkujatel tugineda tema autentimismenetlusele. See laiendab hoolsusmeetmete kohaldamisala olukordadele, kus teingu teostamisse on kaasatud mitu osapoolt.

Tugeva autentimise kohustuse analüüsist võib järeldada, et kliendi autentimise kohustus PSD2 direktiivi kohaselt ei piirdu üksnes makseteenuse kasutaja isikusamasuse tuvastamisega, vaid hõlmab vähemalt kahte olulist hoolsusnõuet. Esiteks kuulub selle alla isikustatud turvavolituste kaitse, mis tuleneb artikli 97 lõikest 3 ning millele viidatakse ka preambula punktis 69. Selle eesmärk on tagada kasutaja autentimisandmete konfidentsiaalsus ja terviklikkus ning ennetada nende väärkasutust kolmandate isikute poolt. Teiseks hõlmab kohustus turvariskide hindamist ja riskijuhtimist, mis põhineb artikli 97 lõigetel 1 ja 2 ning millele viidatakse samuti preambulas punktides 7, 95 ja 96. See nõue eeldab, et makseteenuse pakkuja hindab pettuse ja kuritarvitamise riski ning rakendab tugevat kliendi autentimist vastavalt tuvastatud riskide tasemele. Nii võib PSD2 autentimise hoolsusnõudeid käsitleda laiemas raamistikus, kus SCA moodustab riskipõhise meetme finantsasutuse hoolsusnõuete täitmiseks.

2.1.2. Makseteenuse kasutaja autentimise kohustus kohtupraktikas

Kohtuasjas nr C-287/19 (VKI v DenizBank AG) märkis Euroopa Kohus makseteenuse pakkuja kohustust tagada maksesüsteemi turvalisus ja rakendada asjakohaseid turvameetmeid, et kaitsta kasutajaid ebaõigete või tehniliste probleemide eest.³⁵ Kuigi käesolev kohtuasi käsitles peamiselt NFC-kaardi kasutamist ja lepingutingimuste muutmisega seotud tarbijakaitset, kinnitab see siiski üldist turvameetmete eesmärki, et makseteenuse pakkuja kohustused ei piirdu ainult makse tehnilise täitmisega, vaid hõlmavad ka süsteemide turvalist toimimist ja riski maandamist, mille eest makseteenuse pakkuja vastutab.

Rootsi kõrgem kohus (Högsta domstolen) on 21.06.2022 teinud otsuse nr T 4623-21, milles vastutus pettusejuhtumist oli finantsasutuse ja tema kliendi vahel jagatud. Kuigi nimetatud kohtuasi ei käsitlenud otseselt tugeva kliendi autentimise nõudeid, mis tulenevad PSD2 artiklist 97, on siiski antud kohtuasi magistritöö kontekstis asjakohane. Juhtumi keskseks küsimuseks oli finantsasutuse kliendi (kohtuasjas nimetatud MT) vastutus autoriseerimata maksete eest, mis toimusid pärast seda, kui MT jagas oma turvaseadme koodi petturi poolt loodud eksitava ettekujutuse tulemusena.³⁶

³⁵ EKo C-287/19, DenizBank AG versus Verein für Konsumenteninformation, ECLI:EU:C:2020:897.

³⁶ Högsta domstolen. T 4623-21. 21.06.2022. -

<https://www.domstol.se/globalassets/filer/domstol/hogstadomstolen/avgoranden/engelska-oversattningar/t-4623-21-eng.pdf> (13.03.2026).

Asja lahendamisel hindas kohus MT hoolimatust ja „eriti süülike“ käitumist ning analüüsis, millistel tingimustel võib tarbija olla vastutav kogu autoriseerimata makse summas ning millal tema vastutus on piiratud³⁷. Kuna tehing oli autoriseerimata, lähtus kohus peamiselt makseteenuse pakkuja tsiviilõiguslikust vastutusest ja tarbija võimalikust hooletusest, jättes autentimise kohustuse analüüsi teisejärguliseks. Käesolevas kohtuasjas jõudis kohus järeldusele, et MT vastutab oma hooletu käitumise eest petturiga toimunud teise kõne käigus, kuid kohtu hinnangul ei olnud tegemist „eriti süülike“ tegevusega, sest MT ei andnud koode tahtlikult kolmandale isikule ega tegutsenud teadlikult autoriseerimata tehingu riskiga. Seetõttu oli tarbija vastutus piiratud. Kohus tuvastas, et MT pidas petturit rahulikuks ja professionaalseks pangatöötajaks ning tehingu viis lõpuni üksnes eesmärgil mitte kaotada oma konto kasutamist, kuna loodud asjaolud tekitasid MT-l stressi³⁸. Nagu 1. peatükis kirjeldatud, toimuvad petukõned praktikas sageli mitmes etapis ehk ühe juhtumi puhul võib olla mitu kõnet, mida tuleb analüüsida tervikuna. Antud olukorras märkis kohus, et teise kõne käigus MT käitus hooletult ning toimusid kõik petukõnede skeemile iseloomulikud tunnused (vt 1. peatükk) ehk emotsionaalne manipuleerimine, kiire tegutsemise surve ning kannatanu veenmine, et tegemist on usaldusväärse või hädavajaliku tegevusega. MT kartis kaotada kontrolli oma konto üle, andes petturile turvakooode.³⁹ Selliselt on täidetud kõik pettuse koosseisu elemendid: pettur lõi eksituse, MT tegi varakäsituse, andes petturile oma koode ning selle tulemusena on ta kahju saanud.

Kohtulahendi kohaselt kehtib autoriseerimata tehingute puhul põhireegel, et makseteenuse pakkuja peab taastama konto olukorda, nagu tehingut poleks toimunud. Konto omaniku hooletuse korral ei ületa vastutus tavaliselt 400 Rootsi krooni; äärmise hooletuse korral kogu summa, kuid mitte rohkem kui 12 000 Rootsi krooni; eriti süülike käitumise korral on vastutus piiramatu. Need reeglid põhinevad Rootsis esimesel ja teisel makseteenuste direktiivil (PSD1 ja PSD2). PSD1 sätteid, mis käsitlesid vastutust autoriseerimata tehingute eest, rakendati algselt seadusega „Maksevahenditega tehtud autoriseerimata tehingute kohta“ (2010:738). PSD2 rakendamisega 2018. aastal see seadus tühistati ning autoriseerimata tehingute reeglid viidi üle Makseteenuste seaduse peatükki 5a, mille sätetest kohus oma otsuses lähtus⁴⁰.

Antud juhtumi kontekstis oli MT käitumine hooletu, kuid mitte „eriti süülike“, samal ajal kohtulahendist nähtub, et MT ei kandnud vastutust kõnealuse tehingu eest. Kohus rahuldas

³⁷ Högsta domstolen (viide 36).

³⁸ *Ibid.*

³⁹ *Ibid.*

⁴⁰ *Ibid.*

tema nõue panga vastu, mille kohaselt peab pank hüvitama MT-le 385 000 Rootsi krooni koos intressiga.

Kohus leidis, et tegemist oli autoriseerimata tehinguga, sest klient jagas turvakooode petturi eksituse mõjul. Rootsi seadus (mis põhineb PSD1 ja PSD2 direktiivide alusel) piirab kliendi vastutust, kui ta ei ole tegutsenud eriti süüliselt. Kuna kohus leidis, et klient ei olnud tegutsenud eriti süüliselt, jäi kehtima põhimõte, mille kohaselt pank peab kahju hüvitama. Seetõttu kohus ei analüüsinud detailsemalt, kas pank on täitnud PSD2 direktiivist tulenevad hoolsusnõuded. Sellest nähtub, et tsiviilõiguslik vastutus autoriseerimata tehingu eest ei eelda tingimata makseteenuse pakkuja turvameetmete rikkumise tuvastamist, samas kui karistusõigusliku vastutuse hindamisel võib hoolsusnõuete rikkumise tuvastamine osutuda keskseks küsimuseks. Antud kohtulahendi kontekstis võib tõusetuda küsimus, miks kohus ei analüüsinud üksikasjalikult makseteenuse pakkuja poolt rakendatud turvameetmete piisavust ega hinnanud otseselt, kas pank täitis PSD2 direktiivi artiklist 97 tulenevat tugeva kliendi autentimise kohustust. Nagu autor eelnevalt leidis, tugeva autentimise kohustus hõlmab mitu kohustust, mille hulgas on isikustatud turvavolituste kaitse ning riskipõhiste turvameetmete rakendamine, mille eesmärk on muuhulgas tuvastada ka võimalikke pettusele viitavaid tehingumustreid. Sellest lähtuvalt võiks esmapilgul eeldada, et kohus hindab ka seda, kas makseteenuse pakkuja oleks pidanud tuvastama tehingu pettusele viitavad tunnused ning sekkuma enne tehingu lõplikku täitmist. PSD2 direktiivi artiklid 73 ja 74 kehtestavad autoriseerimata maksetehingute puhul eraldiseisva vastutusskeemi, mille kohaselt peab makseteenuse pakkuja üldjuhul maksjale autoriseerimata tehingu summa viivitamata tagastama. Sellise regulatsiooni eesmärk on jaotada maksesüsteemi riskid ning tagada kasutaja tõhus kaitse. Seetõttu ei ole autoriseerimata tehingu korral makseteenuse pakkuja vastutuse tekkimiseks vajalik eraldi tuvastada, kas pank on rikkunud turvameetmeid või jätnud rakendamata artiklis 97 sätestatud autentimisnõudeid. Kohus keskendub sellisel juhul eeskätt maksja käitumise hindamisele ning sellele, kas kasutaja on rikkunud oma kohustust hoida isikustatud turvaelemente turvaliselt. Samas ei tähenda see autori hinnangul, et makseteenuse pakkuja poolt rakendatavate turvameetmete piisavus oleks õiguslikult ebaoluline. Vastupidi, PSD2 direktiivist tulenevad autentimis- ja riskijuhtimismeetmed kujundavad raamistiku, mille eesmärk on ennetada pettusejuhtumeid enne nende realiseerumist. Kuigi tsiviilõigusliku vastutuse kontekstis ei pruugi nende meetmete rikkumise tuvastamine olla autoriseerimata tehingu puhul alati otsustava tähtsusega, võib selliste hoolsusnõuete täitmata jätmine omandada suurema tähenduse olukordades, kus hinnatakse finantsasutuse laiemat vastutust või analüüsitakse, kas finantsasutus on loonud piisava süsteemi pettuseriskide ennetamiseks. Käesoleva magistritöö kontekstis on see küsimus eriti

oluline, kuna finantsasutuse võimaliku karistusõigusliku vastutuse hindamisel võib keskseks osutada just see, kas makseteenuse pakkuja on täitnud talle Euroopa Liidu õigusest tulenevad hoolsusnõuded, sealhulgas tugeva kliendi autentimise ja riskipõhiste turvameetmete rakendamise kohustuse.

Prantsusmaa Kassatsioonikohtu (La Cour de cassation) praktika rõhutab samuti autoriseeritud ja autoriseerimata maksetehingute eristamise keskset tähtsust. Kohtuasja nr 22-21.200 asjaolude kohaselt esitati pangale mitmeid maksekorraldusi e-posti teel ettevõtte juhi nimel. Hiljem selgus, et ettevõtte juhi e-postikonto oli kolmanda isiku käes ning maksekorraldused ei pärinenud tegelikult ettevõtte esindajalt. Nende korralduste alusel teostas pank mitu rahvusvahelist ülekannet välismaal asuvatele kontodele. Lisaks lõpetati tähtajaline hoius, mille vahendid kanti ettevõtte arvelduskontole ja kasutati samuti ülekande tegemiseks. Ettevõtte vaidlustas tehinguid, väites, et tegemist oli pettusega ning et pank ei oleks pidanud selliseid makseid ilma täiendava kontrollita täitma.⁴¹

Nimetatud kohtuasjas Metzi apellatsioonikohus (Cour d'appel de Metz) leidis, et pangal oli kliendiga sõlmitud lepingulisest suhtest tulenev hoolsuskohustus. Kohus märkis, et pangale esitatud korraldustes esinesid ebatavalised asjaolud, sealhulgas märkimisväärses summas järjestikused ülekanded välisriikidesse ning tähtajalise hoiuse lõpetamine selleks, et rahalised vahendid saaks üle kanda. Apellatsioonikohus järeldas, et sellised asjaolud oleksid pidanud pangas tekitama kahtlusi ning pank oleks pidanud enne maksete täitmist läbi viima täiendavad kontrollid. Kuna pank seda ei teinud, leidis kohus, et pank rikkus oma lepingulist hoolsuskohustust ning vastutab tekkinud kahju eest. Sellest tulenevalt mõistis kohus pangalt ettevõtte kasuks välja kahju hüvitamise.⁴²

Prantsusmaa Kassatsioonikohus hindas aga, et apellatsioonikohus lahendas vaidluse vale õigusliku regulatsiooni alusel. Kassatsioonikohus rõhutas, et olukorras, kus kontoomanik vaidlustab maksetehingud väitega, et ta ei ole neid autoriseerinud, tuleb vaidlust hinnata makseteenuste õiguses sätestatud eriregulatsiooni alusel. Kohus märkis, et selliseid vaidlusi reguleerivad sätted, mis käsitlevad autoriseerimata maksetehinguid ning mis tulenevad makseteenuste regulatsioonist. Seetõttu ei olnud põhjendatud vaidluse lahendamine panga üldise lepingulise hoolsuskohustuse rikkumise kaudu. Sellest tulenevalt leidis kassatsioonikohus, et apellatsioonikohus oleks pidanud esmalt hindama, kas vaidlusalused maksetehingud olid autoriseeritud või autoriseerimata ning kohaldama vastavat makseteenuste regulatsiooni. Kuna apellatsioonikohus seda ei teinud ja lahendas asja üksnes

⁴¹ Cour de cassation (Chambre commerciale). 22-21.200.

<https://www.legifrance.gouv.fr/juri/id/JURITEXT000049385095> (27.03.2024).

⁴² *Ibid.*

panga lepingulise vastutuse raamistikus, tühistas kassatsioonikohus apellatsioonikohtu otsuse ning saatis asja uueks arutamiseks tagasi teisele apellatsioonikohtule.⁴³

Autori hinnangul on käesolevas asjas keskse tähtsusega küsimus, kas vaidlusalused maksetehingud olid autoriseeritud või autoriseerimata vastavalt PSD2 artiklitele 72 ja 73, mis reguleerivad makseteenuse pakkuja vastutust ning tõendamiskoormust autoriseerimata maksetehingute korral. Autoriseerituse hindamisel on oluline välja selgitada, kes tehingud tegelikult algatas. Kui ettevõtte suudab tõendada, et maksekorraldused esitati pettuse tulemusena ning ettevõtte seaduslik esindaja ei andnud tegelikult nõusolekut tehingute teostamiseks, viitab see sellele, et tegemist oli autoriseerimata maksetehingutega. Sellisel juhul kehtib samuti üldpõhimõte, nagu on kirjeldatud eeltoodud Rootsi kohtuasjas ning mis on sätestatud PSD2 direktiivis: makseteenuse pakkuja peab üldjuhul taastama konto olukorra nii, nagu tehingut ei oleks toimunud.

Samas tekitavad antud juhtumi konkreetsed asjaolud küsimuse ka panga turvameetmete piisavuse kohta. Asjaolu, et tegemist oli ettevõtte kontoga ning ülekannete teostamiseks lõpetati isegi tähtajaline hoius, viitab sellele, et tegemist ei olnud tavapäraste maksekorraldustega. Sellises olukorras tekib põhjendatud küsimus, kas pank oleks pidanud rakendama täiendavaid kontrollimehhanisme, et veenduda maksekäsu tegelikus päritolus. PSD2 direktiivi artikli 72 kohaselt ei piisa olukorras, kus makseteenuse kasutaja väidab, et ta ei ole maksetehingut autoriseerinud, üksnes sellest, et makseteenuse pakkuja esitab tehingu dokumentatsiooni. Makseteenuse pakkuja peab suutma tõendada, et tehing oli autenditud, korrektselt dokumenteeritud ning et seda ei mõjutanud tehniline rike või muu puudujääk. Sellest võib järeldada, et pangal on juba enne maksetehingu täitmist kohustus rakendada selliseid kontrolli- ja autentimismehhanisme, mis võimaldavad vältida autoriseerimata maksetehingute teostamist. Lisaks tuleneb PSD2 direktiivi artiklist 97 makseteenuse pakkuja kohustus rakendada tugevat kliendi autentimist ning tagada dünaamiline sidumine, mis seob autentimiskinnituse konkreetse makse summa ja saajaga. Kui makse algatatakse e-posti või muu kaugkanali kaudu, võib tekkida vajadus täiendavate kontrollimeetmete järele, et tagada, et tehingu algatajaks ei ole volitamata kolmas isik. EBA välja töötatud tehniliste regulatiivsete standardite kohaselt peavad makseteenuse pakkujate kontrollimehhanismid olema üles ehitatud viisil, mis võimaldab tuvastada ebatavalisi või riskantseid maksekäsundeid. Näiteks võivad järjestikused suuremahulised ülekanded välismaal asuvatele kontodele või tähtajalise hoiuse likvideerimine tehingute katmiseks kujutada endast riskinäitajaid, mis peaksid pangas tekitama kahtlusi võimaliku pettuse suhtes. Üksnes ettevõtte juhi nimel saadetud e-posti teel

⁴³ Cour de cassation (viide 41).

esitatud korraldustega piirdumine võib viidata turvameetmete ebapiisavusele. Sellistes olukordades võib pangalt oodata täiendavaid ennetavaid meetmeid, näiteks maksekorralduse täiendavat kinnitamist kliendi poolt või muude kontrollimehhanismide rakendamist.

Kuigi makseteenuste regulatsioon näeb ette selliste juhtumite lahendamist tavapäraselt tsiviilõigusliku vastutuse raamistikus, võib autori hinnangul käesoleva juhtumi asjaolude põhjal selline olukord teoreetiliselt avada ka võimaluse hinnata, kas panga turva- ja hoolsusnõuete võimalik eiramine võiks omada tähendust ka karistusõigusliku vastutuse kontekstis. See rõhutab, et makseteenuse pakkuja kohustused ei piirdu üksnes maksete tehnilise täitmisega, vaid hõlmavad ka maksesüsteemi turvalise toimimise tagamist ning klientide kaitset autoriseerimata maksete eest.

Karistusõigusliku vastutuse perspektiivist on keskne küsimus, kas ja millal võib PSD2 direktiivi artiklis 97 sätestatud kohustuste rikkumine kujutada endast sellist normatiivset kõrvalekallet, mis on piisavalt oluline, et kõne alla tuleks juriidilise isiku karistusõiguslik vastutus. Kui makseteenuse pakkuja ei rakenda tugevat kliendi autentimist olukorras, kus see on artikli 97 lõike 1 kohaselt kohustuslik, või kui kasutatav autentimislahendus ei vasta dunaamilise sidumise nõudele, on tegemist õigusnormi rikkumisega. Samas ei tähenda iga tehniline või organisatsiooniline puudus automaatselt karistusõiguslikku vastutust. Karistusõigusliku vastutuse tekkimiseks tuleb täiendavalt hinnata, kas rikkumine oli piisavalt oluline ning kas see oli põhjuslikus seoses tekkinud kahju või ohu realiseerumisega.

2.1.3. Operatsiooniriski juhtimine ja turvameetmete kohustus normatiivses raamistikus

Lisaks autentimisprotsessile hõlmab PSD2 direktiivi artikli 97 lõige 3 makseteenuse pakkuja kohustust rakendada piisavaid turvameetmeid isikustatud turvavolituste kaitseks. Selle nõude praktiline täitmine eeldab ka finantsasutuse sisemiste riskijuhtimismehhanismide toimimist, sealhulgas operatsiooniriski juhtimist. PSD2 direktiivi artikli 95 lg 1 sätestab, et liikmesriigid tagavad makseteenuse pakkujatele kohustuse kehtestada asjakohased leevendusmeetmed ja kontrollimehhanismid, et juhtida operatsiooni- ja turvariske, mis on seotud pakutavate makseteenustega. See hõlmab ka intsidentide juhtimise menetlusi ja suurte operatsiooni- ja turvaintsidentide avastamist ning liigitamist, samuti regulaarset hindamist nende leevendusmeetmete ja kontrollimehhanismide piisavuse kohta (art 95 lg 2). Seega on operatsiooniriski juhtimine otseselt seotud artikli 97 lõike 3 kohustusega rakendada piisavaid turvameetmeid isikustatud turvavolituste kaitseks. Operatsiooniriski juhtimise eesmärk on tagada, et turvameetmed toimivad süsteemselt ja efektiivselt, tuvastades ebatavalised või

riskantsed tehingud ning võimaldades pangal rakendada täiendavaid kontrollimehhanisme enne tehingu täitmist. See normatiivne raamistik määratleb, millised turvameetmed ja kontrollimehhanismid on makseteenuse pakkujal kohustuslikud ning loob aluse, mille alusel hinnata finantsasutuse hoolsusnõuete täitmist praktilistes olukordades, sealhulgas võimalike pettuste ennetamisel.

2.1.4. Operatsiooniriski juhtimine ja turvameetmete kohustus kohtupraktikas

Prantsusmaa juhtum illustreerib operatsiooniriski juhtimise ja turvameetmete kohustuse vajadust praktiliselt: asjaolud näitavad, et pank piirdus maksekorralduse täitmisel ainult e-posti kontrolliga ning ei rakendanud täiendavaid turvameetmeid ega autentimist, et veenduda tehingu algataja õigsuses. Selline olukord näitab, kuidas operatsiooniriski juhtimise ja turvameetmete ebaefektiivne rakendamine võib viia autoriseerimata maksete teostumiseni, rõhutades vajadust süsteemsete ja tõhusate kontrollimehhanismide järele, nagu artiklis 95 ette nähtud.

Lisaks on see juhtum oluline ka võimaliku karistusõigusliku vastutuse hindamise kontekstis. Kui pank ei täida artiklitest 97 (lg 3) ja 95 tulenevaid kohustusi piisava turvameetmete rakendamise ja autentimise osas, võib tegemist olla õigusnormi rikkumisega, millel on eeskätt tsiviilõiguslikud tagajärjed. Sellise rikkumise võimalikku karistusõiguslikku tähendust saab hinnata üksnes juhul, kui tegu vastab konkreetse süüteokoosseisu tunnustele. Käesoleva magistritöö fookuses oleva KarS § 217² kontekstis tuleb arvestada, et nimetatud koosseisu üheks keskseks elemendiks on tahtlus. Analüüsitava juhtumise ei ilmne selgelt tahtluse olemasolu panga tegevuses, mistõttu ei saa teha lõplikku järeldust selle koosseisu kohaldatavuse kohta. Seetõttu võib käsitletud olukord olla asjakohane pigem selliste normide analüüsimisel, mis hõlmavad hoolsuskohustuse rikkumist ilma tahtluse nõudeta, näiteks väärteokoosseisu raames MERAS § 113 alusel. Autori hinnangul just nimetatud alus võimaldaks hinnata, kas puudulikud turvameetmed ja operatsiooniriski juhtimine võivad kaasa tuua mitte ainult tsiviilõigusliku, vaid teatud tingimustel ka väärteo- või potentsiaalselt karistusõigusliku vastutuse küsimuse ja käsitletud Prantsusmaa kohtulahend kujutab endast seejuures head näidet.

Praktikas on kohtud pidanud lahendama olukordi, kus maksetehing on formaalselt autoriseeritud, kuid selle tegemine on toimunud pettuse mõjul. Sellise olukorra näitena võib

tuua Rootsi esimese astme kohtu (Stockholms tingsrätt) lahendi nr T 18737-23, milles hinnati panga vastutust Swish-maksetega seotud pettusejuhtumis⁴⁴.

Juhtumi asjaolude kohaselt sattus tarbija 2023. aasta alguses pettuse ohvriks petukõne skeemi järgi. Tarbijaga võtsid telefoni teel ühendust petturid, kes väitsid, et tema identiteeti on kuritarvitatud ning et tema pangakontolt on juba üle kantud või on kohe üle kandmisel 100 000 Rootsi krooni. Petturid selgitasid, et väidetava ülekande peatamiseks peab tarbija tegema nn „tühistamistehingu“ Swishi kaudu. Petturite juhiste järgi kandis tarbija esmalt raha oma säästukontolt isiklikule kontole, seejärel tõstis Swishi makselimiidi 5 000 kroonilt 100 000 kroonini ning lõpuks kandis 100 000 krooni Swishi kaudu petturite poolt etteantud telefoninumbrile. Tegelikult kuulus see konto tarbijale tundmatule isikule, kes tegutses petturite nimel. Tarbija tegutses petturite loodud eksimuse mõjul, uskudes, et tema tegevus aitab vältida raha kaotamist.

Pärast tehingut esitas tarbija panga vastu hagi, väites esiteks, et tegemist oli autoriseerimata maksetehinguga ning pank oleks pidanud raha kontole tagasi kandma. Teiseks väitis tarbija, et pank tegutses hooletult, kuna lubas Swishi makselimiiti märkimisväärselt suurendada ega rakendanud täiendavaid turvameetmeid võimaliku pettuse tuvastamiseks.

Kohus analüüsis esmalt maksetehingu olemust, et selgitada välja, kas tegemist oli autoriseeritud või autoriseerimata tehinguga. Kohtu hinnangul oli tehing autoriseeritud, kuna makse tehti tarbija enda poolt ja tema nõusolekul, kuna tarbija kinnitas makse ise Swishi rakenduses oma autentimisvahendiga (BankID)⁴⁵. BankID on Rootsi e-identifitseerimise lahendus, mille kasutatakse digitaalseks isikusamasuse tuvastamiseks ja elektrooniliseks allkirjastamiseks⁴⁶. BankID abil antud elektrooniline allkiri vastab Rootsi e-identiteedi kvaliteedimärgi kohaselt usaldustasemele 3, mis tähendab kõrget turvalisuse ja usaldusväärsuse taset elektroonilise identifitseerimise protsessis. Samuti kvalifitseerub BankID abil antud allkiri Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (eIDAS-määrus) kohaselt täiustatud elektrooniliseks allkirjaks. Lisaks vastab BankID kasutamine PSD2 direktiivis sätestatud tugeva kliendi autentimise nõuetele ja täidab BankID-l põhinev autentimine ka dünaamilise sidumise nõudeid, mille eesmärk on tagada maksetehingute turvalisus ning siduda autentimisprotsess konkreetse maksetehingu

⁴⁴ Stockholms tingsrätt. T 18737-23. 11.11.2024. Lahendi täistekst on autori valduses; lühikokkuvõte on kättesaadav veebilehel:

<https://www.domstol.se/nyheter/2024/11/dom-i-mal-om-en-banks-skyldigheter-vid-swishbedragerier/>.

⁴⁵ *Ibid.*

⁴⁶ TIC. Secure Digital Identification - BankID. - <https://tic.io/en/produkter-tjanster/bank-id> (20.03.2026).

andmetega.⁴⁷ Kohtu hinnangul asjaolu, et tarbija tegutses petturite mõjutusel, ei muutnud tehingut makseteenuste regulatsiooni mõttes autoriseerimata tehinguks. Seejärel hindas kohus panga võimalikku hoolsus- ja turvakohustuse rikkumist. Analüüsi käigus uuriti, kas pank oleks pidanud rakendama täiendavaid turvameetmeid, näiteks nõudma Swishi limiidi tõstmisel isiklikku kontakti kliendiga, kasutama reaajas tehingute jälgimise süsteeme kahtlaste maksete tuvastamiseks või rakendama täiendavat riskianalüüsi pettuse vältimiseks. Kohus lähtus analüüsis eelkõige PSD2 direktiivist, Rootsi makseteenuste seadusest, EBA turvariskide juhenditest (EBA Guidelines 2017/17) ning Rootsi finantsjärelevalve regulatsioonidest makseteenuse pakkujatele. Samuti võeti arvesse rahapesu ja terrorismi rahastamise tõkestamise regulatsiooni. Kohtu hinnangul ei tulenenud ühestki nimetatud regulatsioonist kohustust rakendada Swishi limiidi tõstmisel isiklikku kontaktikontrolli ega tehingute reaajas jälgimist olukorras, kus makse oli kliendi poolt autoriseeritud, st tehti see tarbija enda nõusolekul. Samuti ei tuvastanud kohus panga hoolsuskohustuse rikkumist, kuna kehtiv regulatsioon ega pangandustava ei nõudnud täiendavate turva- või kontrollimeetmete rakendamist sellises olukorras. Sellest tulenevalt jäeti tarbija kahju hüvitamise nõue panga vastu rahuldamata.⁴⁸

Eeltoodud kohtulahend illustreerib hästi praktilist probleemi, mis tekib tugeva kliendi autentimise nõuete rakendamisel makseteenuste kontekstis. Kohtuasjast nähtub, et isegi juhul, kui klient tegutseb petturite mõjutusel ja kannab raha kolmandale isikule, loetakse tehing autoriseerituks, kui makse algatatakse ja kinnitatakse kliendi enda autentimisvahendi kaudu. Selline lähenemine toob esile olulise regulatiivse probleemi: tugev kliendi autentimine tagab küll tehingu tehnilise turvalisuse ja kasutaja identiteedi kontrolli, kuid ei pruugi takistada pettusi olukordades, kus klient ise pettuse mõjul makse algatab. Seega võib tekkida olukord, kus tehing on formaalselt autoriseeritud, kuid sisuliselt on tegemist pettusega. Sellest järeldub, et makseteenuse pakkuja ei riku sellises olukorras oma hoolsuskohustust, kui ta on täitnud PSD2 direktiivist tulenevat autentimise kohustust ning kliendi eksimusest tingitud kahju ei ole üldjuhul üle kantav makseteenuse pakkuja vastutuseks. Samas ei välista eeltoodu täielikult küsimust, kas teatud erandlikes olukordades, kus tehingu asjaolud viitavad selgelt ebatavalisele või kõrge riskiga käitumisele, võiks makseteenuse pakkujalt oodata täiendavate riskipõhiste kontrollimeetmete rakendamist pettuse tuvastamiseks või selle riski vähendamiseks.

⁴⁷ Finansiell ID-Teknik BID AB. Sustainability Report 2022. -

https://www.bankid.com/assets/files/Sustainability_report_BankID_2022.pdf (20.03.2026).

⁴⁸ Stockholms tingsrätt. T 18737-23. 11.11.2024. Lahendi täistekst on autori valduses; lühikokkuvõte on kättesaadav veebilehel:

<https://www.domstol.se/nyheter/2024/11/dom-i-mal-om-en-banks-skyldigheter-vid-swishbedragerier/>.

Magistritöö kontekstis näitab käsitletud kohtulahend, et PSD2 artikli 97 lõikes 3 sätestatud turvanõuete täitmine ei pruugi olla piisav pettuste ennetamiseks, kui makseteenuse pakkuja ei rakenda täiendavaid riskipõhiseid kontrollimeetmeid. Rootsi esimese astme kohtu hinnangul puudusid aga kehtivad regulatsioonid ega valdkonna tavapraktika, mis kohustaksid pank viima läbi täiendavaid kontrollimehhanisme, näiteks isiklikku kontaktivestlust kliendiga enne Swish-limiidi olulist tõstmist (nt 5 000 kroonilt 100 000 kroonini), tehingute reaajas jälgimist või süsteemseid mehhanisme pettusekatsete tuvastamiseks. Samas, PSD2 jõustus 13.jaanuaril 2018.aastal, aga tarbija kõnealuse kohtulahendi kohaselt sattus pettuse ohvriks 2023.aasta jaanuaris, ehk PSD2 direktiivi kehtivuse ajal. Autori hinnangul tehingu suurus või ebatavalisus on asjaolude kohaselt viidanud suuremale riskile, mida tuleks pangal enne tehingu teostamist täpsustada. Piiratud turvameetmete rakendamine tähendab operatsiooniriski süsteemse hindamise puudumist ning vähendab võimalust tuvastada tehinguid, mis viitavad pettusele, kuigi operatsiooni- ja turvariskide juhtimine on PSD2 direktiivist otsene kohustus. Selline puudulik turvameetmete piisavuse hindamine on oluline ka karistusõigusliku vastutuse kontekstis, kuna võib anda aluse küsimusele, kas pank teadlikult jättis täiendavad hoolsusmeetmed rakendamata, mis tekitas kliendile kahju. Seega illustreerib juhtum, et autoriseeritud tehing ei välista pettuse riski ja tõhusa hoolsus- ning kontrollimehhanismide rakendamise olulisust, et kaitsta kliente ning vähendada pankade võimalikku tsiviil- ja karistusõiguslikku vastutust.

2.2. Finantsasutuste hoolsusnõuete regulatsioon Eesti õiguses

PSD2 direktiiv on Eestis peamiselt üle võetud Makseasutuste ja e-raha asutuste seadusega (edaspidi MERAS). PSD2 direktiivi ülevõtmisega muudeti ka Võlaõigusseaduse (edaspidi VÕS) sätteid, mis käsitlevad makseteenuse lepingut. VÕS sätestab makseteenuse pakkuja ja kliendi õigused ja kohustused seoses maksetehingute algatamise, täitmise ja autoriseerimata tehingutega. Selle kaudu määratletakse ka vastutus ebaõigete või autoriseerimata maksete täitmise eest ning kohustused kahju hüvitamiseks. VÕS täpsustab nii lepingulise kohustuse rikkumise tagajärgi kui ka ajutisi meetmeid, näiteks tehingu tühistamise või tagasikutsumise võimaluse.

Pettusejuhtumi analüüsimisel ja maksetehingute teostamisel peab makseteenuse pakkuja järgima hoolsusnõudeid, mis tulenevad peamiselt VÕS-ist, MERAS-est ning Rahapesu ja terrorismi rahastamise tõkestamise seadusest (edaspidi RahaPTS). Eesti õiguses sätestatud hoolsusmeetmed eelnimetatud õigusaktides peegeldavad PSD2 direktiivis kehtestatud kohustusi, sealhulgas kasutaja autentimise, isikustatud turvavolituste kaitset, turvariskide

hindamist ja riskijuhtimist ja piisavate turvameetmete rakendamist. Eesti regulatsioon ühendab direktiivi põhimõtted riikliku õiguse spetsiifikaga ning võimaldab selgelt määratleda makseteenuse pakkuja ja kliendi kohustused. RahaPTS sätestab kohustatud isikute, kohustused kliendi isikusamasuse tuvastamisel, tehingute jälgimisel, riskide hindamisel ning täiendavate kontrollimeetmete rakendamisel (§-d 31-38)⁴⁹. RahaPTS-i kohaldatakse RahaPTS § 2 lg 1 p 2 kohaselt finantseerimisasutuste majandus-, kutse- ja ametitegevuses. RahaPTS § 6 lg 2 p 2 kohaselt finantseerimisasutusena käsitletakse RahaPTS tähenduses muuhulgas makseteenuse pakkujat MERAS tähenduses. Samuti on makseasutus finantseerimisasutus krediitiasutuste seaduse tähenduses MERAS § 5 lg 1 kohaselt.⁵⁰

Makseteenuse pakkuja on RahaPTS § 19 lg 1 alusel kohustatud kohaldama hoolsusmeetmeid äri- ja tehingusuhete loomisel, rahapesu või terrorismi rahastamise kahtluse tekkimisel ning olukordades, kus hoolsusmeetmete käigus kogutud andmete piisavus on kahtluse all. Juhuti tehtavate rahaülekannete puhul tuleb RahaPTS § 25 lg 1¹ kohaselt isikusamasus tuvastada, kui tehingu väärtus ületab 1000 eurot. RahaPTS § 20 kohaselt hoolsusmeetmed peavad hõlmama kliendi ja tegeliku kasusaaja tuvastamist ning andmete kontrolli usaldusväärsest allikast, samuti ärisuhte eesmärgi ja olemuse hindamist. Need sätted tagavad, et isikusamasuse tuvastamine ei piirdu vaid formaalse kontrolliga, vaid hõlmab ka kliendi ärisuhete ja riskiprofiili põhjalikku mõistmist. Praktikast tähendab see, et makseteenuse pakkuja saab hinnata iga tehingu konteksti ning võrrelda seda kliendi varasemate tehingute mustritega. Teatud tehingud võivad olla kooskõlas kliendi tavapärase tegevustega ning neid on lihtsam riskivabalt täita. Samas võivad tehingud, mis erinevad oluliselt kliendi tavapärasest mustrist, näiteks ebatavaliselt suured summad, rahvusvahelised ülekanded uutele saajatele või keerukad makseinstrumendid, viidata kahtlasele tegevusele ja vajada täiendavat kontrolli.

RahaPTS eristab kolme peamist hoolsusmeetmete taset: tavalised, lihtsustatud ja tugevdatud hoolsusmeetmed. Eelnimetatud hoolsusmeetmed on suunatud eelkõige ärisuhte loomiseks, jätkamiseks ja lõpetamiseks ning mille peamine eesmärk on vältida rahapesu ja terrorismi rahastamist. Käesoleva magistritöö kontekstis ei ole seaduse esmaseks eesmärgiks rahapesu ja terrorismi rahastamise regulatsiooni analüüs, kuid seadus sisaldab ka makseteenuse pakkujatele olulisi kohustusi, mis on otseselt seotud tehingute turvalisuse ja pettuste ennetamisega.

RahaPTS § 23 lõige 1 sätestab, et makseteenuse pakkujatel on kohustus pidevalt jälgida kliendi ja ärisuhtega seotud tehinguid, et tagada nende kooskõla kliendi riskiprofiili ja

⁴⁹ Rahapesu ja terrorismi rahastamise tõkestamise seadus. - RT I, 14.03.2025, 23.

⁵⁰ Makseasutuste ja e-raha asutuste seadus. - RT I, 13.02.2026, 9.

varasemate tehingute mustritega. RahaPTS § 23 lõige 2 punkt 1 sätestab, et tehingute seire peab hõlmama hindamist, kas tehingud vastavad pakkuja teadmiste kliendist ja tema riskiprofiilist. Erilist tähelepanu tuleb makseteenuse pakkujal pöörata keerukatele või ebatavaliselt suurtele tehingutele ning tehingumustritele, millel puudub nähtav majanduslik eesmärk (RahaPTS § 23 lõige 2 punkt 4).

Ärisuhte pidev seire tähendab, et makseteenuse pakkuja jälgib kogu kliendi ärisuhet, sealhulgas sissetulevaid tehinguid, hinnates muutusi kliendi tegevuses ja riskiprofiilis. Selline seire võimaldab tuvastada kahtlaseid tegevusi, rahapesu või terrorismi rahastamisega seotud riske. Praktikas rakendatakse skriinimist ehk tehingute reaalajas jälgimist ja monitoorimist ehk hilisemat analüüsi, kasutades vajadusel automaatseid IT-süsteeme või manuaalseid protseduure.⁵¹ Selle põhjal võib kindlalt järeldada, et skriinimise ja monitoorimise kombinatsioon võimaldab nii varajast sekkumist kui ka põhjalikumat hilisemat analüüsi. Autori hinnangul on tähelepanuväärne, et tegemist on rahapesu ja terrorismi rahastamise tõkestamisega seotud kohustusega, mille rakendamine on oluline ka pettuste kontekstis ning mille seos makseteenuse pakkuja regulatsiooni laiemate kohustustega võib olla analüüsimiseks huvipakkuv. Kõrge riski korral kohaldatakse tugevdatud hoolsusmeetmeid, sh tehingu eesmärgi ja vahendite allika täiendavat kontrolli ning dokumenteeritakse tuvastatud kahtlased toimingud⁵². See näitab, kuidas regulatiivsed nõuded realiseeruvad praktilises tegevuses. Antud protsess võimaldab makseteenuse pakkujal tuvastada ja hinnata kõrgema riskiga tehinguid, sealhulgas potentsiaalset rahapesu või terrorismi rahastamist. Samuti tagab dokumenteerimine, et tehingute analüüs ja otsused on jälgitavad, mis on oluline nii juriidilisest kui ka teaduslikust vaatenurgast. Magistritöö seisukohalt illustreerib see punkt riskipõhise lähenemise rakendamist, näidates, kuidas tehingute seire ja hoolsusmeetmete kohaldamine aitab tagada kliendi tegevuse kooskõla teadaoleva riskiprofiiliga ning võimaldab makseteenuse pakkujal tuvastada ebatavalisi või riskantseid tehinguid, mis võivad viidata pettusele. Praktikas tähendab see, et tehingud, mis ei ole kooskõlas kliendi varasemate tavapärase makseharjumuste ja ärisuhete mustritega, saavad automaatselt täiendava kontrolli. PSD2 artikli 97 lõige 3 kohaselt peab makseteenuse pakkuja rakendama piisavaid turvameetmeid, et kaitsta makseteenuse kasutaja isikustatud turvavolituste konfidentsiaalsust ja terviklikkust. See nõue on otseselt seotud tehingute pideva seire ja riskiprofiili hindamisega, nagu nõuab RahaPTS § 23. Kliendi tehingute jälgimine ja analüüsimine võimaldab rakendada RahaPTS-i riskipõhiseid meetmeid. Samal ajal aitab see tagada, et

⁵¹ Finantsinspektsioon. Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks. 26.11.2018. - https://www.fi.ee/sites/default/files/2018-11/FI_AML_Soovituslik_juhend.pdf, lk 50. (14.03.2026).

⁵² *Ibid.*

autentimisprotsessid ja turvameetmed vastavad PSD2 standarditele, toetades PSD2 direktiivis sätestatud kohustuslikku autentimise kohustust ning vähendades pettuse, volituste väärkasutuse ja teiste turvariskide tekkimise võimalust.

Kokkuvõttes võib järeldada, et on hoolsusmeetmete kohaldamine nii RahaPTS-i kui PSD2 nõuete valguses ühtse eesmärgiga: tagada makseteenuse kasutaja andmete turvalisus ja ennetada väärkasutust. Magistritöö kontekstis on oluline siiski hoolsusnõuete regulatsioone eristada: RahaPTS-is sätestatud nõuded on suunatud peamiselt rahapesu ja terrorismi rahastamise tõkestamisele ning nimetatud seadus ei pruugi olla vahetult asjakohane pettusejuhtumite lahendamisel, mistõttu moodustavad need omaette regulatiivse raamistikku. Autor keskendub PSD2 raamistikule, analüüsides makseteenuse pakkuja kohustusi pettuste ja volituste väärkasutuse ennetamisel ning järgmises alapeatükis käsitleb kohustusliku autentimise nõuet, mis on pettuse kontekstis võtmetähtsusega vastutuse määramisel.

2.2.1. Makseteenuse kasutaja autentimise kohustus Eesti õiguses

Autentimise kohustus tuleneb Eesti õiguses VÕS-ist. VÕS-i § 709 eristab autentimist ja kliendi tugevat autentimist.⁵³ Autentimine on automaatne toiming, mis võimaldab makseteenuse pakkujal tuvastada kliendi isikusamasuse või konkreetse makseinstrumendi kasutamise õiguse kehtivuse, sealhulgas isikustatud turvaelementide kasutamise (VÕS § 709 lg 12¹). Kliendi tugev autentimine on autentimine, mis põhineb vähemalt kahe teineteisest sõltumatult toimiva ja autentimisandmete konfidentsiaalsust tagava turvaelemendi kasutamisel, mida teab või omab üksnes klient või mida saab omistada üksnes talle (VÕS § 709 lg 12²). Isikustatud turvaelement on VÕS § 709 lg 12³ isikuga seostatud autentimist võimaldav komponent. Autentimise korral kasutatav üks turvaelement tähendab, et kliendi isikusamasuse või makseinstrumendi kasutamise õiguse kontrollimiseks kasutatakse ainult ühte autentimisfaktorit. Turvaelemendid ehk turvavolitused jagunevad kolme kategooriasse: teadmise element - midagi, mida teab üksnes klient (nt parool, PIN-kood); valduse element - midagi, mida omab üksnes klient (nt pangakaart, mobiiltelefon, autentimiskendur); isikuomaduse element - midagi, mis on kliendile omane (nt sõrmejalg, näotuvastus)⁵⁴. Tavalise autentimise puhul kasutatakse neist ainult ühte elementi, mistõttu põhineb kliendi tuvastamine või makseinstrumendi kasutamise õiguse kontroll ainult ühel kontrollimehhanismil. Näiteks võib teadmise elemendil põhinev autentimine seisneda selles, et klient sisestab internetipanka sisenemiseks kasutajanime ja parooli või muu üksnes talle

⁵³ Võlaõigusseadus. - RT I, 11.11.2025, 16.

⁵⁴ Tugev kliendituvastus (SCA) ja kuidas see mõjutab veebimakseid. - EveryPay tugikeskus, s.a. - <https://support.every-pay.com/et/articles/11478038-tugev-kliendituvastus-sca> (03.03.2026).

teada oleva koodi. Valduse elemendi kasutamise näiteks võib olla olukord, kus klient teeb internetipoes makse üksnes pangakaardi andmete - näiteks kaardinumbri, kehtivusaja ja turvakoodi - sisestamisega. Isikuomaduse elemendi kasutamine esineb praktikas eelkõige nutiseadmete puhul, kus kliendi isikusamasuse tuvastamiseks kasutatakse biomeetrilisi tunnuseid, näiteks sõrmejälge või näotuvastust mobiilipanga rakendusse sisenemisel või tehingu kinnitamisel. Sellisel juhul ei toimu täiendavat kontrolli teise sõltumatu turvaelemendi kaudu ning autentimine ei vasta kliendi tugeva autentimise nõuetele. Seetõttu on ühe turvaelemendi kasutamine üldjuhul vähem turvaline, kuna turvaelemendi sattumisel kolmanda isiku valdusse võib tekkida võimalus tehingu tegemiseks ilma kliendi tegeliku nõusolekuta. Seetõttu kehtestati nõue, et elektrooniliste maksete puhul tuleb üldjuhul kasutada kliendi tugevat autentimist, mitte ainult tavalist autentimist. See tähendab, et tehingu autoriseerimiseks peab makseteenuse pakkuja kasutama vähemalt kahte sõltumatut turvaelementi ning kaugteel tehtud maksete puhul peab autentimine olema seotud konkreetse tehingu summa ja saajaga (dünaamiline seos).

Kliendi tugeva autentimise kohustus tuleneb võlaõigusseaduse § 724⁶ lõikest 3, mille kohaselt peab makseteenuse pakkuja nõudma kliendi tugevat autentimist iga kord, kui maksja soovib juurdepääsu maksekontole interneti teel, algatada elektroonilist maksetehingut või teha muud toimingut, millega kaasneb makseteenusega seotud andmete väärkasutamise või pettuse oht. Interneti kaudu algatatud elektrooniliste maksete puhul peab autentimine lisaks võimaldama maksetehingu dünaamilist sidumist konkreetse maksesumma ja saajaga (VÕS § 724⁶ lg 4). Võlaõigusseaduse § 724⁶ lõiked 3 ja 4 võtavad sisuliselt üle makseteenuste direktiivi (PSD2) artikli 97 lõigetes 1 ja 2 sätestatud tugeva kliendi autentimise nõuded. Samas kajastub direktiivi artikli 97 lõikes 3 sätestatud kohustus tagada makseteenuse kasutajate isikustatud turvavolituste konfidentsiaalsus ja terviklus VÕS § 724⁶ lg-s 1 sätestatud üldises turvanõudes.

Nimetatud sätted näitavad, et PSD2 direktiivist tulenevad nõuded on Eesti õigusesse üle võetud ning rakendatud võlaõigusseaduse kaudu. VÕS § 724⁶ väljendab selgelt seadusandja eesmärki kehtestada makseteenuse pakkujatele kohustus rakendada piisavaid turvameetmeid, sealhulgas kliendi tugevat autentimist kui ühte olulisemaid makseturbe mehhanisme, mis aitavad võimalikult suurel määral ennetada makseteenuste väärkasutamist ja pettusi.

2.2.2. Operatsiooniriski juhtimine ja turvameetmete kohustus Eesti õiguses

PSD2 artikli 97 lõige 3 ei ole VÕS-is üks-ühele üle võetud, vaid kajastub VÕS § 724⁶ lõikes 1 üldises turvanõudes, mille kohaselt peavad makseteenuse pakkujad kasutama turvalist teabevahetust ning rakendama turvameetmeid, mis tagavad isikustatud turvaelementide

konfidentsiaalsuse ja andmete tervikluse, selle turvanõude praktilist täitmist täpsustab MERAS § 63⁵, mis käsitleb operatsiooniriski juhtimist, kohustades makseteenuse pakkujat rakendama turvameetmeid ja kontrollimehhanisme operatsiooniriski ja turvariskide haldamiseks ning esitama igal aastal Finantsinspeksioonile (edaspidi FI) hinnangu rakendatavate meetmete piisavuse kohta. Antud paragrahv loob otsese seose PSD2 eesmärgi ja artiklis 95 sätestatud hoolsusnõuetega, mille järgi finantsasutusel on kohustus ennetada riske juba enne, kui need realiseeruvad ning tagada, et makseteenuste osutamine oleks turvaline ja kontrollitud. Operatsioonirisk - risk saada kahju sisemiste protsesside, inimeste tegevuse või süsteemide ebaadekvaatsusest või mittetoimimisest oodatud viisil või välistest sündmustest⁵⁵. Operatsiooniriski juhtimine on oluline hoolsusnõue, kuna see kujutab endast kontrollimehhanismi, mille raames süsteemsete jälgimis- ja hoiatusmechhanismide abil tuvastatakse kahtlaseid maksetehinguid ning töötajate volituste kontroll aitab vältida ekslikke või petturlikke tehinguid. Selline ennetav riskijuhtimine vastab MERAS § 63⁵ nõuetele ning PSD2 direktiivi artikli 95 eesmärgile tagada maksete turvalisus ja finantsasutuste kohustus hoolsalt tegutseda klientide vara kaitsmisel.

Eestis on makseteenuste pakkujate järelevalveasutuseks FI, kellel on Finantsinspeksiooni seaduse (edaspidi FIS) § 57 lg 1 kohaselt õigus välja anda soovitusliku iseloomuga juhendeid finantssektori tegevust reguleerivate õigusaktide selgitamiseks või finantsjärelevalve subjektide suunamiseks. Kuigi FI juhendid on soovitusliku iseloomuga, moodustavad need siiski lahutamatu osa finantsasutuste siseriiklike regulatsioonidest. FI juhend operatsiooniriski juhtimise kohta täpsustab MERAS § 63⁵ sätteid, rõhutades, et operatsiooniriski juhtimine peab olema osa organisatsiooni üldisest juhtimis- ja riskijuhtimissüsteemist ning toetuma tõhusale sisekontrollile, riskikultuurile ja juhtimisprotsessidele. Juhendi eesmärk on tagada, et finantsasutus tuvastab ja hindab operatsiooniriske, rakendab nende ennetamiseks kontrollimehhanisme ning loob süsteemi, mis võimaldab reageerida ka viivitusega või kaudselt tekkivatele kahjudele. Lisaks operatsiooniriski ennetamisele sätestab MERAS § 63⁶ makseteenuse pakkujatele kohustuse teavitada FI-s viivitamata olulistest operatsiooni- või turvaintsidentidest, sh küberohust, mis võivad mõjutada makseteenuseid või klientide finantshuve. Teavitamine hõlmab ka intsidendi üksikasju ning rakendatud või kavandatud abinõusid, võimaldades järelevalvel hinnata riskide ulatust ja tõhusust. Kui intsidendil on mõju klientidele, peab finantsasutus teavitama ka kliente ning esitama regulaarselt statistilisi andmeid pettuste kohta. See teavitamiskohustus on operatsiooniriski juhtimise loomulik jätk ning toimib praktilise kontrollimehhanismina. Koos § 63⁵ sätestatud riskijuhtimisega tagab §

⁵⁵ Finantsinspeksioon. Nõuded operatsiooniriski juhtimise korraldamiseks. 18.05.2005. - https://www.fi.ee/failid/20050518_juh_Nouded_OR_juhtimise_korraldamiseks.pdf (16.03.2026).

63⁶, et organisatsioon suudab tuvastada, hinnata ja lahendada ka juba realiseerunud või tekkida võivaid ohte. FI juhendi ja § 63⁶ nõuete rakendamine loob finantsasutuses süsteemi, kus operatsiooniriske käsitletakse ühtse protsessina: kontrollmehhanismide rakendamine, riskide ennetamine ning intsidendi korral adekvaatne ja dokumenteeritud reageerimine. Seega moodustavad MERAS §-d 63⁵ ja 63⁶ koos FI juhendiga hoolsusnõuete õigusraamistikku, mis võimaldab finantsasutusel täita PSD2 direktiivi artikli 95 eesmärki - tagada maksete turvalisus, ennetada pettusi ja kaitsta klientide vara, muutes kogu makseteenuse osutamise protsessi läbipaistvaks, kontrollitavaks ja vastavaks nii siseriiklikele kui ka EL õigusaktidele.

Lisaks tuleb arvestada, et digitaalallkirja ehk eID kasutamise ehtsuse tõendamise koormus ei lange eID omaniku täielikult kanda, vaid krediidiandjal on selleks piisavad ressursid ja tehnilised võimalused, mis võimaldavad tagada tehingute autentimise ja eID omaniku kaitse pettuste eest. Krediidiandjal on võimalik kasutada näiteks IP-aadressi jälgimist, täiendavaid autentimis- ja teavitamismeetmeid (SMS, e-kirjad, telefoni teavitused) ning üldist oskusteavet, et kontrollida tehingu tegelikku algatajat.⁵⁶ Magistritöö kontekstis näitab see, et tõendamiskoormust krediidiandja ja eID omaniku vahel tuleb õiglaselt jaotada. Eeltoodud seisukoht tugevdab VÕS § 724¹ ja § 709 kohaldamist, mis määratlevad makseteenuste autoriseerimise ja kliendi autentimise alused. Autentimise ja tõendamiskoormuse kooskõlastamine võimaldab tagada, et autoriseerimata tehingu korral ei peaks eID omanik kandma kogu tõendamiskoormust, vaid krediidiandja saab oma turvasüsteemide kaudu tõendada tehingu autentsust.

Lisaks näitab artikli sisu, et krediidiandja täiendavad kontrollimehhanismid on kooskõlas PSD2 artikli 97 ja VÕS § 724⁶ nõuetega tugeva kliendi autentimise rakendamisel. See tähendab, et digitaalsete teenuste kontekstis saab krediidiandja oma hoolsusnõudeid täita, samal ajal kaitstes eID omaniku vara pettuste eest. Kokkuvõtvalt toetab see argumenti, et eID omaniku tõendamiskoormus ei tohiks olla üleliia suur, kuna pettuste tuvastamine ja tehingu kontrollimine on krediidiandja tehniliste ja inimressurssidega teostatav. See loob õiguslase ja praktilise põhjenduse, miks tõendamiskoormuse jaotamine eID omaniku ja krediidiandja vahel on mõistlik ja kooskõlas hoolsusnõuetega.

MERAS § 114 sätestab finantsasutuste kohustuse kaitsta kliendi vara ning määrab rikkumise korral sanktsioonid rahatrahvi või kahekordses väärteto tulemusel teenitud kasu suurus. Kuna see säte reguleerib finantsasutuse kohustuste rikkumise tagajärgi ning sanktsioonid on seotud rikkumisega teenitud kasu hüvitamise või rahalise trahviga, ei ole tegemist

⁵⁶ Kalamees, P. „Näita käppa“ ehk minu digiallkiri, järelikult minu tehtud tehing. - 2024/9-10. - https://juridica.ee/article_full.php?url=2024_9-10_n_ita_k_ppa_ehk_minu_digiallkiri_j_relikult_minu_tehtud_tehing

karistusõigusliku vastutusega. Tegemist on siiski tsiviilõiguslike sanktsioonidega, sest need lähtuvad finantsasutuse lepingu- või seadusjärgse kohustuse rikkumisest ja on mõeldud kahju või rikkumise hüvitamiseks.

Autoriseeritud ja autoriseerimata tehingute puhul on vastutus selgelt määratletud VÕS-is, mille sätted on samuti üle võetud PSD2 direktiivist. Nimelt tõendamiskoormus autoriseeritud tehingu puhul lasub makseteenuse pakkujal (§ 733⁴ lg 1-2), kui on vaieldav, kas tehing on toimunud nõuetekohaselt või kas kasutatud makseinstrumenti on võimalik pettuse teel kasutada. See tähendab, et makseteenuse pakkuja peab tõendama tehingu autentimise, kliendi tugeva autentimise rakendamise, korrektselt dokumenteerimise ja kontodel kajastamise. Makseteenuse pakkuja ei vastuta kliendile tekitatud kahju eest pettuse mõjul, kui makseteenuse pakkuja suudab tõendada, et makse algatanud maksja on andnud oma nõusoleku ning makseteenuse pakkuja on tehingu täitnud kooskõlas maksejuhiseiga, sealhulgas kordumatu tunnusega. Kui maksja ei ole tehingule andnud nõusolekut või kui tehing algatati ilma nõuetekohase autentimiseta, loetakse tehing autoriseerimatuks ja peamiseks vastutajaks on makseteenuse pakkuja, kes peab tagama maksesumma tagastamise maksjale ja taastama maksja kontrol olukorra, mis oleks olnud, kui autoriseerimata makset ei oleks toimunud (§ 733² lg 2, § 733³ lg 1-2). Maksja vastutus on piiratud ja kehtib vaid juhul, kui makse tehti kadunud või varastatud makseinstrumenti kasutades või maksja rikkus tahtlikult või raske hooletuse tõttu kohustusi (§ 733⁸ lg 1-2). See kinnitab, et olukorras, kus klient ise, petturi mõjul algatab ja kinnitab tehingu, ei kaasne makseteenuse pakkujaga tsiviilõiguslikku vastutust. Samas, kui tehing on algatatud kolmanda isiku poolt, on vastutus makseteenuse pakkujal ja tõendamiskoormus selgelt määratletud PSD2 ja VÕS sätetes.

Eeltoodust tulenevalt nähtub, et pettusejuhtumi hindamisel tuleb esmalt tuvastada, kas tegemist oli autoriseeritud või autoriseerimata tehinguga. Vastutuse määramisel tuleb lähtuda peamiselt VÕS-i sätetest ning makseteenuse seaduse normidest. Autori hinnangul tekib Eesti õiguses sarnane probleem, nagu on tuvastatud Euroopa Liidu makseteenuse pakkujate direktiivi rakendamisel: kuigi seadus sätestab otseseid sätteid vastutuse määramiseks, ei ole autoriseerimata tehingu puhul selgelt nõutud kontrollida makseteenuse pakkuja hoolsusnõuete täitmist, sealhulgas turvameetmete piisavust ja riskipõhist lähenemist. Selline lähenemine ei võimalda hinnata võimalikku karistusõiguslikku vastutust. Tsiviilõiguslik vastutus on VÕS-is nii aluse kui ulatuse mõttes selgelt määratletud, probleem tekib aga hoolsusnõuete analüüsimisel. Kui ei hinnata, milles seisnes finantsasutuse rikkumine ja kas see oli oluline hoolsusmeetmete rikkumine, jääb ebaselgeks, kuidas kindlaks teha tsiviilvastutuse ulatus. Lisaks üldkohustusele tagada maksesumma tagastamine maksjale ja taastada maksja kontrol

olukord, mis oleks olnud, kui autoriseerimata makset ei oleks toimunud (VÕS § 733²-733³), näeb MERAS § 114 ette ka finantsasutuste kohustuse kaitsta kliendi vara ning määrab rikkumise korral sanktsioonid rahatrahvi või kahekordses väärteo tulemusel teenitud kasu suurus. Seega ei piisa konto taastamisest - vastutus hõlmab ka muid sanktsioone autoriseerimata tehingu korral. Turvameetmete piisavus on otseselt seotud kliendi vara kaitsmisega, mille hindamata jätmine piirab ka karistusõigusliku vastutuse analüüsi, sest see ei võimalda selgitada, kas finantsasutus võis teadlikult jätta vajalikud hoolsusmeetmed täitmata, mis tõi kliendile kahju. Karistusõiguslik vastutus tekib ainult tahtliku delikti korral. Hoolsusnõuete rikkumine maksetehingutes (VÕS § 733¹-§ 733⁹) ei too automaatselt kaasa karistusõiguslikku vastutust, vaid eeldab makseteenuse pakkuja tahtliku tegutsemist. Selle seose ja võimaliku karistusõigusliku vastutuse analüüsi käsitleb autor järgmises alapeatükis.

2.2.3. Eesti kohtupraktika

Tsiviilasjas nr 2-24-1667 esitas AS LHV Pank (hageja) hagi R.S-i (kostja) vastu, nõudes 981,19 euro tagastamist ning viivist alates 05.11.2022 kuni nõude täitmiseni, väites, et kostja viis hageja teadlikult eksimusse, esitades vale makse saaja andmed. Hageja väitis, et makse pidi minema Spece Yinja OÜ kontole, kuid kuna äriühing oli registrist kustutatud 16.08.2021, viidi makse ekslikult kostja isiklikule kontole. Hageja esitas hagi VÕS § 1027, § 1028 lg 1 ja § 1032 lg 1 alusel, tuginedes alusetu rikastumisele ning ühtlasi nõudis viivist VÕS § 113 lg 1 teise lause alusel, väites, et kostja sai hageja arvel rahalist kasu. Maakohus jättis 24.04.2025 otsusega hagi rahuldamata, tuvastades, et hageja ei olnud tõendanud, et ülekanne toimus kostja isiklikule kontole ning et kostja tegevuses ei olnud õigusvastasust ega kahju tekitamist. Maakohus analüüsis tehingu iseloomu ja leidis, et hageja oli teostanud makse ilma Spece Yinja OÜ kehtiva maksejuhiseta, mis VÕS § 724¹ lg 1 tähenduses kvalifitseerib tehingu autoriseerimata makseks. Samuti hinnati panga hoolsusnõuete täitmist, sealhulgas kohustust makseteenuse pakkujana enne makse sooritamist kontrollida makse õiguslikku alust ja vajadusel taastada maksekonto seis VÕS § 733² lg 2 alusel. Kohus leidis, et kostja ei ole viinud hagejat eksimusse valeandmete avaldamisega. Tegemist oli hageja enda eksimusega, sest hageja töötaja ise pöördus kostja poole raha ülekandmiseks. Hageja töötaja ei olnud teadlik asjaolust, et Spece Yinja OÜ kontot ei olnud suletud mitte ainult ettevõtte tegevuse lõpetamise tõttu, vaid ka seetõttu, et ettevõtte võlg hageja ees oli maksmata. Seega oli tegu eksimusega, mida oleks saanud vältida, kui hageja töötaja oleks enne makse tegemist kontrollinud ettevõtte konto staatust. Ringkonnakohus hindas apellatsioonkaebuse menetluslikke aspekte ja leidis, et maakohtu otsus ei olnud selgelt ebaõigesti kohaldatud materiaal- ega menetlusõiguse norme ning jättis apellatsioonkaebuse menetlusökonoomia

kaalutlustel menetlusse võtmata. Ringkonnakohus rõhutas, et ei saanud kostja ega tema nimel mõni muu isik anda hagejale VÕS § 709 lg 7 tähenduses makse korralduse ning hageja tegi vaidlusaluse ülekande ilma kehtiva maksejuhiseta ehk makseteenuse pakkujal ei olnud makse teostamiseks õiguslikku alust. Kokkuvõttes leidsid kohtud, et tegemist oli autoriseerimata maksega, mille tagajärjel pangal on VÕS § 733² lg 2 alusel kohustus taastada maksja maksekonto endisesse olukorda. Samas rõhutas Ringkonnakohus, et hageja ei ole tõendanud, et ta oleks maksekonto seisu taastanud, mistõttu ei saa järeldada, et kostja oleks hageja arvel rikastunud. Lisaks ei tõendanud hageja, et vaidlusalune konto kuulus kostjale. Nendel põhjustel jäi apellatsioonkaebus menetlusse võtmata.⁵⁷

Antud lahend näitab hoolsusnõuete rakendamist praktikas Eesti õiguses: ekslikult teostatud makse ei vabasta finantsasutust hoolsusnõuete täitmisest ning pangal on vastutus autoriseerimata makse teostamise eest. Hoolsusnõuete täitmine on finantsasutuse õiguslik kohustus, mis sõltub panga enda tegevusest, mitte üksnes kliendi käitumisest. Kohtu analüüs näitab, et pank on kohustatud kontrollima makse andmete õigsust veendumaks, et maksejuhis on antud õiguspäraselt, dokumenteerima maksetehinguid ning vajadusel taastama maksekonto seisundit VÕS § 733² lg 2 alusel, mis on otse võetud PSD2 direktiivist. Samuti kinnitab lahend, et kui makse on õiguslikult aluseta (autoriseerimata), ei tähenda see automaatselt kahju tekkimist, mida saaja peaks hüvitama ning vastutab pank makse eest oma arvel, mitte saaja tegevuse tõttu. Antud lahend näitab, kuidas kohtud hindavad panga ja klientide vastutust eraldi, rakendades VÕS-i sätteid hoolsusnõuete ja õiguslikult aluseta maksete kohta. See praktika on kooskõlas Euroopa Liidu õiguse üldiste põhimõtetega, mille kohaselt makseteenuse pakkuja vastutab autoriseerimata makse eest, samas kui tarbijat ei saa pidada vastutavaks, kui tema tegevus ei tekita õigusvastast kahju. Lahend illustreerib seega Eesti õiguse rakendamist autoriseerimata maksete hoolsusnõuete kontekstis, säilitades kooskõla ELi standarditega finantsvastutuse jagamisel.

Tsiviilasjas nr 2-23-11584 esitas hageja Olga Žuravska hagi Coop Finants AS-i (alates 1. aprillist 2024 Coop Pank AS) vastu, milles hageja palus tuvastada laenulepingu ja sellega seotud kindlustuskulude tasumise kokkuleppe tühisus või tunnistada need kehtetuks. Hageja väitis, et tema nimel sõlmisid lepingud kolmandad isikud, kes kasutasid tema andmeid, sealhulgas ID-kaarti, Smart-ID koodi ja isikut tõendavat fotot ning et tema ei ole tehingute sõlmimise tahteavaldust teinud. Hageja nõudis hagiavalduses lepingute tühisuse tuvastamist, viidates sellele, et laen ja konto avamine toimusid tema teadmata ning pettuse kaudu, mistõttu kostja rikkus laenuandja kohustusi.⁵⁸

⁵⁷ TlnRnKo 2-24-1667.

⁵⁸ RKTkm 2-23-11584.

Harju Maakohus keeldus hagi menetlusse võtmast, eeldades, et hageja ise andis digitaalse allkirja vahendite kaudu tahteavalduse ning märkides, et hageja esindusõiguslikku tõendit volikirja näol ei esitanud. Maakohus leidis, et hageja õiguste rikkumine ei ole tema väidete õigsust eeldades tõenäoline ning pidas hagi perspektiivituks (TsMS § 371 lg 1 p-de 9 ja 12, lg 2 p 1). Tallinna Ringkonnakohus jättis 24. novembri 2023 määrusega maakohtu resolutsiooni muutmata, kuid muutsid põhjendusi, rõhutades, et hageja ei tõendanud faktiliselt, et tema Smart-ID koodid sattusid kolmandate isikute valdusse tema tahte vastaselt. Ringkonnakohus rõhutas, et isik, kellele digitaalse allkirja vahendid on väljastatud, peab näitama hoolsust nende hoidmisel ja avaldamisel, kuid ei saanud otsustada hagi sisu üle.⁵⁹

Riigikohtu kolleegium leidis, et nii maakohus kui ringkonnakohus eksisid hagi perspektiivi hindamisel, sest hagi menetlusse võtmise otsus peab põhinema hagiavalduses esitatud faktilistel väidetest, eeldades nende õigsust (TsMS § 371 lg 2 p 1, § 340¹ lg 1). Kolleegium rõhutas, et hageja väide, et kolmandad isikud sõlmisid lepingud tema nimel, võib anda aluse hagi menetlusse võtmiseks, sest lepingute sõlmimine eeldab vastastikuseid tahteavaldusi (VÕS § 9 lg 1) ja esindusõiguseta tehing, kus tehingu tegi kolmas isik hageja identiteeti kasutades, on TsÜS § 129 lg 1 kohaselt tühine, välja arvatud juhul, kui hageja hiljem lepingud heaks kiidab. Samuti tuletati kolleegiumi praktikas meelde, et Smart-ID ja ID-kaardi vahendite puhul on tegemist digitaalallkirjaga, millel on omakäelise allkirjaga võrreldav tähendus ning mille väärkasutuse korral peab kohus arvestama hageja väidete õigsusega, et leping sõlmiti tema teadmata.⁶⁰

Kuigi Riigikohtu määrus ei käsitlenud otseselt maksetehinguid ega sisaldanud lõplikku hinnangut hageja väidete põhjendatusele, on see praktikas oluline seoses sellega, milliseid asjaolusid kohus peab asjakohaseks vaidluse edasisel lahendamisel, sh rõhutas kohus faktiliste asjaolude ja tõendite hindamise vajalikkust isiku võimaliku volituse ja vastutuse üle otsustamisel. Lahendi analüüs näitab, et kohtud peavad hindama hageja käitumist ning tema hoolsuse taset, eeldades, et digitaalsed vahendid, nagu ID-kaart ja Smart-ID, on tehingu sooritamiseks vajalikud. Sarnaselt Rootsi Riigikohtu 21.06.2022 otsusele nr T 4623-21, mida käsitles autor peatükis 2.1.2., kus hinnati tarbija (MT) vastutust autoriseerimata maksete eest pettusejuhtumis, tuleb ka kõnealuse juhtumi puhul eristada olukordi, kus isik andis kolmandale isikule volitusi tahtlikult või hooletuse tõttu. Nii nagu Rootsi kohtus hinnati MT hooletust ja „eriti süülise“ tegevust, analüüsisid Eesti kohtud Žuravska juhtumis, kas Smart-ID koodide ja ID-kaardi andmine kolmandale isikule toimus tema süül või tema tahte vastaselt ning kuidas see mõjutab tehingu kehtivust. Mõlemas juhtumis on keskne küsimus,

⁵⁹ RKTKm 2-23-11584.

⁶⁰ *Ibid.*

millises ulatuses kannab isik vastutust oma vahendite sattumise eest kolmandate isikute kätte ning millal vastutab finantsasutus või tehingu sooritaja, lähtudes hoolsusnõuete täitmisest või täitmata jätmisest. Seetõttu võib lahendeid käsitleda ühiselt praktika näidetena, kuidas kohus hindab volituste väärkasutust, hoolsuskohustuse täitmist ja vastutuse ulatust, sõltumata sellest, kas tegu on laenulepingu sõlmimise või maksetehingu autoriseerimata tehinguga.

3. FINANTSASUTUSTE KARISTUSÕIGUSLIK VASTUTUS KAR § 217² ALUSEL

Finantsasutuse tegevuses või tegevusetuses pettuse skeemide rakendamisel kurjategijate poolt küll puudub kelmuse koosseis KarS-i § 209 tähenduses, kuid autori arvates võiks teatud juhtudel kaaluda finantsasutuste võimalikku täiendava karistusõigusliku vastutuse kaasnemist. Seda põhjusel, et finantsasutustes rahaliste vahendite hoiustamise üheks peamiseks eesmärgiks oli alati olnud rahaliste vahendite turvaline säilitamine, välistades olukorda, kus isik satub varguse ohvriks. Digitaliseerides rahaliste vahendite käsutamise võimalusi, peavad finantsasutused endiselt tagama turvalist rahaliste vahendite hoiustamist, vältides või vähemalt minimiseerides sisuliselt 21. sajandi “vargust”. Digikeskkonnas, kuhu kurjategijad on liikunud koos ühiskonnaga, on tänapäeval väiksem vahelejäämise risk ning kasu on traditsioonilistest kuritegudest saadavaga võrreldes kordades suurem⁶¹. Nii on ka Advokaadibüroo Widen nõunik Siim Tammer 19.02.2026.a oma ettekandes Riigikogu istungil öelnud, et asjaolu, et finantsasutused ei lase seda vara pangast füüsiliselt ära võtta, peaks tähendama ka seda, et nad ei lase seda vara ka elektrooniliselt pangast ära võtta⁶². Käesolevas peatükis analüüsib autor KarS §-i 217² lg 1 rakendamise võimalikkust maksepettuste puhul finantsasutuste vastutuse vaatenurgast.

3.1. Usalduse kuritarvitamise koosseisu eeldused

Karistusseadustiku § 217² lg 1 kohaselt on ettenähtud karistusõiguslik vastutus isikutele, kes seadusest või tehingust tuleneva teise isiku vara käsutamise või teisele isikule kohustuse võtmise õiguse ebaseaduslikult ära kasutab või rikub teise isiku varaliste huvide järgimise kohustust ning sellega tekitab suurt varalist kahju ja isiku teos puudub KarS §-s 201 sätestatud süüteokoosseis.

Usalduse kuritarvitamise objektiivse koosseisu tunnuste hulka kuuluvad: 1) erisubjekt, kellel on õigus käsutada teise isiku vara, võtta talle varalisi kohustusi või järgida tema varalisi huve, 2) varaliste huvide järgimise kohustuse rikkumine, 3) suure varalise kahju tekkimine ning 4) teo mittevastavus KarS §-s 201 sätestatud omastamise koosseisule.

KarS § 217² kaitstavaks õigushüveks on vara sarnaselt KarS § 209 poolt kaitstavaga. Usalduse kuritarvitamise koosseisu loomise kriminaalpoliitiline vajadus seisnes selles, et võimalikult

⁶¹ Riigikogu. (2026). Küberkuritegevuse ohjeldamine finantsvaldkonnas - olulise tähtsusega riikliku küsimuse arutelu 19.02.2026. Istungi ülevaade. - <https://www.riigikogu.ee/istungi-ulevaated/riigikogu-arutas-olulise-riikliku-k-simusena-k-berkuritegevuse-ohjeldamist-finantsvaldkonnas/> (03.04.2026).

⁶² *Ibid.*

suures ulatuses katta karistatavuslõnga, mis võib tekkida varalise kahju tekitamisega, kui tegu ei vasta ei omastamise ega kelmuse koosseisude tunnustele, kattes tahtliku teise isiku vara käsutamist või teise isiku varaliste huvide järgimise kohustuse rikkumist, kui isik ei tegutse vara enda või kolmandale isikule pööramise tahtlusega.⁶³

Usalduse kuritarvitamise koosseisu KarS § 217² lg 1 alt 1 tähenduses realiseerimiseks peab eksisteerima ärakasutamisseisund, mille alusel sooritatakse tehing ja käsutatakse teise isiku vara. Ärakasutamisseisundi aluseks on kannatanu ja süüdlase vahelise tsiviil- või avalik-õigusliku suhe, mis tekib seaduse (nt eestkoste) või tehingu alusel (nt tööleping) ning annab süüdlasele esindusõiguse kannatanu vara käsutamiseks või tema nimele kohustuste võtmiseks. Kuid selline esindusõigus on tavapäraselt piiratud sisesuhtest tulenevate piirangutega nagu näiteks hoolsus- ja lojaalsuskohustus.⁶⁴

KarS § 217² lg 1 alt 1 koosseisupäraseks teoks on sisesuhte tingimusi rikkuva tehingu sõlmimine ehk seisundi ärakasutamine. Riigikohtu praktikas on usalduse kuritarvitamise koosseisupärase teo kinnitatud olukorras, kus juhatuse liige on sõlminud ühingu lepingu teise juriidilise isikuga, kellele see tehing oli kasulik ja kellega juhatuse liige oli isiklikult seotud. Selles kohtuasjas on juhatuse liige rikkunud sisesuhtest tuleneva lojaalsuskohustust ehk kasutanud ära oma seisundi, mis annab talle õigust lepingute sõlmimiseks⁶⁵. Vara käsutamise õiguse kuritarvitamiseks on teise isiku nimel tema teadmata või kehtestatud kooskõlastuskorda rikkudes ebaseaduslike tehingute tegemine ja kohustuste võtmine, mida teine isik täita ei saa. Koosseisupäraseks tehinguks on kehtiv tehing, mis annab aluse vara käsutamiseks või kohustuste võtmiseks. Seega ei ole koosseisupärane näiliku tehingu tegemine või tehingu tegemine vastaspoolega, kes on teadlik esindusõiguse puudumisest TsÜS § 129 mõttes.⁶⁶

Käesoleva magistritöö raames on keskse tähendusega makseteenuse leping kui finantsasutuste ja ohvrite vahelise tsiviilõigusliku suhte alus. Makseteenuse leping reguleerib konto avamist, pidamise tingimusi, kasutamist, käsutamist, sulgemist ja muid makseteenuste osutamiseks vajalikke tingimusi. Nii makseteenuse lepingute raames makse sooritamiseks peab maksja ehk klient andma finantsasutusele makseteenuse lepingus kokkulepitud viisil nõusoleku maksetehingu teostamiseks ehk autoriseerima maksejuhise - maksetehingu korraldus, mille klient annab pangale, sealhulgas saaja kaudu. Finantsasutus omakorda aktsepteerib⁶⁷ või

⁶³ Sootak, J., Pikamäe, P. (koostajad). Karistusseadustik kommenteeritud väljaanne. Tallinn: Juura 2021, e-väljaanne, § 217² komm 1 - <https://karistusseadustik.juuraveeb.ee/>.

⁶⁴ *Ibid*, § 217² komm 3.2.

⁶⁵ RKKK 3-1-1-61-09.

⁶⁶ Sootak, J. Pikamäe, P. Karistusseadustik kommenteeritud väljaanne (viide 63), § 217² komm 3.3.

⁶⁷ Maksejuhiste aktsepteerimise tingimused. - RTL 2010, 25, 446; § 2 lg 4.

lõkkab tagasi maksejuhise.⁶⁸ Finantsasutuste võimaliku vastutuse kontekstis tavapäraste petukõnede puhul, kui ohver teeb petturitele ülekande, ei ole antud alternatiiv asjakohane, kuna finantsasutus ei kasuta tehingust tuleneva teise isiku vara käsutamise õiguse ebaseaduslikult ära. Seda põhjusel, et maksejuhise aktsepteerimise näol ei ole tegemist vara käsutamisega, vaid selle kinnitamisega. Seega ei ole finantsasutustel KarS § 217² lg 1 alt 1 jaoks vajalikku esindusõigust kliendi vara käsutamiseks ilma kliendi poolset tegevust ehk maksejuhist.

KarS § 217² lg 1 alt 1 ei ole asjakohane ka õngitsuskõnede (*vishing*'u) puhul. Olukorras, kus petturid saavad petmise teel e-ID andmeid, logivad sisse internetipanka ning teevad ülekandeid või võtavad ohvrite nimele laenu, panevad nemad toime arvutikelmust KarS § 213 tähenduses, sisestades ebaseaduslikult andmed ja käivitades seekaudu lubamatult andmetöötlusprotsessi. Nendel juhtudel on finantsasutuste tegevuseks samamoodi üksnes maksejuhise aktsepteerimine, mitte aga sisesuhte tingimusi rikkuva tehingu sõlmimine, sealhulgas kliendi nimele kohustuse võtmine, kui oma seisundi ärakasutamine. Nende kahe pettuse liigi oluliseks erinevuseks käesoleva magistrilöö vaatevinklist on asjaolu, et õngitsuskõnede puhul teeb finantsasutus põhimõtteliselt ekslikult maksejuhise aktsepteerimise, kuna maksejuhise andjaks ei ole klient ise, vaid pettur ja finantsasutus on petetud maksejuhise andva isiku õigsuses.

Karistusseadustiku § 217² lõike 1 alternatiivi 2 näol ehk teise isiku varaliste huvide järgimise kohustuse rikkumise näol on tegemist usalduse murdmise koosseisuga. Usalduse murdmise koosseis on oma olemuselt oluliselt laiem kui ärakasutamiskoosseis, kuna selle täitmiseks ei ole vajalik toimepanija vara käsutamise või kohustuste võtmise õiguse olemasolu, piisab vaid usaldusseisundi ehk varaliste huvide järgimise kohustuse olemasolust. Usaldusseisund toimepanijal lasuvast hoolsus- ja järelevalvekohustusest kui teise isiku varaliste huvide järgimise kohustusest, mis põhineb avalik- või tsiviilõiguslikul suhtel, on oma olemuselt laiem kui vara käsutamise või kohustuste võtmise õigus. Usaldusseisund võib lisaks juriidilise isiku nõukogu liikme või, käsundisaaja omadele olla võetud ka muude lepinguliste kohustuste vormis⁶⁹. Olukorras, kui isikute vahel sõlmitud tehingu alusel on tekkinud usaldusseisund, peab teise isiku varaliste huvide järgimise kohustuse tuletama tehingus sätestatud kohustustest. Teise isiku varaliste huvide järgimise kohustuse näol ei ole tegemist tsiviilõiguslikult defineeritud instituudiga. Seega tuleb vastava kohustuse olemasolu igakord tehingu tingimuste tõlgendamisel tuvastada. Hoolsus- ja järelevalvekohustus peab olema

⁶⁸ Luminor kontolepingu tingimused. - <https://luminor.ee/s3fs-public/documents/luminori-kontotingimused.pdf> (15.03.2026).

⁶⁹ Kairjak, M., Sootak, J. Varavastased süüteod. Tallinn: Juura 2017, vnr 8.

suunatud teise isiku varaliste huvide järgimisele ja olema oluline kohustus kogu tehingu seisukohalt ehk nende näol peab olema tegu tehingu kesksema kohustusega. Sellise hoolsus- või järelevalvekohustuste lasumist finantsasutustel makseteenuslepingu puhul analüüsis autor käesoleva magistritöö 2. peatükkis.⁷⁰

KarS § 217² lõike 1 alternatiivi 2 puhul koosseisupäraseks teoks on hoolsus- ja järelevalvekohustuse, mis on suunatud varaliste huvide järgimisele, rikkumine. Kohustuse sisu ja ulatuse määratlemine ning rikkumise mõiste sisustamine toimub läbi VÕS 4. ja 5. peatükki. Teisisõnu tegemist on tsiviilõigusaktssesoorse koosseisuga kohustuse rikkumise osas - koosseisupärane rikkumine peab olema rikkumiseks tsiviilõiguse tähenduses. Võlaõigusseaduse § 100 kohaselt kohustuse rikkumiseks on võlasuhtest tuleneva kohustuse täitmata jätmine või mittekohane täitmine, sealhulgas täitmisega viivitamine. Võlaõigusseaduse §-s 709 sätestatud ja käesoleva magistritöö jaoks keskse tähendusega olev makseteenuse leping on võlasuhe VÕS § 2 lg 1 tähenduses. Hoolsus- või järelevalvekohustuse rikkumine võib toimuda nii tegevuse kui ka tegevusetuse kaudu (näiteks kui vallasekretär ei püüa peatada kohaliku omavalitsuse jaoks kahjuliku tehingu täitmist). Varaliste huvide järgimise kohustuse rikkumine tuleb kõne alla olukorras, kus näiteks õigus- või finantsnõustamise teenuse pakkuja kasutab ära kliendi nõustamisel saadud informatsiooni enda huvides (finantsnõustaja omandab soodsalt kinnisvara, millest sai teada kliendi käest ja ostab selle ise ära). Kohustuse rikkumine peab olema ebaseaduslik.⁷¹

KarS § 217² koosseis eeldab tagajärjena isikul, kelle usaldust kuritarvitatakse suurt varalist kahju KarS § 12¹ punkti 2 tähenduses ehk kahju peab ületama 4000 eurot. Vastutusele võtmise piiramine suure varalise kahju tekitamisega on tehtud selleks, et vältida KarS § 217² muutmist tsiviilkohtumenetluse alternatiiviks.⁷²

Usalduse kuritarvitamise koosseisu subjektiivne külg eeldab tahtlust koosseisu kõigi asjaolude suhtes ehk koosseisu võib lugeda täidetuks siis, kui isik tegutseb vähemalt kaudse tahtlusega KarS § 16 lg 4 tähenduses nii teo kui tagajärje suhtes. KarS § 16 lg 4 kohaselt tegemist on kaudse tahtlusega siis, kui isik peab võimalikuks süüteoosseisule vastava asjaolu saabumist ja möönab seda. Teisisõnu usalduse kuritarvitaja nägi ette võimalikku kahju suurusjärku ehk seda, et tegemist võib olla suure varalise kahjuga ning seda, et tema rikkub temal lasuvat kohustust järgida teise isiku varalisi huve.⁷³

⁷⁰ Sootak, J. Pikamäe, P. Karistusseadustik kommenteeritud väljaanne (viide 63), § 217² komm 4.1-4.2.

⁷¹ *Ibid*, § 217² komm 4.3.

⁷² *Ibid*, § 217² komm 6.1-6.2.

⁷³ *Ibid*, § 217² komm 7.

Seega usalduse kuritarvitamise koosseisude realiseerimiseks esiteks peab olema tegemist erisubjektiga, kellel on kas alternatiivi 1 kohaselt õigus käsutada teise isiku vara või võtta talle varalisi kohustusi (*ärakasutamisseisund*) või alternatiivi 2 kohaselt kohustus järgida isiku varalisi huve (*usaldusseisund*). Teiseks peab isik kas kasutama ära oma seisundi (alt 1) või rikkuma temal lasuvat kohustust (alt 2). Kolmandaks peab rikkumise või ärakasutamisega kaasnema kahju, mis ületab 4000 eurot ning neljandaks tagajärg peab olema omistatav. Hoolsuskohustuse näol peab olema tegemist tehingu kesksema kohustusega, mis on suunatud teise isiku varaliste huvide järgimisele. Käesoleva magistritöö autor leiab, et finantsasutuste võimalik vastutusele võtmine maksepettuste puhul võiks kõne alla tulla KarS § 217² lõike 1 alternatiivi 2 rakendamise kaudu.

Järgmises alapeatükis hakkab autor analüüsima finantsasutustel lasuvate hoolsuskohustuste võimalikku rikkumist maksepettuste toimepanemisel kurjategijate poolt ning hindama KarS § 217² lõike 1 alternatiivi 2 rakendamise võimalust.

3.2. Finantsasutuste hoolsusnõuete täitmata jätmise/rikkumise ja KarS § 217² seos

Finantsasutuste võimaliku hoolsusnõuete puuduliku täitmise või täitmata jätmise hindamisel petukõnede puhul ning sellega kaasneda võiva karistusõigusliku vastutuse hindamisel on asjakohane usalduse kuritarvitamise koosseisu teine alternatiiv ehk usaldusseisundi koosseis KarS § 217² lg 1 alt 2. Karistusseadustiku § 217² lg 1 alt 2 kui usalduse kuritarvitamise objektiivse koosseisu tunnuste hulka kuuluvad: 1) erisubjekt, kellel on kohustus järgida teise isiku varalisi huve, 2) varaliste huvide järgimise kohustuse rikkumine, 3) suure varalise kahju tekkimine ning 4) tagajärg on omistatav. Usalduse kuritarvitamise koosseisu subjektiivne külg eeldab omakorda vähemalt kaudset tahtlust KarS § 16 lg 4 tähenduses koosseisu kõigi asjaolude suhtes ehk seda, et usalduse kuritarvitaja nägi ette võimalikku kahju suurusjärku ja seda, et tema rikkub temal lasuvat kohustust järgida teise isiku varalisi huve.

Selleks, et rääkida KarS § 217² lg 1 alt 2 alusel finantsasutuse karistusõiguslikkule vastutusele võtmisest, peab esialgu tuvastama, kas finantsasutustel lasuvad ja seadustest tulenevad hoolsus- ja järelevalvekohustused on suunatud teise isiku varaliste huvide järgimisele ja on olulised kohustused kogu tehingu seisukohalt ehk kas nende näol on tegemist tehingu kesksete kohustustega. Seejärel tuleb läbi viia konkreetsete pettuste liikide (petukõnede erinevad variandid) ja siseprotsesside analüüsi, et selgitada välja, kas pank on täitnud oma hoolsusnõudeid ehk rakendanud piisavaid kontroll- ja turvameetmeid või jätnud olulised riskid teadlikult tähelepanuta ehk tahtlikult rikkunud kohustust järgida kliendi varalisi huvisid.

Võttes arvesse, et kliendid on vabatahtlikult ära viinud oma rahaliste vahendite hoiustamist finantsasutustesse, võib tõdeda, et finantsasutustes rahaliste vahendite hoiustamise üheks peamiseks eesmärgiks oli alati olnud rahaliste vahendite turvaline säilitamine, välistamaks olukorda, kus isik satub varguse ohvriks. Eesti seadusandluses on finantsasutustele ettenähtud mitmed hoolsus- ja järelevalvekohustused. Petukõnede ja finantsasutuste KarS § 217² lg 1 alt 2 alusel vastutusele võtmise kontekstis on autori hinnangul peamiseks kohustuseks autentimise kohustus. VÕS § 724⁶ lg-d 3 ja 4 sisaldavad tugeva autentimise ja dünaamilise sidumise nõudeid, mis on kehtestatud elektrooniliste maksete jaoks. Selle sätte kohaselt tehingu autoriseerimiseks peab makseteenuse pakkuja kasutama vähemalt kahte sõltumatut turvaelementi ning kaugteel tehtud maksete puhul peab kasutama ka dünaamilist seost ehk autentimine peab olema seotud konkreetse tehingu summa ja saajaga. See hoolsuskohustus on sisuliselt hõlmatud ka RahaPTS §-ga 20, mille kohaselt lasub finantsasutustel kohustus tuvastada kliendi, kontrollides andmeid usaldusväärse allika kaudu, sealhulgas e-identimise kaudu. VÕS § 724⁶ lg 2, viitab muuhulgas EBA poolt välja töötatud tehnilistele regulatiivsetele standarditele tugeva kliendi autentimise ja turvalise kommunikatsiooni kohta. EBA regulatsioonist tulenevalt peavad finantsasutused hindama iga tehingu riski erinevate indikaatorite alusel, sealhulgas võtta arvesse maksetehingu summat, kasutatavat seadet, võimalikku pahavara olemasolu ning ebatavalisi kasutusmustreid. Selline operatsiooniriskide juhtimise kohustus sisaldub MERAS §-s 63⁵. Seega eelnimetatud finantsasutustel lasuvad hoolsuskohustused on suunatud klientide varaliste huvide järgimisele, minimiseerides autoriseerimata, ebatavalisi ja pettuslikke tehingute toimumist ning nende näol on tegemist tehingu keskmate kohustustega. Seda põhjusel, et rahaliste vahendite turvalise säilitamise puudumisel ei oleks makseteenuse kasutajatel mingit huvi makseteenuslepingute vabatahtlikuks sõlmimiseks.

Petukõnesid on sisuliselt kahte tüüpi. Esimeseks on standartne petukõne, mille tagajärjena teeb finantsasutuse klient ehk ohver varakäsutuse ise või annab oma kontole teadlikult ligipääsu teisele isikule. Varakäsutus võib toimuda mitmel erineval viisil. Justiits- ja Digiministeeriumi 2024. aastal Eestis toimunud kuritegevuse kohta käiva analüüsis olid toodud järgmised petukõnedes antud juhised: 1) raha tuleb kanda teisele “turvalisele” kontole, 2) raha tuleb võtta sulas välja ja panna pakiautomaati, 3) anda sularaha koju järgi tulevale kullerile, 4) vormistada (kiir)laenu, 5) anydesk lahenduse kaudu tuleb luua enda seadmetele juurdepääs, et “spetsialist” saaks kontodel ise tegutseda, 6) tuleb ära anda “ohustatud” pangakaart ja paroolid, 7) kanda raha krüptokontole, 8) müüa maha kinnisvara⁷⁴. Kuigi mitte

⁷⁴ Justiits- ja Digiministeerium. (2024). Kuritegevus Eestis 2024: Kelmused. - <https://www.justdigi.ee/kuritegevus2024/kelmused.html> (25.03.2026).

kõik nendest juhistest on antud magistritöö kontekstis asjakohased, sest need ei toimu interneti maksetena, leiab käesoleva magistritöö autor leiab, et kõigil nendel juhtumitel ei tule kõne alla finantsasutuste karistusõiguslik vastutus. Seda põhjusel, et kõikidel nendel juhtumitel on makseteenuse kasutaja teadlik, kas sellest, et tema teeb varakäsituse ehk ühel või teisel moel annab oma rahalised vahendid oma valdusest ära, teadlikult annab teisele isikule ligipääsu oma rahaliste vahendite juurde või võtab rahalist kohustust (laenute puhul). Nende kõiki juhtumite puhul, isegi kui need toimuvad elektrooniliste maksetena, ei ole finantsasutus rikkunud temal lasuvaid hoolsuskohustusi. Elektrooniliste maksete puhul ehk näiteks rahaliste vahendite ülekandmisel kas krüptokontole või “turvakontole”, mis ilmselgelt ei kuulu ohvrile endale, läbib ohver ise VÕS § 724⁶ lg-ga 3 nõutud tugevat autentimist VÕS § 709 lg-s 12² tähenduses. Olukorras, kus finantsasutus on küsinud tehingu sooritamiseks kahte turvaelementi, teinud ka dünaamilist sidumist ning klient on omakäeliselt sisestanud e-ID PIN-koodid ja kinnitanud maksejuhise andmist, ei esine finantsasutuse VÕS § 724⁶ lg-tes 3 ja 4 ning RahaPTS §-s 20 sätestatud hoolsuskohuse rikkumist. Sellisel juhul tegemist on üksnes kliendile kuuluva riskiga, sarnaselt olukorraga, kus klient otsustab panna raha pakiautomaati, kuna nendel juhtudel leiab aset kelmuse kui enesekahjustusdeliktile omane kannatanu enda varakäitus⁷⁵. Finantsasutuste poolt on loodud turvameetmed sisuliselt ka puhkudeks, kui klient võtab sularaha välja ja annab üle petturitele ühel või teisel moel. Nimelt, et Eestis asuvatel finantsasutustel seatud sularaha väljavõtmise limiidid, millede kohaselt on päevalimiidiks enamasti 3500 eurot ehk summa, mis ei ületa KarS § 12¹ punktis 2 sätestatud suurt varalist kahju ning kuulimiiks 7500 eurot, mida finantsasutused võivad erandjuhtudel tõsta, küsides mis eesmärgil on kliendil seda vaja. Limiidid annavad kliendile võimaluse oma tegevust rahulikumalt läbi mõelda. Seega olukorras, kus ohver läbib iseseisvalt tugevat autentimist ning teeb varakäituse omakäeliselt ära või omakäeliselt ja teadlikult (arusaades, et annab teisele isikule ligipääsu, sealhulgas ka uskudes, et annab näiteks pangatöötajale), annab petturitele ligipääsu ei rikku finantsasutused nendel lasuvaid hoolsuskohustusi ja seega ei kaasne ka võimalikku karistusõiguslikku vastutust KarS § 217² lg 1 alt 2 alusel. Kõne alla ei tule ka MERAS § 113 lg 2 alusel vastutust, kuna finantsasutused ei rikku sellisel juhul lisaks ka operatsiooniriskide juhtimise kohustust, mis sisaldub MERAS §-s 63⁵ ja millele viitab muuhulgas ka VÕS § 724⁶ lg 2 EBA regulatsiooni kaudu. Seda põhjusel, et ei ole võimalik teha etteheidet finantsasutustele selle kohta, et maksejuhise oli antud ja tugev autentimine läbitud uue seadme ja Smart-ID kaudu, mis võiksid viidata võimalikule identiteedipettusele finantsasutuse suhtes ehk puudub üldse mingi kahtlus, et tugevat autentimist on kuidagi võltsitud.

⁷⁵ P. Pikamäe. Mõningad kelmuse üldkoosseisu sisustamisprobleemid kohtupraktikas. - Juridica 2011/2, lk 2.

Teiseks petukõnede alternatiiviks on *vishing* ehk õngitsuskõnesid, kus petturid saavad petmise teel e-ID andmeid, logivad sisse internetipanka ning teevad ülekandeid või võtavad ohvrite nimele laenu. Selliste petukõnede tagajärjena on identiteedipettus ja petetakse finantsasutust ennast, kuna makseteenuselepingu kasutajana astub üles teine isik, kes saab ligipääsu teise isiku kontol olevatele rahalistele vahenditele ning kellel tegelikult ei tohiks olla. Kõige levinumaks skeemiks on pangatöötajana või politseinikuna esinemise pettus, mille toimepanemisel, hoiatatakse kontohäkkimise eest ja veendakse ohvrit tühistada Smart-ID, luues aga tegelikult seekaudu ohvri andmetega uus Smart-ID⁷⁶. Sellise pettuse liiki probleemkohaks on ka Smart-ID süsteemi loomise tingimused. Nimelt on Bigbanki pettuste tõkestamise osakonna juht Kristofer Evert oma intervjuus öelnud, et tänapäeva suureks probleemiks on fakt, et inimesele Smart-ID loomiseks ei ole vaja läbida näotuvastust ja näokuva võrdlust kehtiva isikutuvastusdokumendiga, mis lihtsustab kurjategijate elu ja soodustab pettuste laia levikut⁷⁷. Formaalselt on ka sellisel juhul täidetud VÕS § 724⁶ lg-s 3 nõutud tugeva autentimise kohustus, kuna maksetehing on kinnitatud isikustatud turvaelementide abil. Kuid käesoleva magistritöö autor leiab, et sellise petuskeemi puhul on alust rääkida finantsasutuste hoolsuskohustuse rikkumisest. Seda põhjusel, et autentimise ajal saadetakse autentimist läbi viivale isikule ehk finantsasutusele, sertifikaat, mis näitab muuhulgas ka selle kehtivusaega (alguskuupäev - lõpp)⁷⁸. Finantsasutustel on võimalus võtta rakendusele mehhanisme, mis hakkavad analüüsima sertifikaatide alguskuupäevad ning kontrollima, kas kliendi sisselogimised toimuvad üksnes ühe või mitme sertifikaatidega. Selline kohustus on tuletatav VÕS § 724⁶ lg-st 2 ehk EBA regulatsioonist, mille kohaselt peavad finantsasutused hindama iga tehingu riski erinevate indikaatorite alusel, sealhulgas võtta arvesse maksetehingu summat, kasutatavat seadet, võimalikku pahavara olemasolu ning ebatavalisi kasutusmustreid. Olukorras, kus petturid on loonud enda seadmesse uue Smart-ID kliendi nimele, tekivad kaudsed viited, et kasutusel on uus seade (sertifikaadi loomise kuupäeva järgi) ning petturid hakkavad suurema tõenäosusega tegema ebatavaliselt suured ülekanded ehk leiab aset ebatavaline kasutusmuster. Sellises olukorras peaks pank tegema täiendavat isiku tuvastamist, kuna on oht, et tugev autentimine oli petuslikult läbitud ning sisuliselt ei ole finantsasutus täitnud kõiki hoolsusnõudeid autentimisel ning tehing on

⁷⁶ Elisa Eesti. (30.10.2025). Uue Smart-ID loomisega seotud pettused põhjustavad miljonikahjusid - inimesed ei teadvusta ohumärke. -

<https://www.elisa.ee/et/uudised/ue-smart-id-loomisega-seotud-pettused-pohjustavad-miljonikahjusid-inimesed-ei-teadvusta> (08.04.2026).

⁷⁷ Postimees Majandus. (12.12.2025). Bigbank: pettustele piiri panemiseks tuleb Smart-ID loomise protseduur ümber teha -

<https://majandus.postimees.ee/8378672/bigbank-pettustele-piiri-panemiseks-tuleb-smart-id-loomise-protseduur-umber-teha> (08.04.2026).

⁷⁸ SK ID Solutions AS, Kvalifitseeritud Smart-ID sertifikaatide kasutustingimused (alates 15.04.2024). - <https://c.sk.ee/SK-TCU-QUALIFIED-SMART-ID-ET-CURRENT.pdf> (03.04.2026).

tegelikult autoriseerimata. Uue seadme kaudu autoriseerimise ja ebatavalise kasutusmustril ilmunisel võiks kõne alla tulla finantsasutuste poolt operatsiooniriski juhtimise kui hoolsuskohustuse rikkumine, mis sisaldub MERAS §-s 63⁵ ja millele viitab muuhulgas ka VÕS § 724⁶ lg 2 EBA regulatsiooni kaudu. Kuid sellise pettuse liiki puhul ka olukorras, kus ohvrile tekitatakse suurt varalist kahju KarS § 12¹ punktis 2 sätestatud, võib olla raske rääkida tahtlusest kõikide koosseisu asjaolude suhtes ning on vaja igat pettuse juhtumit hinnata üksikasjalikult, analüüsides finantsasutuse tegevust, makseteenuse kasutaja käitumismustrit ning petturite tegevust. Seda põhjusel, et pangaliidu liikmepankade andmetel on 2025. aastal mitme kuu jooksul leidnud aset 133 sellist pettuse juhtumi kahju summaga kokku üle 2,5 miljoni eurot, kuid pankadel on õnnestunud ära hoida pea sama suuruses kahju tekkimist⁷⁹. See näitab, et pangad panustavad sellise pettuse liiki tuvastamisse ja ära hoidmisesse. Samuti ei pruugi petturid teha koheselt ülekandeid või võtta laenud, mis erinevad kliendi käitumismustrist oluliselt. Teisisõnu, leiab käesoleva magistritöö autor, et ainuüksi uue sertifikaadi alusel maksejuhiste andmise korral ja ebatavalise käitumise puudumisel, ei ole põhjendatud rääkida finantsasutuste kaudsest tahtlusest KarS § 16 lg 4 tähenduses kõikide KarS § 217² lg 1 alt 2 koosseisu tunnuste kohta. Kuid tahtluse või suure varalise kahju mitte täitmisel võib kaasneda selliste pettuste tagajärjena finantsasutuste vastutus väärteokoosseisu MERAS § 113 lg 2 alusel ehk maksekonto pidamise nõuete ehk MERAS §-s 63⁵ ja MERAS § 63 lg 1 (viitab VÕS 40. ptk-le, sealhulgas VÕS §-le 724⁶) rikkumise eest.

Eespool öeldust tulenevalt, leiab käesoleva magistritöö autor, et reeglina ei kaasne finantsasutuste karistusõiguslikku vastutust KarS § 217² lg 1 alt 2 alusel, kuna tänapäeva petukõnede tagajärjena toimuvad enamasti autoriseeritud maksed. Makseteenuse kasutajad logivad internetipanka, teevad varakäsutused iseseisvalt, läbides tugevat autentimist, või teadlikult annavad teisele isikule ligipääsu oma kontole, kuigi eksides. Finantsasutuste vastutus võib kõne alla tulla *vishing*'u ehk õngitsuskõnede puhul, kus petturid saavad petmise teel e-ID andmeid, logivad sisse internetipanka ning teevad ülekandeid või võtavad ohvrite nimele laenud. Sellisel juhul toimub finantsasutuste suhtes identiteedipettus ning teatud kelmuse juhtumite puhul on alust rääkida finantsasutuste poolt hoolsusnõuete rikkumisest ning vastutusest kas KarS § 217² lg 1 alt 2 või MERAS § 113 lg 2 alusel, sõltuvalt varalise kahju suurusest ja subjektiivse koosseisu täidetusest.

⁷⁹ Elisa Eesti. (30.10.2025). Uue Smart-ID loomisega seotud pettused põhjustavad miljonikahjusid - inimesed ei teadvusta ohumärke. - <https://www.elisa.ee/et/uudised/uu-smart-id-loomisega-seotud-pettused-pohjustavad-miljonikahjusid-inimesed-ei-teadvusta> (08.04.2026).

4. DE LEGE LATA JA DE LEGE FERENDA HINNANGUD

4.1. De lege lata hinnang: kehtiva õiguskorra analüüs Eestis

Käesolevas peatükis antakse hinnang kehtivale õigusele (*de lege lata*), tuginedes eelnevates peatükkides käsitletud finantsasutuste hoolsusnõuetele ning karistusõigusliku vastutuse eeldustele. Analüüsi eesmärk on hinnata, kas kehtiv õigusraamistik võimaldab piisavalt tõhusalt ennetada maksepettusi ning tagada finantsasutuste vastutus olukordades, kus kliendi vara käsutamine toimub pettuse mõjul. Seejuures keskendutakse eelkõige küsimusele, kas kehtivad normid koos finantsasutustele kehtestatud hoolsusnõuetega moodustavad selge ja toimiva regulatsiooni või esineb selles puudujääke.

Eesti kohtupraktika analüüs näitab, et finantsasutuste võimalikku karistusõiguslikku vastutust käsitlevad lahendid puuduvad. Autori läbiviidud kohtupraktika otsingu tulemusel ei tuvastatud lahendeid, milles oleks sisuliselt analüüsitud finantsasutuse rolli kliendi vara käsutamise võimaldamisel pettuse mõjul ega hinnatud selle pinnalt karistusõigusliku vastutuse eeldusi, sealhulgas KarS § 217² kohaldamise kontekstis. Seevastu ilmneb, et pettuse juhtumite käsitlemisel keskendub kohtupraktika valdavalt teo vahetule toimepanijale, kelle tegevust hinnatakse KarS § 209 alusel. Selline lähenemine viitab praktika fookusele petturi tuvastamisel ja vastutusele võtmisel, samas kui finantsasutuse võimalik roll pettuse realiseerumisel seoses hoolsusnõuete täitmata jätmisega ei jõua karistusõigusliku analüüsi tasandile. Eeltoodust võib järeldada, et kuigi teoreetiliselt ei ole välistatud finantsasutuse karistusõiguslik vastutus olukordades, kus kliendi vara käsutamine toimub finantsasutuste suhtes identiteedipettuse toimepanemise tagajärjena, ei kajastu selline käsitus kehtivas kohtupraktikas. Finantsasutuse roll võib sellistes juhtumites jääda kas menetluslikult tagaplaanile või käsitletakse seda muudes õiguslikes raamides, eeskätt võlaõigusliku vastutuse kontekstis või isegi kannatanu positsioonis. Selline praktika võib viidata olukorrale, kus finantsasutuste suhtes karistusõigusliku vastutuse kohaldamine on kas õiguslikult raskendatud - näiteks tulenevalt tahtluse tõendamise kõrgest lävest või ei peeta seda praktikas põhjendatuks. Samas tõstatab see küsimuse, kas kehtiv õigusraamistik võimaldab piisavalt tõhusalt hinnata ja vajadusel sanktsioneerida olukordi, kus finantsasutuse tegevus või tegevusetus võib kaasa aidata pettuse realiseerumisele.

Lisaks karistusõigusliku vastutuse käsitlemise puudumisele ilmneb kohtupraktikast, et ka finantsasutuse võlaõigusliku vastutuse hindamine on teatud juhtudel suhteliselt piiratud. Autori poolt analüüsitud lahendite põhjal ilmneb, et keskendub kohus eelkõige küsimusele, kas tegemist oli autoriseerimata maksetehinguga, s.t kas makseteenuse kasutaja on andnud

tehingu teostamiseks kehtiva nõusoleku. Juhul kui tuvastatakse, et klient ei ole tehingut autoriseerinud ega ole tegutsenud tahtlikult või raske hooletuse tõttu, kohaldatakse finantsasutuse suhtes üldjuhul VÕS § 733² lg 2, mille kohaselt on finantsasutus kohustatud taastama maksekonto seisundi, mis eksisteeris enne vaidlusaluse tehingu tegemist. Seejuures ei nähtu praktikas ulatuslikumat analüüsi selle kohta, kas ja millisel määral finantsasutus rakendas piisavaid hoolsusmeetmeid maksepettuse ennetamiseks. Näiteks jäävad sageli käsitlemata küsimused finantsasutuse tehingute jälgimise mehhanismide tõhususe, riskipõhiste kontrollide rakendamise ning võimaliku reageerimiskohustuse kohta olukorras, kus tehingu asjaolud võisid viidata pettusele. Selline lähenemine viitab sellele, et finantsasutuse vastutus realiseerub praktikas eelkõige formaalse kriteeriumi kaudu, nagu tehingu autoriseeritus, samas kui hoolsusnõuete tegelik täitmine ja nende võimalik roll pettuse ärahoidmisel ei kujune kohtupraktikas iseseisvaks hindamisobjektiks. See omakorda võib piirata õigusvõimet anda sisulist hinnangut finantsasutuse tegevusele või tegevusetusele maksepettuse kontekstis.

Riigi Infosüsteemi Ameti ja õigusteadlaste hinnangul on Eestis sagenenud juhtumid, kus inimesed satuvad pettuse ohvriks oma e-ID andmete lekkimise tõttu, mis võimaldab petturitel tühjendada kannatanu pangakonto või võtta laene tema nimele. Kuigi krediidasutused on kohustatud kliendile kahju hüvitama, lasub ohvril suur tõendamiskoormus, näiteks tõestada, et makse või laen tehti tema nõusolekuta. Õigusteadlaste hinnangul peaks tõendamiskoormus siiski lasuma pigem finantsasutusel, sest digitaliseerimise kasu on enim asutustele endile ning seda põhimõtet rakendatakse näiteks Norras, kus krediidasutused peavad tõendama, et klient oli tehingust teadlik.⁸⁰ Sellest võib järeldada, et Eesti kehtivas kohtupraktikas keskendutakse peamiselt tehingu autoriseeritusele ja rahalisele hüvitamisele, mis kinnitab ka autori varasemat järeldust, et hoolsusnõuete sisuline hindamine ja finantsasutuse kontrollmehhanismide tõhususe analüüs ei ole hetkel kohtupraktikas rõhutatud. Selline lähenemine võib vähendada finantsasutuste motivatsiooni pettusi ennetada, kuna võlaõiguslik vastutus rakendub ka juhul, kui finantsasutus on kõik nõutavad hoolsusmeetmed rakendanud, mistõttu puudub otsene seos hoolsuskohustuse täitmise ja vastutuse vältimise vahel. Seetõttu on oluline kohtu tasandil hinnata ka finantsasutuse kontrollmehhanismide tõhusust ning tuvastada võimalikud rikkumised või puudujäägid, mis omakorda võib luua alust ka karistusõiguslikuks vastutuseks, olukordades, kus pettust oleks võimalik olnud ennetada.

⁸⁰ Õigusteadlased: pangad peavad tarbijaid petturite eest paremini kaitsma. Novaator (ERR). - <https://novaator.err.ee/1609754031/oigusteadlased-pangad-peavad-tarbijaid-petturite-eest-paremini-kaitsma> (25.07.2025).

4.2. *De lege ferenda* hinnang: normatiivsed kaalutlused ja võimalikud arengusuunad

Euroopa Liidu tasandil on finantsasutuste vastutuse küsimus maksepettuste kontekstis muutumas üha aktuaalsemaks. Euroopa Parlamendi ja Euroopa Liidu Nõukogu vahel on saavutatud poliitiline kokkulepe regulatsiooni osas, mille eesmärk on laiendada makseteenuse pakkujate vastutust pettuse teel teostatud maksete puhul. Rahandusministeeriumi finantsteenuste poliitika osakonna nõunik Jarmo Lilium jagas, et läbirääkimised, mis kestsid alates 2023. aastast, olid keerukad ning erimeelsused liikmesriikide vahel puudutasid eelkõige vastutuse ulatust ja jaotust. Kavandatava regulatsiooni kohaselt nähakse ette, et makseteenuse pakkuja vastutab olukorras, kus pettur esineb kliendi makseteenuse pakkujana ning selle tulemusena toimub kliendi eksitamine ja makse sooritamine. Vastutus on seejuures piiratud juhtudega, kus pettus on otseselt seotud finantsasutuse identiteedi ärakasutamisega, näiteks kui pettur esineb konkreetse panga töötajana, kus kliendil tegelikult konto asub. Seevastu ei kohaldu vastutus juhtudel, kus klient on tegutsenud hooletult või kui pettur esineb muu isikuna, näiteks riigiametniku või teenusepakkujana. Regulatsiooni üheks keskseks eesmärgiks on tugevdada kliendi usaldust makseteenuse pakkujate vastu, arvestades, et just see usaldussuhe võimaldab pettustel realiseeruda. Samas on makseteenuse pakkujad väljendanud vastuseisu sellise vastutuse laiendamisele, leides, et pettus toimub sageli nende kontrolli alt väljas ning seotud kliendi enda käitumisega, eelkõige autentimisandmete edastamisega petturile.⁸¹ Kehtiva õiguse kohaselt loetakse maksetehing üldjuhul autoriseerituks, kui see on kinnitatud isikustatud turvaelementide, näiteks PIN-koodide abil. Autor märgib, et selline käsitlus ei ole praktikas absoluutne, kuivõrd kohtupraktika analüüs näitas, et ka autoriseerituse hindamisel analüüsitakse sisuliselt, millistel asjaoludel autentimisandmeid kasutati ning kas klient sattus pettuse ohvriks ilma tahtluse või raske hooletuseta. Absoluutne lähenemine, mille kohaselt iga PIN2 kinnitusega tehing loetakse automaatselt autoriseerituks, ei tagaks piisavat tarbijakaitset. Samas tuleb arvestada ka vastupidise riskiga: kui käsitleda laialdaselt kõiki pettuse tunnustega tehinguid autoriseerimata tehingutena, võib see soodustada kuritarvitusi klientide poolt, kes võivad pahatahtlikult viidata pettusele eesmärgiga saada finantsasutuselt hüvitist. Seetõttu on vajalik iga juhtumi individuaalne ja sisuline hindamine, võttes arvesse nii kliendi kui ka makseteenuse pakkuja käitumist. Kavandatav regulatsioon ei välista seejuures kehtiva süsteemi säilimist, mille kohaselt vastutab makseteenuse pakkuja autoriseerimata tehingute

⁸¹ Äripäev. Pangad peavad hakkama kelmide ohvritele kahjusid hüvitama. - <https://www.raamatupidaja.ee/raadio/episood/pangad-peavad-hakkama-kelmide-ohvritele-kahjusid-huvitama> (12.12.2025; saade).

eest, kuid laiendab vastutust ka juhtudele, kus klient on küll tehingu tehniliselt kinnitanud, kuid teinud seda pettuse mõjul⁸². Selline lähenemine toob esile finantsasutuste hoolsusnõuete olulisuse, kuna eeldab, et makseteenuse pakkujad arendavad oma kontrollmehhanisme ja riskituvastussüsteeme viisil, mis võimaldaks pettusi paremini ennetada ja tuvastada, mida on rõhutanud nii Rahandusministeeriumi esindaja kui ka käesoleva töö autor. Eeltoodu kinnitab, et finantsasutuse roll ei piirdu üksnes maksete tehnilise vahendamisega, vaid hõlmab ka aktiivset kohustust rakendada tõhusaid meetmeid pettuste ennetamiseks ja klientide kaitsmiseks. Kavandatav Euroopa Liidu määrus näeb ette, et makseteenuse pakkujad peavad arendama oma kontrollmehhanisme ja riskituvastussüsteeme, et pettusi paremini ennetada ja tuvastada⁸³. Sellest tulenevalt ei saa kohtu tasandil jätkata vaid formaalse vastutuse hindamisega, näiteks autoriseerimata tehingu hüvitamisega võlaõiguse alusel, ilma et hinnataks, kas finantsasutus on täitnud oma hoolsusnõuded ja rakendanud efektiivseid ennetusmeetmeid. Kui kontrollmehhanisme ei ole arendatud ega rakendatud, jääb finantsasutuse tegevus ühelt poolt rahaliselt vastutavaks, kuid tegelikult võib see viia olukorrani, kus pettusi ei takistata ja klientidele ei tagata piisavat kaitset.

Artikkel Tarbijakrediidilepingute sõlmimisega seotud aktuaalsed probleemid kinnitab, et praeguse Eesti seadusandluse ja kohtupraktika järgi lasub tarbijal suur tõendamiskoormus, kui tema nimel on sõlmitud tarbimislaen ilma tema teadliku nõusolekuta.⁸⁴ Kuigi artikkel keskendub tarbijakrediidilepingute sõlmimisele pettuse mõjul, on seal käsitletud e-ID kasutamise küsimus olulise tähendusega ka maksepettuse kontekstis, kuna see mõjutab otseselt finantsasutuse võimalikku vastutust. Norra tarbijakrediidilepingute seadus (Lov om finansavtaler, 2023) näeb aga ette, et vaidluse korral peab krediidiandja tõendama, et tarbija oli tehingust teadlik ning piirab tarbija vastutust juhtumites, kus petturid on kasutanud tema eID-d: tavaliselt maksimaalselt 450 Norra krooni (ca 40 eurot), raskelt hooletu tarbija puhul 12 000 Norra krooni (ca 1000 eurot) ja ainult tahtliku rikkumise korral kogu võlgnetav summa.⁸⁵ Autori hinnangul näitab Norra lähenemine, et tõendamiskoormuse panemine krediidiandjale ja tarbija vastutuse piiramine suurendab tarbijate kaitset ning vähendab ebaproportsionaalset koormust. Eesti praktikas jääb tarbijale seevastu endiselt keeruliseks tõestada, et tehing oli autoriseerimata. Norra õiguses on autoriseerimata maksetehingute regulatsioon sarnane Eesti õigusega selles osas, et makseteenuse osutaja on kohustatud kliendi konto taastama. Siiski näeb Norra finantslepingute seadus (*Finansavtaleloven*) § 4-32 ette

⁸² Äripäev. Pangad peavad hakkama kelmide ohvritele kahjusid hüvitama (viide 81).

⁸³ *Ibid.*

⁸⁴ Riigikogu Toimetised. Info on võim. Infomanipulatsioonide ja hübriidsõja tundmine annab võimu, et tulla toime inforuumis, mis on kiires muutumises ja pidevas määramatuses. - RiTo 51/2025. - <https://rito.riigikogu.ee/wordpress/wp-content/uploads/2025/06/RiTo-51.pdf> (2025).

⁸⁵ *Ibid.*

oluliselt rangema tagastamiskohustuse, kohustades teenuseosutajat tegema tagasimakse viivitamata ja hiljemalt järgmisel tööpäeval. Lisaks on Norra õiguses sõnaselgelt sätestatud, et tõendamiskoormus lasub teenuseosutajal (§ 3-5 lg 2), mille kohaselt peab teenuseosutaja tõendama, et ta on täitnud kõik seadusest ja määrustest tulenevad kohustused.⁸⁶ Praktikas tähendab see muu hulgas ka seda, et teenuseosutaja peab vaidluse korral tõendama maksetehingu nõuetekohase autentimise ning vajaduse korral kliendi tahtluse või raske hooletuse. Samuti nagu eelnevalt viidatud, on tarbija vastutus piiratud konkreetsete rahaliste ülemmääradega makseinstrumendi kaotamise, varguse ja raske hooletuse korral. Selline regulatsioon tugevdab tarbijakaitset, kuna finantsasutus on kohustatud kahju esmalt hüvitama ning saab vastutusest vabaneda üksnes juhul, kui ta suudab tõendada kliendi tahtlust või rasket hooletust. Seetõttu võiks Norra mudelit pidada eeskujuks Eesti õigusele, kuna see soodustab finantsasutuste kontrollmehhanismide tõhusamat rakendamist ning vähendab tarbijale langevat ebamõistlikku tõendamiskoormust.

Kohtupraktikas tuleks autori hinnangul pettusejuhtumite hindamisel pöörata suuremat tähelepanu tehingu teostamise üksikasjade põhjalikule analüüsile, et tagada õiglasem ja sisuliselt täpsem otsustamine. Konkreetsete asjaolude analüüs annaks võimaluse hinnata, millistel tingimustel tehing üldse toimus ning kas klient oli tegelikult kaitstud panga poolt rakendatud kontroll- ja turvamehhanismidega. Näiteks näeb autor vajalikuks arvestada, kas pank kasutas riskipõhiseid süsteeme, mis analüüsivad tavapärasest kliendi käitumist kontrol, tuvastavad ebatavalisi tehinguid ja kontrollivad selle juures ka e-ID sertifikaati andmeid, tehes kindlaks selle jaoks kasutatavat seadet ning kas selliste süsteemide rakendamine oleks võimaldanud ennetada pettust või vähendada kahju. Samuti oleks oluline hinnata, kas pank tegutses aktiivselt, rakendades täiendavaid kinnitusi, piiranguid, turvameetmeid või kas puudus igasugune reageerimine tehingule, mis andis petturitele võimaluse raha ebaseaduslikult üle kanda. Selline detailne hindamine võib olla aluseks ka karistusõigusliku vastutuse hindamiseks. Nimelt, võib sellisel juhul tekkida alus kaaluda karistusõiguslikku vastutust KarS § 217² lg 1 alt 2 raames, kuna finantsasutus ei oleks oma kohustusi täitnud ja pettuse tekkimine ei ole üksnes kliendi eksimus või hooletus, vaid osaliselt ka pankade kontrolli puudumise tagajärg.

Oluliseks arengusuunaks on muuhulgas ka riskigruppidega tõhusam koostöö ja pettuseskeemides teadlikkuse tõstmine. Olukorras, kus suurem osa inimesi oleks piisavalt informeeritud petturite lemmik skeemidest ja sellest, millistes olukordades neile meeldib

⁸⁶ Lov om finansavtaler (Finansavtaleloven). - LOV-2020-12-18-146. Justis- og beredskapsdepartementet 2020. - https://lovdata.no/dokument/NL/lov/2020-12-18-146/KAPITTEL_1-2#KAPITTEL_1-2

tegutseda, muutuks petturite tegevus palju raskemaks⁸⁷. Citadele panga uuring näitab, et pettustega kokku puutunud inimeste seas oli suurima osa just 60-74-aastaste vanuserühmas, kes arvasid, et nad pole pettustega kokku puutunud, mis viitab pigem sellele, et vanemaealised võivad olla pettuste suhtes haavatavamad või vähem teadlikud nende äratundmisest. Kuigi pangad kasutavad nutikaid maksete jälgimise süsteeme ja blokeerivad kahtlased tehingud, muudavad petturid ka pidevalt oma meetodeid, et kätte saada ohvri andmed või raha.⁸⁸ See viitab, et vanemaealised kliendid võivad olla pettuste suhtes haavatavamad ning vähem suutlikud nende äratundmiseks. Sellised tähelepanekud annavad finantsasutusele põhjuse kaaluda oma kontrollimehhanismide riskipõhist suunamist. Näiteks, võib olla mõistlik keskenduda täiendavate turvameetmete rakendamisele klientide segmentides, kus risk pettuse ohvriks sattumiseks on suurem, sealhulgas vanemaealiste klientide puhul. Praktikas tähendab see, et finantsasutus võiks ja ka peaks temal lastuvatest hoolsuskohustusest tulenevalt arendama süsteeme, mis analüüsivad kliendi tavapärast kontokäitumist ja raha kasutamise harjumusi ning tuvastavad ebatavalised tehingud, mis erinevad tavapärasest käitumismustrist. Autori hinnangul, tänapäeval on Eestis kasutusel enam-vähem sarnased pettuseskeemid ning neid rakendatakse teatud inimeste gruppide suhtes. See omakorda tähendab aga seda, et finantsasutustel on ammendavaid võimalusi rakendamaks meetmeid, mis aitaksid kaasa pettuste ära hoidmisele ning minimeerida kahju ulatust, mida tekitatakse makseteenuslepingute klientidele.

Riigi Infosüsteemi Amet (RIA) on 2026. aastal võtnud kasutusele riigi e-teenusele sisselogimisel Smart-ID+. RIA elektroonilise identiteedi osakonna juhi Anna Õuekallase sõnul on Smart-ID+ üks sammudest, millega riik ennetab üha keerukamaks muutuvaid pettuskeeme, lisades autentimisprotsessi täiendava kaitsekihi. Smart-ID+ aitab paremini ennetada sotsiaalse manipulatsiooni ja telefonipettuste riske, säilitades samal ajal kasutajatele tuttava ja mugava kasutuskogemuse. Smart-ID+ versiooni loodi just organisatsioonide jaoks, kes peavad toime tulema kasvavate pettuseriskide, rangemate turvanõuete ja kasutajate ootusega lihtsa, kuid turvalise teenuse järele.⁸⁹ Smart-ID+ pakub kahte sisselogimismeetodit, millest esimene on e-teenuse sisselogimise lehel dünaamiliselt muutuva QR-koodi skaneerimise kaudu Smart-ID'ga. Teine on aga rakendustevahelise suhtluse kaudu - seadmes, milles on Smart-ID rakendus, avaneb Smart-ID automaatselt ja seejärel saab oma toimingut kinnitada PIN-koodiga. Mõlema sisselogimismeetodi puhul ei pea sisestama oma isikukoodi.

⁸⁷ Citadele Bank. Uuring: üle 70 protsendi eestlastest on kokku puutunud finantspettuse katsetega. - <https://www.cblgroup.com/et/media/press-releases/2023/financial-fraud/> (15.03.2023).

⁸⁸ *Ibid.*

⁸⁹ Smart-ID+. Turvalisemad tehingud. Rohkem kontrolli kasutajale. - <https://www.smart-id.com/et/smart-id-plus/> (08.04.2026).

See uuendus tagab paremini, et õngitsus- ja sotsiaalse manipuleerimise rünnakud peatatakse enne, kui need jõuavad mõju avaldada.⁹⁰ Kuigi hetkeseisuga ei ole Smart-ID+ finantsasutustel rakendusel ei äppide, kus on aga võimalus kasutada biomeetriat, ega brauseri kaudu internetipanka sisselogimisel, oleks Smart-ID+ rakenduse laiem kasutuselevõtt koosmõjus finantsasutuste poolt riskirühmade tõhusama informeerimise ning kontrollmehanismide parema ja tõhusama rakendamisega aidanud oluliselt vähendada Eestis toimepandavaid petukõnesid.

⁹⁰ Smart-ID. Riigi autentimisteenuses võetakse kasutusele uus Smart-ID+ (30.01.2026). - <https://www.smart-id.com/et/riigi-autentimisteenuses-voetakse-kasutusele-uus-smart-id/> (08.04.2026).

Kokkuvõte

Käesoleva magistritöö eesmärgiks oli analüüsida, kas ja millistel tingimustel võib finantsasutus kanda karistusõiguslikku vastutust pettuse mõjul sooritatud tehingu eest olukorras, kus tehing on formaalselt kliendi poolt algatatud ja nõuetekohaselt autoriseeritud. Magistritöö raames keskendus autor küsimusele, millises ulatuses võivad finantsasutuse hoolsusnõuete rikkumised maksepettuste kontekstis olla käsitletatavad mitte üksnes võlaõiguslike rikkumistena, vaid ka karistusõiguslikku vastutust kaasa toova käitumisena.

Töös püstitatud hüpoteesist lähtudes uuriti, kas finantsasutuse hoolsusnõuete täitmata jätmine või rikkumine võib teatud tingimustel kaasa tuua karistusõigusliku vastutuse, eelkõige usalduse kuritarvitamise koosseisu kontekstis ehk KarS § 217² alusel. Selleks analüüsiti finantsasutustele kehtivaid hoolsusnõudeid, nende eesmärki ning seost maksepettuste ennetamisega. Samuti analüüsis autor Euroopa Liidu liikmesriikide ja Eesti kohtupraktikat, et hinnata, milliseid asjaolusid kohtud peavad pettusejuhtumite lahendamisel määravaks ning millistele kriteeriumidele tuginedes kujundatakse vastutuse jaotus makseteenuse pakkuja ja kliendi vahel. Eelkõige keskenduti sellele, kuidas eristatakse autoriseeritud ja autoriseerimata tehinguid ning millisel viisil hinnatakse kliendi võimalikku süüd, sealhulgas tahtlust ja rasket hooletust. Lisaks selgitati, milliseid hoolsus- ja tõendamiskohustusi on kohtud pidanud oluliseks makseteenuse pakkuja tegevuse hindamisel ning millistest õigusraamistikest, sealhulgas siseriikliku õiguse normidest, vastutuse määramisel lähtutakse.

Analüüsi tulemusena selgus, et finantsasutuste vastutus makseteenuse osutamisel on makseteenuse õiguses selgelt ja ammendavalt reguleeritud ning üles ehitatud selgele riskijaotusele makseteenuse pakkuja ja kasutaja vahel. PSD2 direktiiv näeb ette, et autoriseeritud tehingute puhul lasub tõendamiskoormus makseteenuse pakkujal, kes peab suutma tõendada tehingu nõuetekohast autentimist, korrektset dokumenteerimist ning kliendi nõusoleku olemasolu. Kui need tingimused on täidetud, ei kaasne makseteenuse pakkujale üldjuhul tsiviilõiguslikku vastutust ka juhul, kui tehingu taga on kliendi mõjutamine petturi poolt. Autoriseerimata tehingute puhul on regulatsioon vastupidine: makseteenuse pakkujal lasub kohustus tehing viivitamata hüvitada ning taastada kliendi konto olukord, mis oleks olnud ilma autentimise kohustuse rikkumiseta. Samuti on selgelt piiratud kliendi vastutus, mis tekib üksnes erandjuhtudel, eelkõige tahtluse või raske hooletuse korral. Seega on tsiviilõiguslik vastutussüsteem üles ehitatud selgele hüvitamise mehhanismile, mis jaotab riski eelkõige makseteenuse pakkuja ja kliendi vahel selliselt, et autoriseerimata tehingute puhul kannab esmast kahju riski makseteenuse pakkuja. Kohtupraktika analüüs kinnitas samuti, et vastutuse jaotus makseteenuse pakkuja ja kliendi vahel on suures osas ühtselt määratletud

PSD2 direktiivist tulenevate põhimõtete alusel ning liikmesriikide kohtud lähtuvad selle kohaldamisel valdavalt samadest alusreeglitest. Eelkõige järgivad kohtud selget eristust autoriseeritud ja autoriseerimata tehingute vahel ning sellest tulenevat riskijaotust, kus autoriseerimata tehingute puhul lasub esmane kahju hüvitamise kohustus makseteenuse pakkujal. Samuti kinnitab kohtupraktika, et kliendi vastutus piirdub eelkõige juhtumitega, kus esineb tahtlus või raske hooletus ning vastutuse hindamisel on keskse tähtsusega autentimisprotsessi ja maksejuhise andmise asjaolude kontroll.

Eesti õigusraamistiku analüüs näitas, et PSD2 direktiiv on Eesti õigusse üle võetud ning eelnimetatud vastutuse jaotust makseteenuse pakkuja ja kasutaja vahel autoriseerimata ja autoriseeritud tehingu puhul reguleerivad VÕS sätted. Finantsasutuste kohustuse kaitsta kliendi vara toetab muuhulgas ka MERAS § 114, mis näeb ühtlasi rikkumise korral ette rahalise trahvi või rikkumisest saadud kasu hüvitamise. Karistusõigusliku analüüsi keskmes olnud KarS § 217² koosseisu osas järeldub, et finantsasutuse tegevus makseteenuse osutamisel ei vasta üldjuhul usalduse kuritarvitamise koosseisu tunnustele. Esiteks puudub finantsasutusel maksepettuste tüüpolukordades vara käsutamise või varaliste huvide otsese kuritarvitamise olukord KarS § 217² lg 1 alt 1 mõttes. Seda põhjusel, et petukõnede ja sarnaste skeemide puhul toimub enamasti maksetehing kliendi enda poolt läbi viidud autoriseerimise alusel, kus klient läbib tugeva autentimise ning annab maksejuhise ise, isegi kui ta on pettuse mõjul eksinud. Sellisel juhul ei ole finantsasutuse tegevus käsitletav hoolsuskohustuse rikkumisena, kuna ta täidab seadusest tulenevaid autentimise ja kontrollikohustusi nõuetekohaselt. Seega jääb risk sellistes olukordades kliendi enda vastutusse ning ei saa tekkida finantsasutusel ei tsiviilõiguslikku ega karistusõiguslikku vastutust. Teiseks, isegi usaldusseisundi KarS § 217² lg 1 alt 2 tähenduses rakendamine ei pruugi finantspettuste puhul õnnestuda ning on vaja üksikjuhtumit väga hoolsalt analüüsida. Nimelt, kuigi finantsasutuse vastutus võib kõne alla tulla *vishing*'u ehk õngitsuskõnede juhtumite puhul, kus pettur saab ligipääsu kliendi andmetele ja teostab tehinguid kliendi nimel, jääb finantsasutuse vastutus sõltuvaks varalise kahju suurusest ja subjektiivse koosseisu täidetusest. Kuid oluline on hinnata ka asjaolusid, mis puudutavad finantsasutuse poolt riskihindamise, autentimise ja turvameetmete kohustuste täitmist. Kuigi teoreetiliselt võib nendes olukordades tõusetuda küsimus hoolsuskohustuse rikkumisest, ei pruugi see praktikas viia siiski KarS § 217² lg 1 alt 2 kohaldamiseni, kuna suurema tõenäosusega puudu jääb subjektiivses koosseisus nõutud tahtlus. Subjektiivse koosseisu või suure varalise kahju lävendi mitte ületamisel vastutab finantsasutus aga MERAS § 113 lg 2 alusel. Teisisõnu on finantsasutuse hoolsuskohustused juba detailselt reguleeritud tsiviilõiguslikes normides, mis määratlevad selgelt nii kohustuste sisu kui ka nende rikkumise tagajärjed. Kuid teatud

pettuskeemide puhul võib olla põhjendatud hinnata ka finantsasutuse tegevuse subsummeerimist KarS § 217² lg 1 alt-s 2 sätestatud kuriteo alla.

Samas, *de lege ferenda* tasandil ilmnes siiski, et Euroopa Liidu õiguse arengusuunad liiguvad makseteenuse pakkuja vastutuse teatud ulatusliku laiendamise suunas, eelkõige juhtumites, kus pettus on seotud finantsasutuse identiteedi kuritarvitamisega. Samal ajal jääb kehtima põhimõte, et vastutus ei ole absoluutne ning sõltub kliendi käitumisest, sealhulgas tema hooletusest või tahtlusest. Autor rõhutab, et kohtupraktika arendamise kontekstis oleks põhjendatud suurem tähelepanu finantsasutuse kontrollimehhanismide ja turvameetmete rakendamise sisulisele hindamisele, mitte üksnes tehingu formaalsele autoriseeritusele. See võimaldaks hinnata, kas pettuse ärahoidmine oleks olnud mõistlikult võimalik ning kas finantsasutuse tegevusel või tegevusetusel oli põhjuslik seos kahju tekkimisega. Selline lähenemine suurendaks vastutuse sisulist põhjendatust, kuid ei too siiski kaasa vajadust karistusõigusliku vastutuse laiendamiseks.

Eeltoodust tulenevalt kinnitab töö tervikuna, et finantsasutuse vastutus maksepettuste kontekstis on praegu ammendavalt reguleeritud tsiviilõiguslike ja väärteoõiguslike normidega, mis määravad nii vastutuse ulatuse kui ka selle piirid. Karistusõiguslik sekkumine KarS § 217² lg 1 alt 1 alusel ei ole nende juhtumite lahendamisel põhjendatud, kuna puudub vastava koosseisu täitmiseks vajalik ärakasutamise seisund. KarS § 217² lg 1 alt 1 alusel vastutuse kaasnemiseks aga ei ületa suurema tõenäosusega võimalikud rikkumised karistusõigusliku vastutuse lävendit subjektiivses koosseisus, kuid finantsasutuse vastutus kaasneb sellisel juhul MERAS § 113 lg 2 alusel.

SUMMARY: The Possibility of Criminal Liability of a Financial Institution for a Transaction Executed Through Fraud

The aim of this Master's thesis was to analyse whether, and under what conditions, a financial institution may incur criminal liability for a transaction executed under the influence of fraud in a situation where the transaction has been formally initiated and duly authorised by the customer. Within the framework of the thesis, the author focused on the question of to what extent breaches of a financial institution's duty of care in the context of payment fraud may be regarded not only as breaches under the law of obligations, but also as conduct giving rise to criminal liability.

The relevance of this master's thesis topic lies in the significant and continuous increase in payment fraud, which is closely linked to the widespread adoption of electronic payments and digital banking. Based on statistical overviews derived from various reliable sources, both the number of fraud cases and the resulting financial losses have increased substantially in recent years, both in Estonia and across the European Union. This is not a matter of isolated incidents, but rather a systemic problem that significantly affects both individuals and businesses.

The growth of payment fraud is driven, on the one hand, by the speed and convenience of payment solutions, which reduce control mechanisms in the execution of transactions, and on the other hand, by increasingly sophisticated technological methods used to carry out fraudulent activities. Fraud often occurs in situations where the customer discloses authentication data to the fraudster or personally authorizes a transaction without being aware of its actual nature. In such cases, the transaction is formally treated as having been initiated by the customer, raising questions about the allocation of liability between the customer and the financial institution.

The problem is further exacerbated by the fact that the perpetrator of the fraud often remains unidentified, making it difficult for victims to claim compensation for damages. This, in turn, raises questions about the role and responsibility of financial institutions in preventing fraud and protecting customers. The increasing volume of fraud and the associated risks have also brought the issue to the forefront of political and regulatory attention, highlighting the need for more effective prevention and intervention mechanisms.

In light of the above, the relevance of this master's thesis topic lies in the need to assess whether the existing legal framework is capable of adequately regulating liability in cases of transactions carried out under the influence of fraud, and whether the obligations of financial

institutions in preventing fraud are sufficiently clearly defined to ensure effective consumer protection and maintain trust in the financial system.

Based on the hypothesis formulated in the thesis, the author examined whether a failure to comply with or a breach of the financial institution's duty of care may, under certain conditions, result in criminal liability, in particular in the context of the offence of abuse of trust pursuant to § 217² of the Penal Code. For this purpose, the duties of care applicable to financial institutions, their objectives, and their connection to the prevention of payment fraud were analysed. The author also examined the case law of the Member States of the European Union and Estonia in order to assess which circumstances courts consider decisive when resolving fraud cases and on the basis of which criteria liability is allocated between the payment service provider and the customer. Particular attention was paid to how authorised and unauthorised payment transactions are distinguished and how the customer's potential fault, including intent and gross negligence, is assessed. In addition, the thesis clarifies which duties of care and burden of proof obligations courts have considered relevant when assessing the conduct of a payment service provider, as well as the legal frameworks, including provisions of national law, that are relied upon in determining liability.

The analysis shows that the liability of financial institutions in the provision of payment services is clearly and exhaustively regulated under payment services law and is structured around a clear allocation of risk between the payment service provider and the payment service user. The activities of financial institutions, including payment service providers, in the European Union are regulated by Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (The PSD2 Directive), the objective of which is to ensure the functioning of a unified and secure market for payment services. With regard to due diligence requirements, the author analysed the obligation of user authentication and the obligation to manage operational risk and implement security measures, as the author identified potential grounds for the application of criminal liability in the breach of these obligations. It is important to distinguish between the general authentication requirement and the requirement for strong customer authentication. PSD2 establishes a general authentication obligation for all payments; however, in the author's view, it is the implementation of strong customer authentication that enables the assessment of whether a financial institution has fulfilled its risk-based duty of care and allows the identification of situations where the risk of fraud is higher. Based on the analysis conducted in this master's thesis, it can be concluded that a payment transaction is considered authorised only if the payer has given consent to its execution. In the absence of such consent,

the transaction is treated as an unauthorised payment transaction. When analysing a fraud case and determining liability for the damage incurred by a payment service user, it is first necessary to establish whether the transaction was authorised or unauthorised. The purpose of strong customer authentication is to verify whether the person initiating the transaction is indeed the payment service user. Strong customer authentication must be based on at least two independent authentication elements from three categories: knowledge (e.g. a password or PIN), possession (e.g. a physical device or authentication token), and inherence, i.e. something inherent to the user, such as a biometric identifier. In the author's assessment, strong customer authentication does not function as a sufficiently effective protective measure. The rapid increase in payment fraud demonstrates that fraudsters are able to manipulate individuals so skilfully that customers may approve transactions without fully understanding their actual nature or the details presented to them. Consequently, such transactions are formally considered validly authorised, despite the underlying deception. In the author's view, in such situations, customer confirmation should provide a real-time signal to the payment service provider, enabling the assessment of transaction risk and, where necessary, the application of additional security measures, such as suspending the transaction and requesting further confirmation. Accordingly, the authentication obligation is closely linked to the obligation to manage operational risk and implement security measures, as the information obtained during authentication forms the basis for risk assessment and the application of further protective mechanisms. Operational risk management ensures security measures function systematically. By identifying high-risk transactions, the bank can apply additional controls in real-time, prior to execution. The author concludes that, in resolving fraud cases and determining liability, it is essential to establish the nature of the transaction-whether it was authorised or unauthorised-and to assess whether and which additional security measures the financial institution has implemented to detect and/or prevent fraud.

As a result of the analysis conducted in this master's thesis, the author found that civil liability in cases of authorised and unauthorised transactions is clearly defined within the regulatory framework. The PSD2 Directive provides that, in the case of authorised transactions, the burden of proof lies with the payment service provider, who must be able to demonstrate that the transaction was properly authenticated, accurately recorded, and not affected by a technical breakdown, and that the payer gave consent. Where these conditions are met, the payment service provider generally does not incur civil liability, even if the transaction results from the customer being manipulated by a fraudster. In the case of unauthorised transactions, the regulation operates inversely: the payment service provider is obliged to immediately

refund the amount of the unauthorised transaction and restore the payment account to the state in which it would have been had the transaction not occurred. The customer's liability is also clearly limited and arises only in exceptional cases, in particular in cases of intent or gross negligence. Consequently, the civil liability framework establishes a defined mechanism for risk allocation, ensuring that the primary burden of loss arising from unauthorized transactions is borne by the payment service provider. The analysis of case law likewise confirms that the allocation of liability between the payment service provider and the customer is uniformly determined on the basis of principles derived from the PSD2 Directive, and that the courts of Member States generally rely on the same fundamental rules in its application. In particular, courts follow a clear distinction between authorised and unauthorised transactions and the resulting allocation of risk, according to which the primary obligation to compensate for loss in the case of unauthorised transactions lies with the payment service provider. Case law also confirms that the customer's liability is primarily limited to situations involving intent or gross negligence, and that the assessment of liability focuses on the authentication process and the circumstances in which the payment order was given.

The analysis of the Estonian legal framework demonstrated that the PSD2 Directive has been transposed into Estonian law and that the aforementioned allocation of liability between the payment service provider and the customer, in the case of authorised and unauthorised transactions, is regulated by the Law of Obligations Act. The obligation of financial institutions to safeguard customer funds is also supported, inter alia, by § 114 of the Payment Institutions and E-money Institutions Act, which provides for a pecuniary penalty or the disgorgement of unlawful gains in the event of a breach. With regard to the elements of the offence under § 217² of the Penal Code, which formed the focus of the criminal law analysis, it can be concluded that the conduct of a financial institution in the provision of payment services generally does not meet the criteria of abuse of trust. First, in typical payment fraud scenarios, there is no situation involving the direct misuse of the right to dispose of property or of proprietary interests within the meaning of § 217² clause 1 section 1 of the Penal Code. This is because, in case of scam calls and similar schemes, the payment transaction is typically carried out on the basis of authorisation performed by the customer themselves, where the customer undergoes strong customer authentication and submits the payment order personally, even if they have been misled by fraud. In such cases, the conduct of the financial institution cannot be regarded as a breach of its duty of care, as it fulfils its statutory authentication and control obligations properly. Consequently, the risk in such situations remains with the customer and does not give rise to either civil or criminal liability on the part

of the financial institution. Second, even the application of a position of trust within the meaning of § 217² clause 1 section 2 of the Penal Code may not be successful in cases of financial fraud and requires careful case-by-case analysis. Although liability of a financial institution may be considered in cases of vishing (voice phishing), where a fraudster gains access to a customer's data and executes transactions in the customer's name. Liability for the financial institution is conditional upon the magnitude of the pecuniary damage and the demonstrable presence of the essential subjective elements, such as intent or gross negligence. It is also necessary to assess circumstances relating to the financial institution's fulfilment of its obligations regarding risk assessment, authentication, and security measures. Although, in theory, such situations may raise questions about a breach of the duty of care, in practice this may still not lead to the application of § 217² clause 1 section 2 of the Penal Code, as the required intent within the subjective elements of the offence will most likely be lacking. Where the subjective elements or the threshold for significant pecuniary damage are not met, the financial institution is instead liable under § 113 clause 2 of the Payment Institutions and E-money Institutions Acts. In other words, the duties of care of financial institutions are already regulated in detail under civil law provisions, which clearly define the duties and the consequences of their breach. However, in certain fraud schemes, it may still be justified to assess whether the conduct of a financial institution could be subsumed under the offence set out in § 217² clause 1 section 2 of the Penal Code.

At the same time, at the level of *de lege ferenda*, it appears that developments in European Union law are moving towards a certain expansion of the liability of payment service providers, particularly in cases where the fraud involves the misuse of the identity of the financial institution. At the same time, the principle remains that liability is not absolute and depends on the conduct of the customer, assessing their negligence or intent. The author emphasises that the evolution of case law necessitates a greater focus on the substantive assessment of the control mechanisms and security measures implemented by financial institutions, rather than focusing solely on the formal authorisation of the transaction. This would facilitate the assessment of whether the fraud could have been reasonably prevented and whether there is a causal link between the actions or omissions of the financial institution and the damage incurred. Such an approach would increase the substantive justification of liability, but would not, however, necessitate the expansion of criminal liability.

In conclusion, the thesis as a whole confirms that the liability of financial institutions in the context of payment fraud is currently exhaustively regulated by civil law and misdemeanour law provisions, which define both the scope and the limits of liability. Criminal law

intervention under § 217² clause 1 section 1 of the Penal Code is not justified in resolving such cases, as the required element of exploitation is absent. Likewise, potential breaches are unlikely to exceed the threshold of criminal liability under § 217² clause 1 section 2 due to the lack of the required subjective elements; however, in such cases, the financial institution may incur liability under § 113 clause 2 of the Payment Institutions and E-money Institutions Act.

KASUTATUD MATERJALIDE LOETELU

Kasutatud normatiivmaterjalid ja kommenteeritud väljaanded

1. Karistusseadustik. - RT I, 22.12.2025, 2.
2. Makseasutuste ja e-raha asutuste seadus. - RT I, 13.02.2026, 9.
3. Maksejuhiste aktsepteerimise tingimused. - RTL 2010, 25, 446
4. Rahapesu ja terrorismi rahastamise tõkestamise seadus. - RT I, 14.03.2025, 23.
5. Sootak, J., Pikamäe, P. (koostajad). Karistusseadustik kommenteeritud väljaanne. Tallinn: Juura 2021, e-väljaanne.
6. Võlaõigusseadus. - RT I, 11.11.2025, 16.
7. 25. novembri 2015. aasta Euroopa Parlamendi ja nõukogu direktiiv 2015/2366 makseteenuste kohta siseturul (PSD2). - ELT L 337, 23.12.2015
8. 27. novembri 2017. aasta komisjoni delegeeritud määrus 2018/389, millega täiendatakse EL-i 2015/2366 regulatiivsete tehniliste standarditega, mis käsitlevad kliendi tugevat autentimist ning ühiseid ja turvalisi teabevahetuse avatud standardeid (RTS). - ELT L 69

Kasutatud välisriigi normatiivmaterjalid

9. Lov om finansavtaler (Finansavtaleloven). - LOV-2020-12-18-146. Justis- og beredskapsdepartementet 2020. -
https://lovdata.no/dokument/NL/lov/2020-12-18-146/KAPITTEL_1-2#KAPITTEL_1-2 (Norra finantslepingute seadus).

Kasutatud kirjandus

10. Citadele Bank. Uuring: üle 70 protsendi eestlastest on kokku puutunud finantspettuse katsetega. - <https://www.cblgroup.com/et/media/press-releases/2023/financial-fraud/> (15.03.2023).
11. Elisa Eesti. (30.10.2025). Uue Smart-ID loomisega seotud pettused põhjustavad miljonikahjusid - inimesed ei teadvusta ohumärke. -
<https://www.elisa.ee/et/uudised/uue-smart-id-loomisega-seotud-pettused-pohjustavad-miljonikahjusid-inimesed-ei-teadvusta> (08.04.2026).
12. Finantsinspektsioon. Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks. 26.11.2018. -
https://www.fi.ee/sites/default/files/2018-11/FI_AML_Soovituslik_juhend.pdf (14.03.2026).

13. Finantsinspeksioon. Nõuded operatsiooniriski juhtimise korraldamiseks. 18.05.2005.
- https://www.fi.ee/failid/20050518_juh_Nouded_OR_juhtimise_korraldamiseks.pdf
(16.03.2026).
14. Justiits- ja Digiministeerium. (2024). Kuritegevus Eestis 2024: Kelmused. -
<https://www.justdigi.ee/kuritegevus2024/kelmused.html> (25.03.2026).
15. Kairjak, M., Sootak, J. Varavastased süüteod. Tallinn: Juura 2017.
16. Kalamees, P. „Näita käppa“ ehk minu digiallkiri, järelkult minu tehtud tehing. -
2024/9-10. -
https://juridica.ee/article_full.php?uri=2024_9-10_n_ita_k_ppa_ehk_minu_digiallkiri_j_relikult_minu_tehtud_tehing
17. Luminor kontolepingu tingimused. -
<https://luminor.ee/s3fs-public/documents/luminori-kontotingimused.pdf> (15.03.2026).
18. Maksekeskkonna Foorumil otsiti lahendusi maksepettuste tõkestamiseks. - Eesti
Pangaliit 16.01.2025
<https://pangaliit.ee/uudised-ja-teated/maksekeskkonna-foorumil-otsiti-lahendusi-maksepettuste-tokestamiseks> (06.02.2026).
19. Maksepettuste ülevaade 2025. Eesti Pank; Eesti Pangaliit; Politsei- ja Piirivalveamet
2025. -
https://haldus.eestipank.ee/sites/default/files/2025-12/ep_maksepettuste-ulevaade-2025_0.pdf (06.02.2026).
20. P. Pikamäe. Mõningad kelmuse üldkoosseisu sisustamisprobleemid kohtupraktikas. -
Juridica 2011/2.
21. Petukõned. Riigi Infosüsteemi Amet. -
<https://www.itvaatlik.ee/levinud-pettused/petukoned/> (10.02.2026).
22. Postimees Majandus. (12.12.2025). Bigbank: pettustele piiri panemiseks tuleb
Smart-ID loomise protseduur ümber teha-
<https://majandus.postimees.ee/8378672/bigbank-pettustele-piiri-panemiseks-tuleb-smart-id-loomise-protseduur-umber-teha> (08.04.2026).
23. Reurink, A. (2016). Financial Fraud: A Literature Review. MPIfG Discussion Paper
16/5, 47-49. -
https://www.researchgate.net/publication/303517861_Financial_Fraud_A_Literature_Review#pf33 (11.02.2026).
24. Riigikogu. (2026). Küberkuritegevuse ohjeldamine finantsvaldkonnas - olulise
tähtsusega riikliku küsimuse arutelu 19.02.2026. Istungi ülevaade. -

- <https://www.riigikogu.ee/istungi-ulevaated/riigikogu-arutas-olulise-riikliku-k-simusen-a-k-berkuritegevuse-ohjeldamist-finantsvaldkonnas/> (03.04.2026).
25. Riigikogu Toimetised. Info on võim. Infomanipulatsioonide ja hübriidsõja tundmine annab võimu, et tulla toime inforuumis, mis on kiires muutumises ja pidevas määramatuses. - RiTo 51/2025. -
<https://rito.riigikogu.ee/wordpress/wp-content/uploads/2025/06/RiTo-51.pdf> (2025).
26. Saarepuu, I., Leps, A. Ülevaade enamlevinud kelmuskuritegudest perioodil 2021-2024. Tallinn: Justiits- ja Digiministeeriumi kriminaalpoliitika osakond 2025. -
<https://www.justdigi.ee/sites/default/files/documents/2025-06/%C3%9Clevaade%20enamlevinud%20kelmuskuritegudest%20perioodil%202021%E2%80%932024.pdf> (02.02.2026).
27. SK ID Solutions AS, Kvalifitseeritud Smart-ID sertifikaatide kasutustingimused (alates 15.04.2024). -
<https://c.sk.ee/SK-TCU-QUALIFIED-SMART-ID-ET-CURRENT.pdf> (03.04.2026).
28. Smart-ID. Riigi autentimisteenuses võetakse kasutusele uus Smart-ID+ (30.01.2026). -
<https://www.smart-id.com/et/riigi-autentimisteenuses-voetakse-kasutusele-uus-smart-id/> (08.04.2026).
29. Smart-ID+. Turvalisemad tehingud. Rohkem kontrolli kasutajale. -
<https://www.smart-id.com/et/smart-id-plus/> (08.04.2026).
30. Tugev kliendituvastus (SCA) ja kuidas see mõjutab veebimakseid. - EveryPay tugikeskus, s.a. -
<https://support.every-pay.com/et/articles/11478038-tugev-kliendituvastus-sca> (03.03.2026).
31. Õigusteadlased: pangad peavad tarbijaid petturite eest paremini kaitsma. Novaator (ERR). -
<https://novaator.err.ee/1609754031/oigusteadlased-pangad-peavad-tarbijaid-petturite-eest-paremini-kaitsma> (25.07.2025).
32. Äripäev. Pangad peavad hakkama kelmide ohvritele kahjusid hüvitama. -
<https://www.raamatupidaja.ee/raadio/episood/pangad-peavad-hakkama-kelmide-ohvritele-kahjusid-huvitama> (12.12.2025; saade).

Kasutatud võõrkeelne kirjandus

33. Federal Bureau of Investigation (n.d.) Common frauds and scams. -
<https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams> (10.02.2026).

34. Finansiell ID-Teknik BID AB. Sustainability Report 2022. -
https://www.bankid.com/assets/files/Sustainability_report_BankID_2022.pdf
(20.03.2026).
35. Payment services deal: More protection from online fraud and hidden fees. European Parliament 27.11.2025. -
<https://www.europarl.europa.eu/news/en/press-room/20251121IPR31540/payment-services-deal-more-protection-from-online-fraud-and-hidden-fees> (08.02.2026).
36. Report on payment fraud 2025 (EBA/REP/2025/40). European Banking Authority; European Central Bank 2025. -
<https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202512.en.pdf>
(09.02.2026).
37. Seventh report on card fraud. European Central Bank (2021). -
<https://www.ecb.europa.eu/press/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html> (15.02.2026).
38. TIC. Secure Digital Identification - BankID. -
<https://tic.io/en/produkter-tjanster/bank-id> (20.03.2026).

Kasutatud kohtupraktika

Eesti Vabariigi kohtupraktika

39. RKKK 3-1-1-61-09.
40. RKTKm 2-23-11584.
41. TlnRnKo 2-24-1667.

Euroopa Kohtupraktika

42. EKo C-287/19, DenizBank AG versus Verein für Konsumenteninformation,
ECLI:EU:C:2020:897.

Välisriikide kohtupraktika

43. Cour de cassation (Chambre commerciale). 22-21.200.
<https://www.legifrance.gouv.fr/juri/id/JURITEXT000049385095> (27.03.2024).
44. Högsta domstolen. T 4623-21. 21.06.2022. -
<https://www.domstol.se/globalassets/filer/domstol/hogstodomstolen/avgoranden/engelska-oversattningar/t-4623-21-eng.pdf> (13.03.2026).
45. Stockholms tingsrätt. T 18737-23. 11.11.2024. Lahend on avaldamata, selle täistekst on autori valduses; lühikokkuvõte on kättesaadav veebilehel:

<https://www.domstol.se/nyheter/2024/11/dom-i-mal-om-en-banks-skyldigheter-vid-swishbedragerier/>.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Elizabeth Kirss,

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

“FINANTSASUTUSE KARISTUSÕIGUSLIKU VASTUTUSE VÕIMALIKKUS
PETTUSE MÕJUL SOORITATUD TEHINGU EEST”,

mille juhendaja on Priit Pikamäe,

reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada Tartu Ülikooli digitaalarhiivi kuni autoriõiguse kehtivuse lõppemiseni;

2. annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi kaudu Creative Commons'i litsentsiga CC BY NC ND 4.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni;
3. olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile;
4. kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Elizabeth Kirss

28.04.2026