TARTU ÜLIKOOL

ÕIGUSTEADUSKOND

Eraõiguse osakond

Elisabeth Okk

eID OMAJA VASTUTUS AUTORISEERIMATA MAKSE KORRAL

Magistritöö

Juhendaja

Ph.D. Piia Kalamees

Tallinn

2026

SISUKORD

SISSEJUHATUS

Autoriseerimata maksete regulatsioon kehtivas Eesti õiguses lähtub võlaõigusseaduse[1] (edaspidi VÕS) § 724[1] lg-s 1 ja makseteenuste direktiivi[2] (edaspidi PSD2) artikli 64 lõikes 1 sätestatud põhimõttest, et maksetehing on maksjale siduv üksnes juhul, kui maksja on andnud selle täitmiseks nõusoleku. Kuna Eesti makseteenuste regulatsioon põhineb Euroopa Liidu makseteenuste direktiivi ülevõtmisel, tuleb riigisiseseid sätteid autoriseerimise ja makseteenuse osapoolte vastutuse kohta võimaliku vastuolu korral tõlgendada võimalikult kooskõlas direktiiviga.[3] Juhul, kui maksetehing on tehtud ilma maksja nõusolekuta, on tegemist autoriseerimata maksega, mille puhul on makseteenuse pakkujal VÕS § 733[2] lõike 2 kohaselt kohustus maksetehingu summa maksjale viivitamata tagastada. Seega on maksja nõusolek autoriseerituse ja vastutuse jaotuse keskne lähtepunkt.

Käesoleva magistritöö kontekstis on oluline määratleda maksja roll makseteenuste regulatsioonis. VÕS § 709 lõike 5 kohaselt on maksja maksekonto omanik, kes annab maksejuhise konto debiteerimiseks. Käesolevas töös vastab sellele rollile eID omaja ehk isik, kelle nimel maksetehing algatatakse ja kelle eID-vahendeid tehingu kinnitamiseks kasutatakse.

Eestis, kus eID (ID-kaart, Mobiil-ID ja Smart-ID) igapäevane kasutamine makseteenustes on väga levinud, on kerkinud oluline õiguslik probleem, millel on otsene mõju vastutuse jaotusele maksja ja makseteenuse pakkuja vahel. Kui pettuse tulemusel kasutatakse maksja eID-d või sellega seotud autentimisvahendeid maksetehingu kinnitamiseks, võib makse olla tehniliselt korrektselt täidetud, kuid vaieldavaks jääb, kas makse väljendas maksja tegelikku ja teadlikku tahet konkreetne maksetehing teha. Kehtiv regulatsioon ei anna selget vastust küsimusele, kas sellisel juhul loetakse maksetehing autoriseerituks ning kes kannab tekkinud kahju - maksja, kes eID abil tehingut kinnitas, või makseteenuse pakkuja, kelle süsteemis makse täideti.

Käesoleva probleemi olemust ja ulatuslikku mõju illustreerivad ilmekalt Eesti meedias kajastatud elulised juhtumid, mis toovad esile kaks õiguslikult selgelt erinevat eID väärkasutamise stsenaariumit. Esimese variandi puhul autoriseerib maksetehingu eID omaja ise, tegutsedes näiteks pangapettuse ohvrina, arvates, et päästab oma raha ebatavaliste

[1] Võlaõigusseadus. - RT I, 11.11. 2025, 16.
[2] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/2366, 25. november 2015, makseteenuste kohta siseturul, direktiivide 2002/65/EÜ, 2009/110/EÜ ning 2013/36/EL ja määruse (EL) nr 1093/2010 muutmise ning direktiivi 2007/64/EÜ kehtetuks tunnistamise kohta. – ELT L 337, 23.12.2015, lk 19–127.
[3] Varul, P. jt (koost.). – Võlaõigusseadus IV. 8. osa 40. ptk – 10. osa (§-d 703–1067). Kommenteeritud väljaanne. Tallinn: Juura 2020, § 733² komm 3.1 (M. Ulp).

kaarditehingute eest.[4] Sellises olukorras sisestab isik ise PIN2-koodi ning kõne jooksul teeb pettur inimese kontolt ülekandeid.[5] Petukõnede tõttu kaotati 2025. aastal kelmidele lausa 11,5 miljonit eurot.[6] Teises, eelnevast õiguslikult selgelt erinevas stsenaariumis kinnitab tehingu ohvri teadmata pettur, kasutades selleks eID-d. See stsenaarium ilmneb mitmel kujul: pettur võib pääseda ohvri seadmesse kaughaldustarkvara abil, meelitada ohvrit sisestama autentimisandmeid võltsitud pangalehe kaudu või luua ohvri nimel uus eID, sidudes Smart-ID rakenduse ümber teise seadmega.[7] Nimetatud pettusjuhtumite puhul on tehingu tahteavalduse tegijaks pettur, mitte eID omaja. Viimast nimetatud varianti illustreerib 2025. aasta detsembris Politsei- ja Piirivalveameti registreeritud juhtum, kus kannatanu nimel loodi tema teadmata uus Smart-ID konto ning sooritati volitamata ülekandeid nii tema isikliku kui ka ettevõtte arveldusarvelt, tekitades kokku 73 000 euro suuruse kahju.[8]

Probleemi aktuaalsust kinnitab digitaalse maksekeskkonna kiire arenguga kaasnenud maksepettuste erakordne kasv ning petturite järjest mitmekesisemad toimepanemise meetodid.[9] Üksnes 2025. aastal langes kelmuste ohvriks 3685 inimest ning pettusega tekitatud kogukahju ületas 29 miljonit eurot.[10] Võrreldes aasta varasemaga, suurenes tekitatud kahju ühe aastaga pea kahekordselt.[11] Seetõttu ei ole vastutuse jaotuse küsimus teoreetiline, vaid vahetu praktilise tähtsusega.

Kirjeldatud pettusjuhtumite õiguslik analüüs eeldab arusaamist vastutuse jaotuse süsteemist, mis kohaldub autoriseerimata maksetehingute korral. Lähtepunktiks on VÕS § 733^2 lõikes 2 sätestatud põhimõte, mille kohaselt peab makseteenuse pakkuja autoriseerimata maksetehingu summa maksjale viivitamata tagastama. Tegemist on makseteenuse kasutaja kaitseks kehtestatud reegliga, mille kohaselt jääb autoriseerimata maksetehingust tulenev kahju riisiko

[4] Eesti Pank. Maksepettuste ülevaade 2025. Eesti Pank, 2025, lk 4. – https://haldus.eestipank.ee/sites/default/files/2025-12/ep_maksepettuste-ulevaade-2025_0.pdf (14.04.2026).
[5] ERR. Kelmid on tänavu Eesti inimeste kontodelt varastanud 23 miljonit eurot. ERR, 13.01.2026. – https://www.err.ee/1609865229/kelmid-on-tanavu-eesti-inimeste-kontodelt-varastanud-23-miljonit-eurot (14.04.2026).
[6] Eesti Pangaliit. Pettuste ennetamine. – https://pangaliit.ee/pettuste-ennetamine (09.04.2026).
[7] Eesti Pangaliit. Uue Smart-ID loomisega seotud pettused põhjustavad miljonikahju – inimesed ei teadvusta ohumärke. Eesti Pangaliit, 30.10.2025. - https://pangaliit.ee/uudised-ja-teated/uue-smart-id-loomisega-seotud-pettused-pohjustavad-miljonikahjusid-inimesed-ei-teadvusta-ohumarke (16.01.2026).
[8] Politsei- ja Piirivalveamet. Politseis registreeritud sündmused. 05.12.2025. – https://www.politsei.ee/et/uudised/politseis-registreeritud-suendmused-473cb3-13111 (05.03.2026).
[9] Eesti Pangaliit. Uue Smart-ID loomisega seotud pettused põhjustavad miljonikahju - inimesed ei teadvusta ohumärke. 30.10.2025.
[10] Politsei- ja Piirivalveamet. Kelmid petsid Eesti inimestelt välja 29 miljonit eurot. - https://www.politsei.ee/et/uudised/kelmid-petsid-eesti-inimestelt-vaelja-29-miljonit-eurot-13196 (20.01.2026).
[11] *Ibid.*

esmajärjekorras makseteenuse pakkuja, mitte maksja kanda. Nimetatud esmane vastutus ei ole siiski absoluutne. Sõltuvalt maksja käitumisest võib vastutus teatud juhtudel kanduda maksjale.

Eesti õiguses on maksja vastutus autoriseerimata maksetehingu korral üles ehitatud süü astme järgi. Esiteks, kui eID omaja on rikkunud oma hoolsuskohustusi üksnes hooletusest, vastutab ta VÕS § 733^8 lõikes 1 sätestatud piiratud omavastutuse alusel kahju eest kuni 50 euro ulatuses ning ülejäänud kahju jääb makseteenuse pakkuja kanda. Teiseks, VÕS § 733^8 lõike 2 alusel ei kohaldu 50-eurone omavastutuse piirmäär juhul, kui autoriseerimata maksega seoses on tegemist maksjapoolse pettusega või kui eID omaja on tahtlikult või raske hooletuse tõttu rikkunud makseinstrumendi või eID kasutamisega seotud kohustusi. Sellisel juhul vastutab maksja kahju eest täies ulatuses. Samal ajal näeb regulatsioon ette ka olukordi, kus vastutus jääb makseteenuse pakkujale isegi siis, kui klient on käitunud hooletult, eelkõige juhul, kui makseteenuse pakkuja ei ole täitnud tugeva kliendi autentimise nõuet. Need vastutuse jaotuse põhimõtted moodustavad käesoleva töö edasise analüüsi aluse ning nende täpsem sisu avatakse töö teises peatükis.

Kirjeldatud pettuseskeemid erinevad üksteisest eelkõige selle poolest, millise õigusliku küsimuse need esile tõstavad. Kui isik kinnitab eID-vahendiga tehingu, teadmata, et ta kinnitab maksetehingut, või kui pettur teeb kinnituse ohvri teadmata, tekib esmalt küsimus, kas sellist maksetehingut saab üldse pidada VÕS § 724^1 lõike 1 tähenduses autoriseerituks. Mõlemal juhul on määrav asjaolu, et maksjal puudus tegelik tahe maksetehingut teha, mistõttu muutub küsitavaks ka tehniliselt korrektse kinnituse õiguslik tähendus. Seevastu olukorras, kus isik teeb ülekande teadlikult, kuid pettuse teel loodud eksliku ettekujutuse mõjul, ei seisne probleem enam autoriseerituse puudumises, vaid vastutuse jaotuses. Sellisel juhul soovib maksja küll konkreetse makse teha, kuid küsimus on selles, kas ja millistel tingimustel võib makseteenuse pakkuja esmase vastutuse asemel jääda kahju maksja kanda raske hooletuse tõttu. Eesti kohtupraktikas ja õiguskirjanduses puudub mõlema olukorra osas seni ühtne lähenemine. Esimesel juhul ei ole selge, millistel tingimustel võib eID-vahendi tehnilist kasutamist pidada piisavaks tõendiks maksja tegeliku tahteavalduse kohta. Teisel juhul on vaieldav, millises ulatuses peaks pettuse teel kujundatud ekslik ettekujutus mõjutama vastutuse jaotust maksja ja makseteenuse pakkuja vahel.

Eeltoodust lähtuvalt on magistritöö eesmärk analüüsida, kuidas jaotub vastutus makseteenuse pakkuja ja eID omaja vahel olukorras, kus eID-d on kasutatud pettuse tulemusel makse tegemiseks, ning hinnata, kas kehtiv vastutuse jaotus Eesti õiguses on põhjendatud. Lisaks

analüüsitakse töös, milliseid lahendusi ja muudatusi näevad ette Euroopa Liidu uue makseteenuste direktiivi (PSD3)[12] ja makseteenuste määruse (PSR)[13] eelnõu, ning kas kavandatavad muudatused tooksid kaasa maksja õiguste tasakaalustatuma kaitse. Püstitatud eesmärgi saavutamiseks otsitakse töös vastuseid järgmistele uurimisküsimustele:

1. Mida tähendab autoriseerimata makse eID kasutamise kontekstis ning millistel tingimustel saab eID abil kinnitatud maksetehingut pidada maksjale siduvaks?

2. Kuidas jaguneb kehtiva õiguse kohaselt vastutus makseteenuse pakkuja ja eID omaja vahel juhul, kui autoriseerimiseks on kasutatud pettuse teel saadud isiku eID-d?

3. Millisel viisil mõjutab PSD3 ja PSR rakendumine vastutuse jaotamise reegleid eID omaja ja makseteenuse pakkuja vahel autoriseerimata maksete kontekstis?

Uurimisküsimustele vastamiseks kasutatakse magistritöös analüütilist, dogmaatilist ja võrdlevat uurimismeetodit. Töö tugineb autoriseerimata makseid käsitlevale õiguskirjandusele, asjakohasele kohtupraktikale ning kehtivale Euroopa Liidu, Norra ja Eesti makseteenuste regulatsioonile. Analüüsi keskmes on VÕS makseteenuseid reguleerivad sätted, PSD2 direktiiv ning PSD3 direktiivi ja PSR määruse eelnõu. Täiendavalt tuginetakse siseriiklike seaduste seletuskirjadele ja kommentaaridele ning Euroopa Komisjoni ja Euroopa Pangandusjärelevalve (EBA) suunistele ja küsimuste-vastuste (Q&A) dokumentidele. Võrdleva meetodi raames kasutatakse Norra õigust ja praktikat eelkõige nõusoleku tuvastamise, tõendamiskoormise jaotuse ning makseteenuse pakkuja ja maksja vastutuse piiride käsitlemisel eID kasutamise kontekstis.

Magistritöö teema on uudne, kuna vastutust autoriseerimata maksete puhul eID kasutamise kontekstis ning selle seoseid kavandatava PSD3 direktiivi ja PSR määrusega ei ole autorile teadaolevalt varasemates Eesti uurimis- ega magistritöödes põhjalikumalt käsitletud. Varasemates magistritöödes on analüüsitud autoriseerimata maksete üldist regulatsiooni ja elektrooniliste maksevahendite tehnilist kasutamist[14] ning ka eID rolli tahteavalduste ja

[12] Euroopa Komisjoni ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, milles käsitletakse makseteenuseid ja e-raha teenuseid siseturul ning millega muudetakse direktiivi 98/26/EÜ ja tunnistatakse kehtetuks direktiivid 2015/2366/EL ja 2009/110/EÜ. - COM(2023) 366 final, 28.06.2023.
[13] Euroopa Komisjoni ettepanek: Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse makseteenuseid siseturul ning millega muudetakse määrust (EL) nr 1093/2010. - COM(2023) 367 final, 28.06.2023.
[14] Rink, R. Autoriseerimata maksetehing elektroonilise maksevahendiga. Magistritöö. Juhendaja Urmas Volens. Tartu Ülikool 2012. - https://dspace.ut.ee/server/api/core/bitstreams/0d6468c2-e626-40b3-9de5-9d4cd3c75d00/content (02.12.2025)

esindusõiguse kontekstis tsiviilõiguse üldpõhimõtete raames[15], kuid puudub terviklik käsitlus, mis seoks autoriseerimata maksete vastutuse, eID kasutamise ning PSD3 ja PSR eelnõus kavandatavad muudatused ühtseks uurimisobjektiks. Kehtiva regulatsiooni pinnalt on autoriseerimata maksete ja eID abil antud nõusoleku puudumise problemaatikat Eesti õiguskirjanduses hiljuti põhjalikult käsitlenud P. Kalamees Juridica artiklis "„Näita käppa" ehk minu digiallkiri, järelikult minu tehtud tehing" (2024).[16] Käesolev magistritöö arendab seda käsitlust edasi, keskendudes kehtivas õiguses tuvastatud kitsaskohtadele. Töö panus seisneb Eesti regulatsiooni võrdlemises Norra õiguse ja kohtupraktikaga ning PSD3 ja PSR eelnõu mõju hindamises vastutuse jaotusele.

Magistritöö koosneb kahest peatükist. Esimeses peatükis käsitletakse makse autoriseerimist eID abil, autoriseerimise tõendamist ning maksejuhise täitmist. Esmalt analüüsitakse nõusoleku rolli maksetehingu autoriseerimise eeltingimusena, eristades tehnilist autentimist eID omaja tegelikust tahtest. Seejärel käsitletakse tõendamiskoormise jaotust olukorras, kus eID abil tehtud maksetehingu autoriseeritus on vaidlustatud. Peatüki lõpus analüüsitakse maksejuhise täitmist ja sellest keeldumist pettusekahtluse korral. Teises peatükis käsitletakse vastutuse jaotust autoriseerimata maksete korral eID kasutamise kontekstis. Selleks analüüsitakse makseteenuse pakkuja vastutust ja tõendamiskoormist, eID omaja üldist vastutust, piiratud ja piiramatut vastutust ning vastutuse välistamise aluseid.

Magistritööd iseloomustavad järgmised märksõnad: digitaalne identiteet; maksed; vastutus; tahteavaldus; pettus.

[15] Naabel, K. Esindusõigus näivusvolituse alusel ja selle isikuline piiritlus, sealhulgas eID kasutamise mõju esindusõiguse kehtivusele. Magistritöö. Juhendaja Piia Kalamees. Tartu Ülikool 2024. - https://dspace.ut.ee/server/api/core/bitstreams/7df28517-7669-4a43-9397-755c9cd22e62/content (03.12.2025)
[16] Kalamees, P. „Näita käppa" ehk minu digiallkiri, järelikult minu tehtud tehing. - Juridica 2024 nr 9-10, lk 715-725.

1. MAKSE AUTORISEERIMINE eID-GA JA MAKSEJUHISE TÄITMINE

1.1. MAKSE AUTORISEERIMINE eID-GA

Eesti õiguses on maksetehingu autoriseerituse keskne põhimõte sätestatud VÕS § 724[1] lõikes 1, mille kohaselt loetakse maksetehing autoriseerituks üksnes siis, kui maksja on andnud selleks nõusoleku. Nõusoleku võib anda enne tehingu tegemist või poolte kokkuleppel ka tagantjärele heakskiiduna. Nõusoleku puudumisel on tegemist autoriseerimata maksetehinguga. VÕS § 724[1] lõige 2 täpsustab, et autoriseerimise viis ja kord ühe või mitme maksetehingu täitmiseks määratakse poolte kokkuleppel ning kokkuleppimata viisil maksetehingu täitmiseks antud nõusoleku korral ei loeta maksetehingu täitmist autoriseerituks. Seega eeldab nõusolek lisaks tahte olemasolule ka selle väljendamist kohases vormis ja kokkulepitud viisil, näiteks eID-vahendi abil.

Praktikas määratakse autoriseerimisviisid üldjuhul makseteenuse raamlepingu tüüptingimustes. Swedbanki[17] ja SEB[18] deebetkaardi tingimused seovad nõusoleku andmise muu hulgas PIN-koodi sisestamise, kaardiandmete või turvaelementide kasutamise, viipemakse tegemise, kviitungi allkirjastamise või muu kokkulepitud autoriseerimisviisiga. Turvaelementide hulka kuuluvad sellistes tingimustes ka Smart-ID, Mobiil-ID ja ID-kaart. Seega kujuneb eID abil autoriseerimise viis praktikas eelkõige krediidiasutuse tüüptingimuste kaudu, milles nõusoleku andmine seotakse konkreetse tehnilise toiminguga.

Kuivõrd autoriseerimisviise määratlevad tingimused mõjutavad otseselt seda, millal loetakse maksetehing maksja poolt heaks kiidetuks, tuleb hinnata nende kehtivust tüüptingimustena. Swedbanki deebetkaardi kasutamise lepingu tingimuste punkt 3.7 ja SEB rahvusvahelise deebetkaardi lepingu tingimuste punkt 26 on käsitatavad tüüptingimustena VÕS § 35 tähenduses, sest need sisalduvad krediidiasutuste poolt eelnevalt väljatöötatud standardtingimustes, mida kasutatakse klientidega sõlmitavates lepingutes ühetaolisel kujul ning mille sisu klient üldjuhul mõjutada ei saa. Sellised tingimused saavad lepingu osaks VÕS § 37 lõike 1 alusel, kui kliendile on neile viidatud ja tal on olnud võimalus nende sisuga tutvuda. Autoriseerimisviiside määratlemine ei ole VÕS § 37 lõike 3 tähenduses iseenesest üllatuslik

[17] Swedbank AS. Deebetkaardi kasutamise lepingu tingimused. Kehtivad alates 01.11.2023. - https://www.swedbank.ee/static/pdf/private/d2d/cards/conditions_debitcard_est_01112023.pdf (26.03.2026).
[18] SEB Pank AS. Rahvusvahelise deebetkaardi lepingu tingimused. Kehtivad alates 26.06.2025. - https://www.seb.ee/sites/default/files/tac/rahvusvahelise_deebetkaardi_lepingu_tingimused_20250626_est.pdf (26.03.2026).

ega arusaamatu, sest makseteenuse olemusest tulenevalt on vajalik kokku leppida, milliste toimingutega saab maksja maksetehingule nõusoleku anda.

VÕS § 42 lõike 1 tähenduses ei ole tarbijat ebamõistlikult kahjustav see, et nõusoleku andmise viisid on määratud makseteenuse pakkuja tüüptingimustes. Vastupidi, see suurendab kliendi jaoks ettenähtavust ning võimaldab makseteenuse pakkujal makseid turvaliselt ja kontrollitavalt täita. Selline lahendus on kooskõlas VÕS § 724[1] lõikega 2 ja PSD2 artikli 64 loogikaga, mille kohaselt määratakse nõusoleku andmise viis ja kord poolte kokkuleppel. Probleem võib tekkida üksnes juhul, kui tüüptingimus võimaldab makseteenuse pakkujal autoriseerimisviise ühepoolselt ja kliendile ettenähtamatult laiendada.

Probleem võib tekkida juhul, kui tüüptingimus võimaldab makseteenuse pakkujal autoriseerimisviise ühepoolselt ja kliendile ettenähtamatult laiendada. Sellise küsimuse tõstatab näiteks Swedbanki tingimuste punkt 3.7 osas, mille kohaselt loetakse nõusolek antuks ka „muul poolte vahel kokku lepitud ja/või panga poolt aktsepteeritud viisil“. Seda sõnastust tuleks tõlgendada kitsendavalt: panga poolt aktsepteeritud viis saab olla kehtiv autoriseerimisviis üksnes juhul, kui klient sai enne maksetehingu tegemist mõistlikult aru, et vastava toiminguga annab ta maksetehinguks nõusoleku. Vastasel juhul võiks tingimus olla vastuolus VÕS § 724[1] lõikega 2 ning kahjustada tarbijat ebamõistlikult, sest kliendile ei oleks piisavalt ettenähtav, millise toiminguga loetakse ta maksetehingu siduvalt autoriseerinuks. Seega võivad tüüptingimused määrata nõusoleku andmise viisi ja korra, kuid need ei saa asendada nõusoleku materiaalõiguslikku sisu ega muuta tehnilist autentimistoimingut automaatselt maksja tegeliku tahteavaldusega samastatavaks.

VÕS-i kommenteeritud väljaande kohaselt seisneb nõusolek tegevuses või toimingus, millega maksja annab makseteenuse pakkujale maksejuhise maksetehingu tegemiseks ja kinnitab selle kokkulepitud autoriseerimisviisil, näiteks allkirja või makseinstrumendi kasutamiseks ettenähtud isikustatud turvaelemendi abil.[19] Selline kinnitus võib olla antud ka elektroonilises keskkonnas, näiteks eID abil internetipangas maksetehingu algatamisel, mille puhul on tegemist elektroonilise maksetehinguga VÕS § 724[6] lg 3 tähenduses.[20] Lisaks tuleb kommenteeritud väljaande kohaselt arvestada, et ilma nõusolekuta või puuduliku nõusolekuga tehing on ilma maksja nõusolekuta tehtud tehing ning sellise tehingu toimumisel on maksjal

[19] Ulp, M. VÕS § 724[1], komm 3.1.
[20] *Ibid,* komm 3.3.

makseteenuse pakkuja vastu nõue taastada maksja kontol olukord, nagu tehingu summat ei oleks debiteeritud.[21]

Kuna VÕS-i makseteenuste regulatsioon ei ava nõusoleku sisulise olemasolu kriteeriume, tuleb selle hindamisel tugineda tsiviilõiguse üldpõhimõtetele, eeskätt tahteavalduse üldreeglitele. Tsiviilseadustiku üldosa seaduse kommenteeritud väljaande kohaselt ei sätesta seadus tahteavalduse mõistet otsesõnu, kuid selle sisu on võimalik avada tehingu mõiste kaudu.[22] Tsiviilseadustiku üldosa seaduse (TsÜS)[23] § 67 lõike 1 järgi on tehing toiming või omavahel seotud toimingute kogum, milles sisaldub kindla õigusliku tagajärje kaasatoomisele suunatud tahteavaldus. TsÜS-i kommenteeritud väljaandes täpsustatakse, et tahteavaldus on õigusliku tagajärje kaasatoomisele suunatud tahte väljendamine.[24] Sellest tuleneb, et ka eID kaudu antud kinnitus peab autoriseerimise tähenduses väljendama tahet tuua kaasa konkreetsele maksetehingule omane õiguslik tagajärg, s.o maksetehingu tegemine.

P. Kalamehe hinnangul ei ole olukorras, kus eID omajal puudub tegelik tahe maksetehingu tegemiseks, VÕS § 724[1] lõike 1 tähenduses nõusolekut antud ning maksetehing ei saa olla maksjale siduv.[25] Selline järeldus eeldab siiski iga juhtumi eraldi hindamist, eeskätt seda, kas manipuleeritud isik mõistis PIN-koodide sisestamisel oma tegevuse tegelikku tähendust ja soovis sellega kaasnevaid varalisi tagajärgi. Seega ei saa eID abil antud tehnilist kinnitust automaatselt samastada maksja tegeliku nõusolekuga, kui asjaolud viitavad sellele, et eID omajal puudus tahe maksetehingu tegemiseks.

Nõusoleku materiaalõigusliku käsitluse kõrval tuleb eraldi käsitleda tugeva autentimise nõuet. VÕS § 724[6] lõike 3 kohaselt peab makseteenuse pakkuja nõudma kliendi tugevat autentimist iga kord, kui maksja soovib interneti kaudu juurdepääsu oma maksekontole, algatada elektroonilist maksetehingut või teha muid kaugühenduse kaudu toiminguid, millega kaasneb makseteenusega seotud andmete väärkasutamise või pettuse oht. VÕS kommenteeritud väljaandes on selgitatud, et tugev autentimine tähendab kõrge turvalisusega kliendi isikusamasuse tuvastamist vähemalt kahe eraldiseisva tunnuse abil ning Eesti kontekstis on sellised vahendid peamiselt ID-kaart, Mobiil-ID, Smart-ID ja PIN-kalkulaator.[26]

[21] Ulp, M. VÕS § 724[1], komm 3.2.
[22] Varul, P. jt (koost). TsÜS § 67, komm 3.1.2. - Tsiviilseadustiku üldosa seadus. Komm vlj. Tartu: Juura 2023.
[23] Tsiviilseadustiku üldosa seadus. - RT I, 31.12.2024, 48.
[24] Sein, K., Varul, P. TsÜS § 67, komm 3.1.2.
[25] Kalamees, P. „Näita käppa“ ehk minu digiallkiri, järelikult minu tehtud tehing. - Juridica 2024 nr 9-10, lk 721.
[26] Ulp, M. VÕS § 709, komm 3.7.15.

Elektroonilises keskkonnas toimub kliendi isikusamasuse tuvastamine kliendile väljastatud isikustatud turvaelemendi abil, mille eesmärk on tagada kliendi andmete konfidentsiaalsus, rahaliste vahendite turvalisus ning andmete terviklikkus, muutumatus ja konfidentsiaalsus.[27]

VÕS § 724[1] lg 1 ja § 724[6] lg 3 reguleerivad seega maksetehingu autoriseerimise kontekstis eri tasandi küsimusi. VÕS § 724[1] lõige 1 vastab küsimusele, kas maksja on andnud nõusoleku maksetehingu tegemiseks. VÕS § 724[6] lõige 3 reguleerib aga seda, kuidas seda nõusolekut elektroonilises keskkonnas tuleb tehniliselt vastu võtta, st milliste turvanõuete ja autentimisvahendite abil. Teisisõnu puudutab VÕS § 724[1] nõusoleku materiaalõiguslikku olemasolu, samas kui VÕS § 724[6] puudutab elektroonilises keskkonnas vastuvõtmise tehnilist turvanõuet. Tugev autentimine võib olla viis, mille kaudu maksja oma nõusolekut väljendab, kuid see ei ole iseseisev nõusoleku materiaalõiguslik alus.

Sellest eristusest tulenevalt tuleb eID-ga tehtud maksetehingu autoriseerimist hinnata kahel tasandil: tehnilisel ja materiaalõiguslikul. Tehniline autoriseerimine tähendab, et maksetehing kinnitati kokkulepitud autentimisvahendi abil ja infosüsteem registreeris kinnituse nõuetekohaselt. Materiaalõiguslik autoriseerimine eeldab aga, et eID omajal oli tegelik ja teadlik tahe kinnitada just konkreetne makse, sealhulgas selle summa, saaja ja eesmärgi.[28] Tugeva autentimise nõue aitab küll vähendada kõrvaliste isikute ligipääsu elektroonilistele maksetele, kuid ei lahenda kõiki autoriseerimisega seotud probleeme.[29] Õiguskirjanduses on märgitud, et petturid on kohandanud oma tegutsemisviise, kuna PSD2-st tulenevad tugeva autentimise nõuded on vähendanud mitmete varem kasutatud pettusmeetodite tõhusust.[30] Seetõttu võivad tehniline ja materiaalõiguslik tasand pettuse korral lahkneda: maksetehing võib olla tehniliselt korrektselt kinnitatud, kuid maksja tahe ei pruugi olla suunatud konkreetse maksetehingu tegemisele.

Kuna VÕS § 724[1] ja § 724[6] põhinevad PSD2 regulatsioonil, tuleb neid sätteid tõlgendada võimalikult kooskõlas direktiivi sõnastuse, ülesehituse ja eesmärgiga. Seetõttu tuleb hinnata, kas Eesti õiguses tehtud eristus maksja nõusoleku ja tugeva kliendi autentimise vahel on

[27] Ulp, M. VÕS § 724[6], komm 3.
[28] Kjørven, M. E., Høgberg, A. P., Woxholth, G. The customer's liability for fraud-induced use of BankID and payment instruments. Oslo Law Review, 2024, 11(2). – https://www.scup.com/doi/10.18261/olr.11.2.3#sec-4 (12.03.2026).
[29] European Commission. Questions and answers: Strong Customer Authentication and open banking. European Commission, 16.09.2019. – https://ec.europa.eu/commission/presscorner/detail/et/qanda_19_5555 (14.03.2026)
[30] European Banking Authority. EBA Consumer Trends Report 2024/25. European Banking Authority, 26.03.2025, lk 37. – https://www.eba.europa.eu/sites/default/files/2025-03/514b651f-091b-42d3-b738-1fae79264044/Consumer%20Trends%20Report%202024-2025.pdf (14.04.2026).

kooskõlas PSD2 süsteemiga. PSD2 eesmärk on muu hulgas tagada makseteenuste turvalisus ning makseteenuse kasutajate kõrgetasemeline kaitse, sealhulgas pettuseriskide eest.[31] Sellest eesmärgist lähtudes tuleb eristada PSD2 artiklis 64 sätestatud nõusolekupõhist autoriseerimist ning PSD2 artiklites 97 ja 98 sätestatud tugeva kliendi autentimise nõudeid.

PSD2 artikli 64 lõike 1 kohaselt loetakse maksetehing autoriseerituks ainult siis, kui maksja on andnud nõusoleku maksetehingu täitmiseks, sealjuures võib makse olla autoriseeritud nii enne selle täitmist kui ka poolte kokkuleppel tagantjärele. Nõusoleku andmise viis määratakse PSD2 artikli 64 lõike 2 kohaselt kindlaks maksja ja asjaomase makseteenuse pakkuja vahelisel kokkuleppel. See vastab sisuliselt VÕS § 724[1] lõigetes 1 ja 2 sätestatud regulatsioonile. PSD2 artikli 97 lõige 1 reguleerib tugeva kliendi autentimise kasutamist, nähes ette selle kohustuslikkuse muu hulgas juhul, kui maksja soovib pääseda interneti kaudu ligi oma maksekontole, algatab elektroonilise maksetehingu või teeb kaugjuurdepääsu teel muu toimingu, mille puhul võib esineda maksepettuse või muu kuritarvitamise riski oht. Elektrooniliste kaugmaksetehingute puhul täpsustab PSD2 artikli 97 lõige 2, et tugev kliendi autentimine peab hõlmama elemente, millega seostatakse tehing dünaamiliselt konkreetse summa ja konkreetse makse saajaga. PSD2 artikli 98 lõike 1 kohaselt täpsustatakse regulatiivsete tehniliste standarditega muu hulgas tugeva kliendi autentimise nõudeid, selle kohaldamise erandeid, isikustatud turvavolituste konfidentsiaalsuse ja tervikluse kaitse nõudeid ning turvalise teabevahetuse nõudeid. PSD2 artikli 98 lõige 2 näitab omakorda, et nende standardite eesmärk on muu hulgas tagada makseteenuse kasutajate ja makseteenuse pakkujate jaoks vajalik turvalisuse tase, makseteenuse kasutajate rahaliste vahendite ja isikuandmete turvalisus ning tehnoloogia- ja ärimudeli neutraalsus.

Sellest ülesehitusest tuleneb, et PSD2 ei samasta maksja nõusolekut tugeva kliendi autentimisega. PSD2 artiklis 64 sätestatud nõusolek puudutab maksetehingu siduvust maksja suhtes, samas kui artiklites 97 ja 98 sätestatud tugev kliendi autentimine puudutab elektrooniliste maksete turvalist teostamist. Seetõttu toetab PSD2 süsteem VÕS § 724[1] ja § 724[6] tõlgendust, mille kohaselt võib tugev autentimine olla nõusoleku väljendamise tehniline viis, kuid see ei asenda nõusoleku materiaalõiguslikku olemasolu.

Õiguskirjanduses on rõhutatud, et elektrooniliste kaugmaksete puhul peab tugev kliendi autentimine olema seotud konkreetse maksesumma ja konkreetse makse saajaga. See tähendab,

[31] PSD2 põhjendus 33.

et autentimisprotsess peab võimaldama maksjal aru saada, millist summat ja millisele saajale ta kinnitab.[32] Käesoleva magistritöö seisukohalt on see oluline, sest eID abil tehtud maksete puhul ei ole määrav üksnes PIN-koodi sisestamise fakt, vaid ka see, kas eID omaja sai autentimistoimingu hetkel aru, millist maksetehingut ta kinnitab.

Autoriseerimise mõiste tõlgendamisel ei ole EL-i liikmesriikides kujunenud ühtset seisukohta. Õiguskirjanduses on eristatud kolme peamist tõlgendust. Esiteks loetakse tehing autoriseerituks juhul, kui maksja andis makseteenuse pakkujale korralduse kanda kindel summa kindlale kontole, sõltumata sellest, kas ta tegi seda pettuse või eksituse mõjul. Selle käsitluse keskmeks on maksekorralduse formaalne andmine. Teiseks on tehing autoriseeritud üksnes siis, kui maksjal oli tegelik tahe teha makse konkreetsele saajale ja kindlal eesmärgil. Kolmanda käsitluse kohaselt ei ole määrav mitte niivõrd see, kas maksja soovis maksta just sellele saajale või konkreetsel põhjusel, vaid see, kas ta vähemalt mõistis, et tema tegevuse tulemusena teostatakse maksetehing.[33]

Esimese ja kolmanda tõlgenduse vahel on oluline sisuline erinevus. Esimese käsitluse puhul piisab autoriseerituse jaatamiseks sellest, et maksja tegi toimingu, mille alusel makse tehniliselt täideti, sõltumata sellest, kas ta mõistis selle toimingu tegelikku tähendust või tagajärge. Kolmanda lähenemise järgi eeldab autoriseerimine seevastu vähemalt seda, et maksja sai aru, et tema tegevuse tulemusena toimub maksetehing. Seega paikneb kolmas lähenemine esimese ja teise käsitluse vahel, nõudes enamat kui pelgalt toimingu tegemist, kuid mitte teadlikkust konkreetsest saajast ega makse eesmärgist. Käesoleva töö autori hinnangul haakub PSD2 eesmärkide ja Eesti õiguse ülesehitusega kõige paremini teine lähenemine: nõusoleku olemasolu eeldab, et maksjal oli tegelik tahe teha konkreetne makse konkreetsele saajale. Selline käsitlus on kooskõlas TsÜS § 67 lõike 1 nõudega, mille kohaselt peab tahteavaldus olema suunatud kindla õigusliku tagajärje kaasatoomisele.

Sellist tõlgendust toetab ka õiguskirjanduses esitatud seisukoht, et makseteenuse tüüptingimused võivad küll määrata nõusoleku väljendamise viisi ja korra, kuid need ei saa asendada nõusoleku materiaalõiguslikku olemasolu. Makseinstrumendi või turvaelemendi igasugune kasutamine ei saa seetõttu automaatselt tähendada, et maksetehing on maksjale

[32] Steennot, R. Reduced payer's liability for unauthorized payment transactions under the second Payment Services Directive (PSD2). – Computer Law & Security Review 2018/34(4), lk 959-960. - https://www.sciencedirect.com/science/article/pii/S0267364918301924?via%3Dihub (15.03.2026)
[33] Van Praag, E. jt, „Authorised Push Payment Fraud: Suggestions for the Draft Payment Services Regulation", EBI Working Paper Series 2025, nr 190, lk 4-5.

omistatav, sõltumata tema tegelikust tahtest konkreetne makse teha. Vastasel juhul jääks maksja kanda kogu risk ka olukorras, mida makseteenuste regulatsiooni eesmärgi järgi tuleks hinnata autoriseerimata maksetehinguna.[34]

Eeltoodud Eesti õiguse ja PSD2 süsteemi käsitlusest tuleneb, et eID kasutamisega seotud pettusjuhtumites tuleb eristada kahte olukorda. Kui pettur kasutab eID omaja autentimisvahendeid tema teadmise ja osaluseta, puudub eID omaja tahteavaldus ning maksetehingut ei saa pidada VÕS § 724[1] lõike 1 tähenduses autoriseerituks. Kui aga eID omaja sisestab PIN-koodi ise, kuid teeb seda pettuse mõjul, ei saa autoriseeritust järeldada üksnes PIN-koodi sisestamisest. Sellisel juhul tuleb hinnata, kas maksja mõistis toimingu tegelikku tähendust ja soovis kinnitada konkreetset maksetehingut. Kui selline tahe puudus, on küsitav ka nõusoleku olemasolu.

Võrdlus Norra õiguse ja praktikaga toetab samuti tehnilise autentimise ja sisulise nõusoleku eristamist. Norra praktika on käesolevas kontekstis asjakohane eelkõige seetõttu, et ka Norras kasutatakse laialdaselt eID-põhiseid autentimislahendusi ning kohtud ja vaidluste lahendamise organid on pidanud käsitlema sarnaseid pettusjuhtumeid. Norra Ülemkohus on rõhutanud, et makse autoriseerimine eeldab maksja tegelikku tahet ning autentimisvahendi tehniline kasutamine ei pruugi alati tähendada kehtiva nõusoleku olemasolu.[35] Samuti on Norra vaidluste lahendamise praktikas leitud, et sotsiaalse manipulatsiooni juhtumites tuleb hinnata, kas tarbija sooritas autentimistoimingu teadmises, et ta kiidab heaks konkreetse makse. Nõusolek ei tähenda sellises käsitluses pelgalt autentimistoimingu tegemist, vaid tahte väljendamist makse tegemiseks.

Kokkuvõttes ei saa Eesti õiguses kokkulepitud autoriseerimisviisi tehnilist kasutamist samastada maksja materiaalõigusliku nõusolekuga. VÕS § 724[1] lõige 1 määrab maksetehingu autoriseerimise materiaalõigusliku eelduse ehk maksja nõusoleku olemasolu, VÕS § 724[1] lõige 2 võimaldab pooltel kokku leppida selle nõusoleku väljendamise viisi ja korra ning VÕS § 724[6] lõige 3 reguleerib tugeva kliendi autentimise kohustust elektrooniliste maksete puhul. Nende sätete koosmõjust tuleneb, et eID kasutamine võib olla kokkulepitud viis nõusoleku

[34] Wold, V., Kalamees, P. Identity Theft in Consumer Finance: Consent, Contract and Liability: Analysing Rules on Loss Allocation in Norwegian, Estonian and EU Law. – Oslo Law Review 2025/11(2), lk 12–13. - https://www.scup.com/doi/epdf/10.18261/olr.11.2.3 (13.12.2025)
[35] Norra Ülemkohus (Norges Høyesterett). Rt-2011-410. – https://lovdata.no/avgjorelse/hr-2011-00410 (19.02.2026).

väljendamiseks, kuid tehniliselt korrektne autentimine ei asenda iseenesest maksja tegelikku ja teadlikku tahet teha konkreetne maksetehing. Seetõttu tuleb eID-ga tehtud maksetehingu autoriseeritust hinnata nii tehnilise kinnituse nõuetekohasuse kui ka maksja tegeliku tahte olemasolu alusel.

1.2. TÕENDAMISKOORMIS

Käesoleva alapeatüki eesmärk on analüüsida autoriseerimise tõendamist olukorras, kus maksja vaidlustab eID abil tehtud maksetehingu. VÕS § 733[4] lõikes 1 on sätestatud üldreegel makseteenuse pakkuja tõendamiskoormise kohta juhuks, kui tekib vaidlus selle üle, kas maksetehing on tehtud maksja nõusolekul või kas makseteenuse pakkuja on maksetehingu nõuetekohaselt täitnud.[36] Kuigi säte reguleerib vahetult makseteenuse pakkuja tõendamiskoormist, on sellel keskne tähendus ka eID omaja seisukohalt, sest see määrab, milliseid asjaolusid peab makseteenuse pakkuja eID abil tehtud maksetehingu vaidlustamise korral tõendama ning milline tähendus on autentimislogidel, tugeva kliendi autentimise rakendamisel ja eID tehnilise kasutamise faktil.

VÕS § 733[4] lõike 1 kohaselt peab makseteenuse pakkuja juhul, kui on vaieldav, kas maksetehing on autoriseeritud või nõuetekohaselt täidetud, tõendama, et maksetehing on autenditud, muu hulgas rakendatud kliendi tugevat autentimist, korrektselt dokumenteeritud ja kontodel kajastatud ning et tehingu tegemist ei ole mõjutanud ükski puudus. Seega lasub autoriseerimise vaidlustamise korral esmane tõendamiskoormis makseteenuse pakkujal. Makseteenuse pakkuja peab näitama, et tehing läbis tehniliselt nõuetekohase autentimisprotsessi ja et tema süsteemis ei esinenud viga, mis oleks võinud mõjutada tehingu tegemist või kajastamist.

VÕS § 733[4] lõige 2 täpsustab makseteenuse pakkuja tõendamiskoormise piire. Sätte kohaselt, kui on vaieldav, kas makseinstrumendi abil tehtud maksetehing on autoriseeritud, ei ole ainuüksi makseinstrumendi kasutamise dokumenteerimine makseteenuse pakkuja poolt piisav tõendamaks, et maksetehing oli autoriseeritud, et makseinstrumenti kasutati pettuse teel või et maksja rikkus seadusest või makseinstrumendi väljastamise ja kasutamise tingimustest tulenevaid kohustusi tahtlikult või raske hooletuse tõttu. Sellest tuleneb oluline piirang

[36] Ulp, M. VÕS § 733[4], komm 3.1.

makseteenuse pakkuja tõendamiskoormise täitmisele: autentimislogid võivad tõendada, et maksetehing läbis tehnilise autentimise, kuid need ei ole iseseisvalt piisavad tõendamaks maksja nõusolekut ega tema käitumise etteheidetavust. eID abil tehtud maksete puhul tõendab autentimislogi eelkõige tehnilise kinnitustoimingu toimumist, mitte iseseisvalt maksja nõusolekut. Seetõttu tuleb VÕS § 733[4] lõike 2 kohaselt hinnata autentimisandmeid koos muude asjaoludega.

VÕS-i kommenteeritud väljaandes on selgitatud, et makseteenuse pakkuja peab tõendama, et makseinstrument ja selle isikustatud turvaelemendid on väljastatud konkreetsele kliendile ning olid tehingu tegemise ajal kehtivad ja vastasid makseteenuse pakkuja infosüsteemis olevatele andmetele.[37] Nende asjaolude tõendamiseks võib makseteenuse pakkuja tugineda infosüsteemi väljavõtetele, kuid üksnes nendest ei piisa järeldamaks, et maksja andis maksetehinguks nõusoleku. Tegemist on vaid ühe osaga tõendikogumist ning nõusoleku olemasolu tuleb hinnata kõiki asjaolusid kogumis arvestades.[38] Kommentaari kohaselt võib kliendi vaidlustuse korral tekkida tõendamiskoormise vastastikune toimimine: kui makseteenuse pakkuja tõendab tugeva kliendi autentimise kasutamist ning maksja omakorda tõendab, et tehing ei olnud tema poolt tehtud, võib teatud juhtudel tekkida eeldus, et maksja oli makseinstrumendi hoidmisel raskelt hooletu, mistõttu ta vastutab § 733[8] lg 2 alusel. Sellise eelduse saab maksja omakorda ümber lükata.[39]

Praktikas muudab eID vahendite laialdane kasutuselevõtt tõendamiskoormise keerukaks. Õngitsuskirjade, petukõnede või võltsitud pangalehtede puhul võib eID omaja sisestada PIN-koodid ise, mistõttu autentimislogi ei erine väliselt tavapärasest, pettuseta tehingust. P. Kalamees on rõhutanud, et eID abil antud tehniline kinnitus ei pruugi väljendada eID omaja tegelikku tahet teha konkreetne tehing.[40] Selline lähenemine võiks viia olukorrani, kus autoriseerimata maksete kaitse muutub sisuliselt näiliseks, sest tarbijal puudub reaalne võimalus dokumenteeritud autentimisfakti ümber lükata.[41] Samas peab eID omaja esitama vähemalt sellised asjaolud või tõendid, mis teevad usutavaks, et suure tõenäosusega ei andnud ta ise konkreetsele maksetehingule nõusolekut.[42] Selliste asjaoludena võivad kõne alla tulla

[37] Ulp, M. VÕS § 733[4], p 3.1.
[38] *Ibid*, p 3.2.
[39] *Ibid*, p 3.1.
[40] Kalamees, P. „Näita käppa“ ehk minu digiallkiri, järelikult minu tehtud tehing. - Juridica 2024 nr 9-10, lk 721.
[41] *Ibid.*
[42] *Ibid*, lk 722.

näiteks pettusele viitavad sõnumid, tehingu ebamõistlikkus eID omaja seisukohalt või muud asjaolud, mis viitavad sellele, et isik võis tegutseda eksimuses või pettuse mõjul.[43] Kui sellised asjaolud on esitatud, ei saa makseteenuse pakkuja autoriseerimise tõendamisel piirduda üksnes autentimislogide esitamisega, vaid nõusoleku olemasolu tuleb hinnata kõiki asjaolusid kogumis arvestades.

Kuna VÕS § 733[4] põhineb PSD2 artiklitel 41, 72, 73 ja 90, tuleb sätet tõlgendada kooskõlas direktiivi sõnastuse, ülesehituse ja eesmärgiga. PSD2 artikkel 41 puudutab tõendamiskohustust teabele esitatavate nõuete täitmise korral, PSD2 artikkel 73 reguleerib makseteenuse pakkuja tagastamiskohustust autoriseerimata maksetehingu korral ning PSD2 artikkel 90 käsitleb vastutust maksetehingu täitmata jätmise, valesti või hilinenud täitmise korral makse algatamise teenuste puhul. Need artiklid moodustavad VÕS § 733[4] laiema direktiivipõhise tausta, kuid käesoleva alapeatüki fookuses on küsimus, milline tõenduslik tähendus on makseinstrumendi kasutamise dokumenteerimisel ja tugeva kliendi autentimise rakendamisel olukorras, kus maksja vaidlustab maksetehingu autoriseerituse. Seetõttu on analüüsi keskmes eelkõige PSD2 artikkel 72.

PSD2 artikli 72 lõike 1 kohaselt peab makseteenuse pakkuja vaidluse korral tõendama, et maksetehing oli autenditud, korrektselt dokumenteeritud ja kontodel kajastatud ning et seda ei mõjutanud tehniline rike ega muu puudus. Kui maksetehing on algatatud makse algatamise teenuse pakkuja kaudu, lasub tõendamiskoormis oma pädevuse piires ka makse algatamise teenuse pakkujal. PSD2 artikli 72 lõige 2 täpsustab, et makseinstrumendi kasutamise registreerimine makseteenuse pakkuja poolt ei ole iseenesest piisav tõendamaks, et maksetehing oli maksja poolt autoriseeritud või et maksja pani toime pettuse või tegutses hooletuse või raske hooletusega.

PSD2 artiklit 72 tuleb tõlgendada koostoimes PSD2 artikliga 64, mille kohaselt eeldab autoriseeritud maksetehing maksja nõusolekut. PSD2 artikkel 72 ei määra seega uuesti kindlaks autoriseerimise materiaalõiguslikku eeldust, vaid reguleerib seda, kuidas nõusoleku olemasolu vaidluse korral tõendada. Kui makseinstrumendi kasutamise registreerimine oleks iseenesest piisav nõusoleku tõendamiseks, kaotaks PSD2 artikli 72 lõige 2 suure osa oma praktilisest tähendusest. Seetõttu toetab PSD2 süsteem VÕS § 733[4] lõike 2 tõlgendust, mille kohaselt on kokkulepitud autentimisvahendi kasutamine ja tugeva kliendi autentimise

[43] *Ibid.*

rakendamine olulised tõendid, kuid mitte iseseisvalt piisavad tõendid maksja nõusoleku, pettuse või etteheidetava kohustuste rikkumise kohta.

Autoriseerimise tõendamise praktilist tähendust aitab selgitada ka Euroopa Kohtu praktika. Euroopa Kohus on leidnud, et liikmesriigi kohus ei või eirata direktiivis tehtud eristust autoriseeritud ja autoriseerimata maksetehingute vahel ega otsustada vaidlusaluste maksete tagastusnõude üle ilma neid eelnevalt autoriseeritud või autoriseerimata makseteks kvalifitseerimata.[44] Samuti peab makseteenuse pakkuja antav teave olema piisavalt täpne ja tähenduslik, et maksja saaks vaidlusaluse maksetehingu tuvastada, sealhulgas võimaldama tuvastada isiku, kelle kasuks maksetehing tehti.[45] Seega ei saa autoriseerimise vaidlustamisel piirduda üksnes tehniliste autentimisandmete esitamisega. Maksjale peab olema kättesaadav ka piisav teave tehingu saaja ja asjaolude kohta, sest vastasel juhul on tal keerulisem hinnata, kas ta andis konkreetseks maksetehinguks nõusoleku, ning kasutada tõhusalt autoriseerimata maksetehingu korral ette nähtud õiguskaitsevahendeid.

Norra seaduse ja kohtupraktika mõistmiseks on oluline silmas pidada, et Norra finantsõiguses on vastutuse jaotus alates 1. jaanuarist 2023 reguleeritud uue finantslepingute seadusega (Finansavtaleloven)[46]. Kehtiv Norra regulatsioon on asjakohane võrdlusmaterjal, sest see sisaldab Eesti õigusega sarnast tõendamiskoormise reeglit, kuid täpsustab tarbijavaidlustes ka tõendamisstandardit. Finansavtaleloven § 3-7 lõike 1 kohaselt peab makseteenuse pakkuja kliendi vaidlustuse korral tõendama, et maksetehing oli autenditud, korrektselt registreeritud ja kontodel kajastatud ning et seda ei mõjutanud tehniline rike ega muu puudus. See vastab sisuliselt VÕS § 733^4 lõikele 1. Käesoleva töö seisukohalt on kesksem § 3-7 lõige 3, mille järgi ei piisa makseinstrumendi kasutamise registreerimisest iseenesest maksetehingu autoriseerituse ega kliendipoolse pettuse, tahtluse või raske hooletuse tõendamiseks. Selles osas on säte võrreldav VÕS § 733^4 lõikega 2 ning kinnitab, et autentimislogisid tuleb hinnata osana kogu tõendikogumist.

Norra õiguse eripära seisneb aga selles, et finansavtaleloven § 3-7 lõige 4 näeb tarbija nõusoleku ning tarbija võimaliku pettusliku või tahtliku kohustuste rikkumise tõendamiseks ette kõrgendatud tõendamisstandardi. Nimetatud sätte kohaselt ei piisa eeltoodud asjaolude tõendamiseks üksnes sellest, et nende esinemine on tõenäolisem kui nende puudumine, vaid

[44] EKo C-351/21, *ZG vs. Beobank SA*, ECLI:EU:C:2023:215, p 37.
[45] C-351/21, *ZG vs. Beobank SA*, p-d 57-59.
[46] *Lov om finansavtaler (finansavtaleloven)* 18.12.2020 nr 146. - Lovdata - https://lovdata.no/dokument/NL/lov/2020-12-18-146 (01.03.2026).

need peavad olema tõendatud suurema veenvusastmega. See tähendab, et tõendamiseks ei piisa üksnes sellest, et asjaolu esinemine on veidi tõenäolisem kui selle puudumine, vaid tõendikogum peab looma selgelt veenvama aluse järelduseks, et tarbija andis nõusoleku või rikkus kohustust tahtlikult. Eesti õiguses sellist sõnaselget kõrgendatud tõendamisstandardit ette nähtud ei ole. VÕS § 733^4 lõige 2 piirab küll makseinstrumendi kasutamise dokumenteerimise tõenduslikku tähendust, kuid ei sätesta eraldi, millise tõendamisstandardiga tuleb tõendada maksja nõusolekut, pettust, tahtlust või rasket hooletust. Seetõttu tuleb Eesti õiguses nende asjaolude tõendamisel lähtuda VÕS § 733^4 lõike 2 eesmärgist ja hinnata autentimislogisid koos muude asjaoludega, mitte iseseisvalt piisava tõendina.

Eesti õiguse seisukohalt toetab Norra võrdlus VÕS § 733^4 lõike 2 sisulist tõlgendamist. Kuigi Eesti õigus ei näe ette Norra õigusega võrreldavat sõnaselget kõrgendatud tõendamisstandardit, välistab VÕS § 733^4 lõige 2 autentimislogide käsitamise iseenesest piisava tõendina maksetehingu autoriseerituse, pettuse või raske hooletuse kohta. Seetõttu ei saa makseteenuse pakkuja eID-põhistes vaidlustes piirduda üksnes tehnilise autentimisjälje esitamisega, vaid peab esitama ka muid asjaolusid, mis kogumis võimaldavad hinnata maksja nõusoleku või etteheidetava käitumise olemasolu.

Kavandatav PSR artikli 55 lõige 2 kinnitab sama tõendamisõiguslikku põhimõtet, sätestades, et makseinstrumendi kasutamise registreerimine, sealhulgas tugeva kliendi autentimise kohaldamine, ei ole iseenesest piisav maksetehingu autoriseerituse tõendamiseks. Säte ei loo sisuliselt uut põhimõtet, sest sama loogika tuleneb juba PSD2 artiklist 72 ja VÕS § 733^4 lõikest 2, kuid PSR seob selle sõnaselgelt ka tugeva kliendi autentimisega. Eesti õiguse seisukohalt toetab see järeldust, et makseteenuse pakkuja ei saa vaidluse korral piirduda üksnes tehnilise autentimise tõendamisega, vaid maksja nõusolekut või etteheidetavat käitumist tuleb hinnata kogu tõendikogumi alusel. Eriti oluline on see eID-põhiste pettuste puhul, kus autentimine võib olla tehniliselt korrektne, kuid vaidlus seisneb maksja tegelikus arusaamas ja tahtes.

Kokkuvõttes tuleneb VÕS § 733^4 lõigetest 1 ja 2, et autoriseerimise tõendamisel ei saa piirduda üksnes autentimislogide või eID tehnilise kasutamise faktiga. Kuigi autentimislogid on olulised tõendid tehniliselt nõuetekohase kinnitustoimingu kohta, ei tõenda need iseenesest VÕS § 724^1 lõike 1 tähenduses maksja nõusolekut ega tema käitumise etteheidetavust. eID abil tehtud maksete puhul tuleb seetõttu eristada tehnilist tõendit autentimise kohta ja sisulist hinnangut sellele, kas maksja andis maksetehinguks nõusoleku või kas tema käitumine oli käsitatav pettuse, tahtluse või raske hooletusena. See tõendamisreegel on edasise vastutuse analüüsi

eelduseks: alles pärast seda, kui on hinnatud, kas maksetehing oli autoriseeritud või autoriseerimata, saab analüüsida makseteenuse pakkuja tagastamiskohustust ja eID omaja võimalikku vastutust.

1.3. MAKSEJUHISE TÄITMINE

Käesoleva alapeatüki eesmärk on analüüsida, kas ja millistel tingimustel võib makseteenuse pakkuja pettusekahtluse korral sekkuda maksejuhise täitmisse enne makse lõplikku teostamist. Maksetehingu õiguslik käsitlus ei piirdu üksnes autoriseerimise küsimusega, vaid hõlmab ka maksejuhise täitmise etappi. Just selles etapis võib tekkida küsimus, kas vormiliselt korrektse ja tehniliselt autenditud maksejuhise täitmine tuleb peatada või täiendavalt kontrollida, kui esineb objektiivselt põhjendatud kahtlus, et makse on algatatud pettuse või maksja manipuleerimise tulemusena. Kui makse peatatakse enne vahendite ülekandmist, võib kahju jääda realiseerumata ning hilisem autoriseerimata maksetehingu tagajärgede käsitlemine ei pruugi osutuda vajalikuks.

Maksejuhis on maksja antud korraldus maksetehingu tegemiseks.[47] VÕS § 709 lõike 7 kohaselt on maksejuhis igasugune maksetehingu tegemise korraldus, mille maksja annab makseteenuse pakkujale ning maksejuhise võib anda ka saaja kaudu. Arvestades makseteenuste tehnoloogilist arengut, võib maksejuhise anda väga erinevates vormides ja kanalites, sh maksekaardi abil, internetipangas, mobiilirakenduses või muus elektroonilises keskkonnas.[48] Maksejuhisega annab maksja makseteenuse pakkujale juhise teha konkreetne maksetehing, näiteks kanda rahasumma ühelt kontolt teisele.[49]

Kui eID vahendi abil kinnitatud maksejuhis jõuab makseteenuse pakkujani, järgneb sellele nii tehniline kui ka õiguslik hindamisetapp. Maksejuhiste aktsepteerimise tingimuste määruse[50] §-i 2 lõike 4 kohaselt tähendab maksejuhise aktsepteerimine krediidiasutuse nõusolekut teostada maksejuhise kohaselt makse ning sellega võtab krediidiasutus maksejuhise täitmiseks vastu. Kui maksejuhiste aktsepteerimise tingimuste määruse § 6 lõikes 1 sätestatud eeltingimused on

[47] Ulp, M. VÕS § 709, komm 3.7.1.
[48] Ulp, M. VÕS § 709, komm 3.7.1.
[49] *Ibid.*
[50] Eesti Panga Presidendi 11.05.2010 määrus nr 4 „Maksejuhiste aktsepteerimise tingimused". – RTL 2010, 25, 446.- https://www.riigiteataja.ee/akt/13312807 (15.03.2026).

täidetud, on krediidiasutus kohustatud maksejuhise aktsepteerima.[51] Eelnevast tuleneb, et makseteenuse pakkuja ülesanne on hinnata, kas maksejuhis vastab kokkulepitud tingimustele ja õigusaktides sätestatud nõuetele.[52]

Maksejuhise täitmisest keeldumist reguleerib VÕS § 724[3]. VÕS § 724[3] lõike 1 kohaselt peab makseteenuse pakkuja maksejuhise täitmisest keeldumise korral teavitama maksejuhise algatanud klienti keeldumisest, võimaluse korral selle põhjustest ning maksejuhise parandamise võimalustest. Keeldumise põhjusi ei pea teatama, kui makseteenuse pakkuja rikuks sellega temale mõne muu õigusaktiga pandud kohustust. VÕS kommenteeritud väljaande kohaselt võib põhjendatud juhtudeks maksejuhise täitmisest keeldumisel lugeda näiteks ebakorrektsete andmetega maksejuhist, saaja suletud kontot või esineb muu seadusest või lepingust tulenev põhjus.[53]

VÕS § 724[3] lõige 4 piirab makseteenuse pakkuja keeldumisõigust, sätestades, et makseteenuse pakkujal ei ole õigust keelduda autoriseeritud maksejuhise täitmisest, kui maksejuhis vastab makseteenuse lepingus määratud tingimustele ning selle täitmisega ei rikuta mõnes muus õigusaktis sätestatud kohustust. VÕS kommenteeritud väljaandes täpsustatakse, et makseteenuse pakkujal ei ole õigust keelduda maksejuhise täitmisest, kui maksejuhis on tehtud kliendi nõusolekul, mis vastab makseteenuse lepingus toodud tingimustele ja maksejuhise täitmisega ei rikuta õigusaktides toodud kohustust.[54] Muuhulgas peab makseteenuse pakkuja veenduma, et maksejuhise täitmiseks on antud nõusolek ja maksejuhis on vormistatud kooskõlas makseteenuse lepingu tingimustega.[55] Lisaks näeb VÕS § 724[3] lg 5 ette, et maksejuhist, mille täitmisest on õigustatult keeldutud, käsitatakse kättesaamata maksejuhisena. Seega ei seisne õigustatud keeldumise tähendus üksnes makse peatamises, vaid ka selles, et maksejuhisest ei teki tavapäraseid õiguslikke tagajärgi.

Autori hinnangul jätab kehtiv regulatsioon ebaselgeks, millises ulatuses võib või peab makseteenuse pakkuja hindama nõusoleku tegelikku olemasolu olukorras, kus maksejuhis on vormiliselt korrektne ja tehniliselt nõuetekohaselt autenditud, kuid esineb objektiivselt põhjendatud pettusekahtlus. VÕS § 724[3] lõige 4 võimaldab maksejuhise täitmisest keelduda eelkõige siis, kui maksejuhis ei vasta makseteenuse lepingus määratud tingimustele või kui

[51] Maksejuhiste aktsepteerimise tingimused § 4 lg 1 ja § 6 lg 1.
[52] Maksejuhiste aktsepteerimise tingimused § 4 lg 1.
[53] Ulp, M. VÕS § 724[3], p 3.1.
[54] Ulp, M. VÕS § 724[3], p 3.2.
[55] *Ibid.*

selle täitmine rikuks mõnest õigusaktist tulenevat kohustust. Säte ei nimeta pettusekahtlust iseseisva keeldumise ega täiendava kontrolli alusena. Seetõttu ei ole kehtivast õigusest üheselt selge, kas makseteenuse pakkuja võib tehniliselt korrektse maksejuhise täitmise peatada üksnes põhjusel, et esineb objektiivselt põhjendatud kahtlus, et maksja nõusolek on saadud pettuse või manipuleerimise teel.

Eeltoodud regulatiivne ebaselgus on omandanud suurema praktilise tähenduse seoses maksekeskkonna kiirenemisega. 2024. aastal võeti Euroopa Liidu tasandil vastu välkmakseid käsitlev määrus (SEPA)[56], mille eesmärk on võimaldada teha rahaülekandeid kümne sekundi jooksul ööpäevaringselt, sh väljaspool tööaega ja teise EL-i liikmesriiki.[57] Eestis pakkusid suuremad pangad välkmakseid juba mitu aastat enne selle määruse vastuvõtmist, kuid määrus ühtlustas vastava regulatiivse raamistiku Euroopa Liidu tasandil.[58] Euroala makseteenuse pakkujatele muutus 9. oktoobrist 2025 kohustuslikuks eurodes välkmaksete saatmise teenuse ja saaja kontrollimise teenuse pakkumine.[59] Saaja kontrollimise teenuse eesmärk on võimaldada enne makse tegemist kontrollida, kas makse saaja nimi vastab makse saaja unikaalsele tunnusele, näiteks IBAN-ile.

Välkmaksete laialdasem kasutamine on ühtlasi suurendanud pettuste riski, kuna see võimaldab kurjategijatel raha väga kiiresti edasi kanda.[60] Seejuures tuleb siiski rõhutada, et välkmaksed ega nende kiirus ei ole iseenesest pettuste põhjus.[61] Probleem seisneb selles, et maksete kiirus vähendab oluliselt aega pettuste avastamiseks ning makse peatamiseks enne nende vahendite edasikandmist petturite poolt.[62] Eesti Panga andmetel tehti 2024. aastal välkmaksete kaudu pettuseid 6 miljoni euro eest, mis moodustas 58% maksekorralduspettuste kogukäibest.[63] Euroopa Pangandusjärelevalve hinnangul on välkmaksete puhul pettuslike ülekannete risk koguni kümme korda kõrgem kui tavapäraste maksete puhul, mis toob eriti selgelt esile

[56] Euroopa Parlamendi ja nõukogu määrus (EL) 2024/886, 13. märts 2024, millega muudetakse määrusi (EL) nr 260/2012 ja (EL) 2021/1230 ning direktiive 98/26/EÜ ja (EL) 2015/2366 eurodes välkkreeditkorralduste osas (EMPs kohaldatav tekst). - ELT L, 2024/886, 19.3.2024, lk 1-21.
[57] Council of the European Union. Council adopts regulation on instant payments. 26.02.2024. - https://www.consilium.europa.eu/et/press/press-releases/2024/02/26/council-adopts-regulation-on-instant-payments/ (16.03.2026).
[58] Soosalu, T. Välkmakse saab normiks kogu euroalal. Eesti Pank, 03.02.2025. - https://www.eestipank.ee/blogi/valkmakse-saab-normiks-kogu-euroalal (19.03.2026).
[59] Euroopa Komisjon. Kiiremad ja turvalisemad eurovälkmaksed toimivad nüüd kogu euroalal. 09.10.2025. - https://estonia.representation.ec.europa.eu/uudised/kiiremad-ja-turvalisemad-eurovalkmaksed-toimivad-nuud-kogu-euroalal-2025-10-09_et (21.03.2026).
[60] Eesti Pank. Maksepettuste ülevaade 2025, lk 13.
[61] *Ibid*, lk 12-13.
[62] Eesti Pangaliit. Pettuste ennetamine. - https://pangaliit.ee/pettuste-ennetamine (12.02.2026).
[63] Eesti Pank. Maksepettuste ülevaade 2025, lk 12-13.

vajaduse teostada tehinguseiret reaalajas, st enne maksetehingu täitmist, ning rakendada tõhusaid pettuste avastamise ja ennetamise meetmeid.[64] Eeltoodust järeldub, et maksejuhise täitmise etapil on lisaks tehnilisele tähendusele ka oluline roll pettuste ennetamisel, sest just siis peab makseteenuse pakkuja lisaks autentimisele hindama tehingu muid tingimusi ja vajaduse korral sekkuma enne vahendite edasikandmist.

Eesti õiguse tõlgendust tuleb kontrollida ka PSD2 regulatsiooni valguses, kuivõrd VÕS § 724[3] põhineb PSD2 artiklil 79. PSD2 artikli 79 lõike 1 kohaselt tuleb makseteenuse pakkujal maksekäsundi täitmisest või maksetehingu algatamisest keeldumise korral teavitada makseteenuse kasutajat keeldumisest ning võimaluse korral selle põhjustest ja keeldumise aluseks olnud vigade parandamise menetlusest, v.a juhul, kui selline teavitamine on keelatud muude asjakohaste Euroopa Liidu või siseriiklike õigusaktidega. Teade tuleb esitada või teha kättesaadavaks kokkulepitud viisil esimesel võimalusel ning igal juhul PSD2 artiklis 83 sätestatud tähtaja jooksul. Raamleping võib ette näha mõistliku tasu objektiivselt põhjendatud keeldumise eest. Magistritöö seisukohalt on oluline, et PSD2 artikkel 79 ei määra kindlaks keeldumise sisulisi aluseid ega täpsusta, kas objektiivselt põhjendatud pettusekahtlus võib iseseisvalt õigustada muidu tehniliselt korrektse ja lepingutingimustele vastava maksejuhise peatamist või täiendavat kontrolli.

Võrdlusena on asjakohane Norra finansavtaleloven § 4-6, mis reguleerib maksekorralduse täitmisest keeldumist. Sätte lõike 1 kohaselt ei või makseteenuse pakkuja, kui seadusest ei tulene teisiti, keelduda autoriseeritud maksekorralduse täitmisest, kui kõik lepingutingimused on täidetud. See kehtib sõltumata sellest, kas maksekorralduse on algatanud maksja ise, makse algatamise teenuse pakkuja kaudu, makse saaja või makse saaja kaudu tegutsev isik. Kui makseteenuse pakkuja siiski keeldub maksetehingu algatamisest või maksekorralduse täitmisest, peab ta lõike 2 kohaselt klienti sellest viivitamata ja kokkulepitud viisil teavitama ning märkima keeldumise põhjused ja võimalike vigade parandamise korra. Lõike 3 järgi ei käsitata keeldutud maksekorraldust kättesaadud maksekorraldusena täitmistähtaegade ega makseteenuse pakkuja täitmata, puuduliku või hilinenud täitmise eest vastutuse reeglite tähenduses.

[64] European Banking Authority. Opinion on new types of payment fraud and possible mitigations, European Banking Authority, 2024, lk 5 ja 10. – https://www.eba.europa.eu/sites/default/files/2024-04/363649ff-27b4-4210-95a6-0a87c9e21272/Opinion%20on%20new%20types%20of%20payment%20fraud%20and%20possible%20mitigations.pdf (02.04.2026).

Norra finansavtaleloven § 4-6 on sisuliselt võrreldav VÕS § 724[3] regulatsiooniga. Mõlema riigi õiguses on lähtekohaks, et makseteenuse pakkuja ei või autoriseeritud ja lepingutingimustele vastava maksejuhise täitmisest omal äranägemisel keelduda. Samuti näevad mõlemad regulatsioonid ette kliendi teavitamise kohustuse ning seovad õigustatud keeldumise tagajärje sellega, et keeldutud maksejuhist ei käsitata tavapärases tähenduses kättesaadud maksejuhisena. Erinevus seisneb eelkõige sõnastuses: Norra õigus kasutab üldist reservatsiooni „kui seadusest ei tulene teisiti", samas kui VÕS § 724[3] lõige 4 seob keeldumise võimaluse muu hulgas sellega, et maksejuhise täitmisega ei rikutaks mõnes muus õigusaktis sätestatud kohustust. Kumbki säte ei nimeta aga pettusekahtlust sõnaselgelt iseseisva keeldumise või täiendava kontrolli alusena.

eID omaja seisukohalt tähendab see, et ei Eesti ega Norra üldine maksejuhise täitmisest keeldumise regulatsioon lahenda üheselt olukorda, kus maksejuhis on tehniliselt korrektselt autenditud, kuid riskihinnang viitab sellele, et nõusolek võib olla saadud pettuse või manipuleerimise teel. Sellisel juhul võib jääda ebaselgeks, kas makseteenuse pakkujal on piisav õiguslik alus makse peatamiseks või täiendavaks kontrolliks. See on eID omaja jaoks oluline, sest eriti välkmakse puhul, võib kahju realiseeruda enne, kui tehingu autoriseeritust või vastutuse jaotust jõutakse sisuliselt hinnata. Seetõttu ei näita Norra võrdlus, et Eesti kehtiv regulatsioon oleks Norra õigusest oluliselt kitsam või vähem kaitsev. Võrdlus Norra regulatsiooniga kinnitab seega, et tavapärane maksejuhise täitmisest keeldumise norm ei lahenda piisavalt selgelt eID-põhiste pettuste erijuhtumit, kus probleem ei seisne maksejuhise formaalses puuduses või lepingutingimustele mittevastavuses, vaid kahtluses, et tehniliselt korrektne maksejuhis ei väljenda maksja tegelikku ja teadlikku nõusolekut.

Eesti õiguses on regulatsiooni ebaselguse kõrvaldamiseks on välja töötatud võlaõigusseaduse ja krediidiasutuste seaduse muutmise seaduse eelnõu[65], mille eesmärk on tõhustada finantspettuste ennetamise ja tõkestamist, muuhulgas andes makseteenuse pakkujatele selge õigusliku aluse maksejuhise täitmisest keeldumiseks.[66] Seletuskirja kohaselt puudub kehtivas õiguses makseteenuse pakkujal selge õiguslik alus keelduda maksejuhise täitmisest olukorras, kus on põhjendatud kahtlus, et maksetehingu täitmiseks antud nõusolek on saadud andmete väärkasutamise, pettuse või maksja manipuleerimise teel. Probleem puudutab eelkõige

[65] Võlaõigusseaduse ja krediidiasutuste seaduse muutmise seadus (finantspettuste ennetamine ja tõkestamine) seletuskiri. - https://eelnoud.valitsus.ee/main/mount/docList/4fb857a3-e037-492d-9d32-7c88e95b4151#MSHX5Up3 (05.04.2026).
[66] *Ibid*, lk 2.

olukordi, kus makse on tehniliselt kinnitatud kliendi autentimisvahendiga, kuid klient on petuskeemi käigus eksitatud makset kinnitama, näiteks uskudes, et ta suhtleb pangaga, kuigi tegelikult suunab teda makset tegema pettur.[67] Sellisel juhul ei seisne probleem autentimistoimingu tehnilises korrektsuses, vaid selles, et makse kinnitamisele viinud nõusolek võib olla kujunenud pettuse või eksituse mõjul.

Eelnõuga lisatakse VÕS §-i 724^3 uus lõige 4^2, mis näeb ette õiguse turvameetmete täiendavaks rakendamiseks, kui makseteenuse pakkuja tehtud riskianalüüsi põhjal tekib kahtlus, et maksetehingu täitmiseks antud nõusolek on saadud andmete väärkasutamise, pettuse või maksja manipuleerimise teel.[68] Lisaks lisatakse VÕS §-i 724^3 uus lõige 4^3, mille järgi peab makseteenuse pakkuja välkmakse puhul hindama tehinguga seotud riske üldjuhul kümne sekundi jooksul, v.a juhul, kui vajalikuks osutub täiendav kontroll, mis tuleb läbi viia ilma ebamõistlike viivituseta. Vastutuse tasandil täiendatakse VÕS § 733^9 lõiget 3 selliselt, et makseteenuse pakkuja ei vastuta hilinenud täitmisest tekkinud kahju eest, kui täiendavate turvameetmete rakendamine viiakse läbi põhjendamatu viivituseta ning rakendamise aluseks on objektiivselt põhjendatud kahtlus, et maksetehingu täitmiseks antud nõusolek on saadud andmete väärkasutamise, pettuse või maksja manipuleerimise teel. Samas tuleb arvestada, et tegemist on seaduseelnõuga, mis ei ole käesoleva magistritöö kirjutamise ajal veel jõustunud, mistõttu ei ole võimalik kindlalt ette näha, millisel kujul kavandatavad muudatused lõplikult vastu võetakse.

Eelnõu tähendus seisneb selles, et see nihutab maksejuhise täitmise regulatsiooni üksnes formaalselt kontrollilt riskipõhisema lähenemise suunas. Kui kehtiva õiguse järgi võib jääda ebaselgeks, kas tehniliselt korrektse ja lepingutingimustele vastava maksejuhise täitmist saab põhjendatud pettusekahtluse tõttu peatada, siis kavandatav regulatsioon annaks makseteenuse pakkujale sõnaselgema aluse sekkuda enne makse lõplikku täitmist. Sisuliselt tähendab see, et tehniliselt korrektne autentimine ei oleks enam iseenesest piisav põhjus makse viivitamatuks täitmiseks, kui riskianalüüs viitab sellele, et nõusolek võib olla saadud pettuse või maksja manipuleerimise teel. eID omaja seisukohalt tugevdaks see ennetavat kaitset just olukorras, kus makse on formaalselt korrektselt kinnitatud, kuid selle kinnitamiseni viinud tahe on kujunenud eksituse või manipulatsiooni mõjul. Eriti oluline on see välkmaksete puhul, kus makse täitmise kiirus jätab pettuse tuvastamiseks ja makse peatamiseks väga piiratud aja.

[67] *Ibid*, lk 1.
[68] *Ibid*, lk 4-5.

Makseteenuse pakkujate jaoks eeldab muudatus, et tehinguseire ja riskihindamine toimiksid enne makse lõplikku täitmist. Seletuskirja kohaselt peavad makseteenuse pakkujatel olema tehinguseiremehhanismid, mis võtavad arvesse muu hulgas varastatud autentimisvahendeid, maksetehingu summat, teadaolevaid petuskeeme, pahavara tunnuseid ning tavapäratut seadme või tarkvara kasutust.[69] Seega annaks eelnõu riskianalüüsi tulemustele selgema õigusliku tähenduse. Kui makseteenuse pakkuja tuvastab põhjendatud pettusekahtluse, ei peaks ta piirduma üksnes tehniliselt korrektse makse täitmisega, vaid peaks makset täiendavalt kontrollima ja vajaduse korral selle täitmisest keelduma.

Sama arengusuunda kinnitab kavandatav PSR. PSR artikkel 50 laiendab makse saaja nime ja kordumatu tunnuse, näiteks IBAN-i, vastavuse kontrolli kreeditkorraldustele ning näeb ette, et maksjat tuleb võimalikust lahknevusest teavitada enne makse autoriseerimist. PSR artikkel 83 tugevdab tehinguseiremehhanisme, mis peavad võimaldama ennetada ja avastada võimalikke pettuse teel tehtavaid maksetehinguid, võttes arvesse muu hulgas makseteenuse kasutaja tavapärast käitumist, maksetehingu summat, makse saaja kordumatut tunnust, teadaolevaid petuskeeme, varastatud autentimisvahendeid ja tavapäratut seadme või tarkvara kasutust. Sama artikkel võimaldab teatud tingimustel jagada teiste makseteenuse pakkujatega pettusega seotud makse saaja kordumatuid tunnuseid. PSR artikkel 84 lisab sellele klientide hoiatamise ja töötajate koolitamise kohustused. Seega näitab PSR, et EL-i makseõigus liigub ennetavama mudeli poole, kus makseteenuse pakkuja roll ei piirdu makse tehnilise autendituse kontrollimisega, vaid hõlmab ka pettuseriski tuvastamist ja maandamist enne makse lõplikku täitmist.

Kokkuvõttes näitab maksejuhise täitmise regulatsioon, et eID-põhiste pettuste korral ei ole oluline üksnes maksetehingu autoriseerituse hilisem hindamine, vaid ka võimalus sekkuda enne makse lõplikku täitmist. Kehtiv VÕS § 724^3 ja selle aluseks olev PSD2 artikkel 79 ei anna piisavalt selget vastust olukorrale, kus maksejuhis on tehniliselt korrektne ja lepingutingimustele vastav, kuid riskianalüüs viitab, et nõusolek võib olla saadud pettuse või maksja manipuleerimise teel. Norra võrdlus kinnitab, et tavapärane maksejuhise täitmisest keeldumise norm ei lahenda seda erijuhtumit oluliselt selgemalt. Seetõttu on Eesti kavandatava eelnõu ja PSR reformisuuna keskne tähendus selles, et maksejuhise täitmise etappi käsitatakse üha enam ennetava riskikontrolli hetkena. eID omaja seisukohalt võib selline lähenemine

[69] Võlaõigusseaduse ja krediidiasutuste seaduse muutmise seadus (finantspettuste ennetamine ja tõkestamine) seletuskiri, lk 3-4.

tugevdada kaitset eriti välkmaksete puhul, kus kahju võib realiseeruda enne, kui autoriseerituse või vastutuse küsimust jõutakse sisuliselt hinnata.

2. VASTUTUS AUTORISEERIMATA MAKSETE KORRAL eID KASUTAMISEL

2.1. MAKSETEENUSE PAKKUJA VASTUTUS JA TÕENDAMISKOORMIS

2.1.1. MAKSETEENUSE PAKKUJA VASTUTUS

Makseteenuse pakkuja vastutus autoriseerimata maksete korral tuleneb Eesti õiguses VÕS § 733^2 lõikest 2, mille esimene lause näeb ette, et autoriseerimata makse puhul tuleb maksja makseteenuse pakkujal tagastada maksesumma maksjale viivitamata, kuid mitte hiljem kui autoriseerimata maksest teadasaamisele järgneval arvelduspäeval. VÕS § 733^2 lõige 1 täpsustab, et autoriseerimata makse eest ei ole maksja makseteenuse pakkujal õigust nõuda maksjalt makse tegemisega seotud tasu ega kulutuste hüvitamist. VÕS-i kommenteeritud väljaande kohaselt väljendab see säte makseteenuse pakkuja üldvastutust autoriseerimata maksete korral.[70]

Eesti õiguse süsteemis tähendab VÕS § 733^2 seda, et autoriseerimata maksetehingu korral lasub esmane tagastamiskohustus makseteenuse pakkujal. See ei tähenda siiski, et kahju jääks igal juhul lõplikult makseteenuse pakkuja kanda. Kui esinevad VÕS § 733^8 kohaldamise eeldused, võib makseteenuse pakkuja hiljem tugineda maksja vastutusele, näiteks juhul, kui maksja on tegutsenud pettuslikult, tahtlikult või raske hooletusega. Seega tuleb eristada ühelt poolt makseteenuse pakkuja esmast tagastamiskohustust VÕS § 733^2 alusel ja teiselt poolt võimalust kanda kahju hiljem maksjale VÕS § 733^8 alusel.

Oluline on rõhutada, et vastutuse jaotuse analüüs sõltub esmalt sellest, kas kõnealune tehing kvalifitseerub autoriseerimata või autoriseeritud maksetehinguks. Kui tegemist on autoriseerimata maksetehinguga, st maksja ei ole andnud nõusolekut VÕS § 724^1 lõike 1 tähenduses, kohaldub VÕS § 733^2 alusel makseteenuse pakkuja tagastamiskohustus ning autoriseerituse tõendamise koormus lasub makseteenuse pakkujal. Kui aga tehing kvalifitseerub autoriseerituks, sh juhul, kui maksja kinnitas tehingu ise, kuid tegi seda manipulatsiooni mõjul, ei kohaldu autoriseerimata maksetehingute jaoks ette nähtud kaitsenormid. Sellisel juhul tuleb võimaliku vastutuse üle otsustada üldiste lepinguõiguslike või deliktiõiguslike normide alusel, mille rakendamise eeldused on oluliselt kitsamad.

Eesti regulatsiooni tuleb tõlgendada PSD2-st tulenevate põhimõtete valguses. VÕS § 733^2 on Eesti õiguses üle võetud PSD2 artiklist 73, mille lõige 1 näeb ette, et autoriseerimata

[70] Ulp, M. VÕS § 733^2, komm 2 ja 3.

maksetehingu korral peab maksja makseteenuse pakkuja tagastama autoriseerimata maksetehingu summa viivitamata ja igal juhul hiljemalt järgmise tööpäeva lõpuks alates tehingu teadasaamisest või sellekohase teate saamisest. Erandina võib makseteenuse pakkuja viivitamatust tagastamisest kõrvale kalduda juhul, kui tal on mõistlik põhjus kahtlustada maksja pettust ning ta teavitab sellest kirjalikult asjakohast riigiasutust. Kui see on asjakohane, peab makseteenuse pakkuja taastama debiteeritud maksekontol olukorra, mis oleks olnud juhul, kui autoriseerimata maksetehingut ei oleks toimunud, ning tagama, et krediteerimise väärtuspäev ei oleks hilisem summa debiteerimise kuupäevast.

PSD2 artikli 73 mõte on tagada, et autoriseerimata makse korral taastatakse maksja olukord kiiresti ning makseteenuse pakkuja ei lükkaks tagastamist edasi üksnes maksja hooletuse või raske hooletuse kahtluse tõttu. Viivitamatu tagastamise edasilükkamine on lubatud üksnes juhul, kui makseteenuse pakkujal on mõistlik põhjus kahtlustada pettust ja ta teavitab sellest pädevat asutust. See toetab VÕS § 733^2 tõlgendust, mille kohaselt tuleb autoriseerimata makse üldjuhul esmalt tagastada ning maksja võimalik vastutus tuleb vajaduse korral eraldi tuvastada VÕS § 733^8 alusel. eID omaja seisukohalt tähendab see, et kui eID abil kinnitatud makse osutub VÕS § 724^1 lõike 1 tähenduses autoriseerimata makseks, ei saa makseteenuse pakkuja tagastamist edasi lükata pelgalt viitega eID omaja võimalikule hooletusele autentimisvahendi kasutamisel. Kahju eID omaja kanda jätmiseks peab makseteenuse pakkuja tõendama VÕS § 733^8 kohaldamise eeldused.

Tagastamiskohustus on esmane ega sõltu sellest, kas makseteenuse pakkuja kahtlustab kliendi hooletust. Tarbijakaitse eesmärgist lähtudes peab makseteenuse pakkuja esmalt täitma viivitamatu tagastamise kohustuse ning alles seejärel võib ta nõuda maksjalt vastava kahju kandmist, kui ta suudab hilisemas vaidluses tõendada maksja tahtlust või rasket hooletust.[71] Seda põhimõtet kinnitab kohtujuristi ettepanek, mille kohaselt ei või makseteenuse pakkuja autoriseerimata maksetehingu summa viivitamatust tagastamisest keelduda üksnes põhjusel, et tal esineb kahtlus kliendi raske hooletuse osas.[72] Tuleb siiski arvestada, et tegemist on kohtujuristi ettepanekuga, mis ei ole Euroopa Kohtule siduv, kuid mida kohus praktikas sageli arvesse võtab. Kõnealuses kohtuasjas ei ole käesoleva töö kirjutamise seisuga veel otsust tehtud.

[71] EK C-70/25, *N. O. versus PKO BP S.A.,* ECLI:EU:C:2026:153, kohtujuristi A.Rantos ettepanek, p-d 26–27, 41 ja 46.
[72] C-70/25, *Tukowiecka*, kohtujuristi A. Rantos ettepanek p 17.

Norra õiguses tuleneb makseteenuse pakkuja vastutus autoriseerimata maksetehingu korral finansavtaleloven'i § 4-30 lõikest 1, mille järgi vastutab makseteenuse pakkuja kliendi ees autoriseerimata maksetehingust põhjustatud kahju eest, kui sama paragrahvi lõigetest 2–5 ei tulene teisiti. See regulatsioon lähtub samast põhimõttest nagu VÕS § 733[2] lõiked 2 ja 4: autoriseerimata makse korral on esmane vastutaja makseteenuse pakkuja, kuid seadus näeb ette erandid, mille korral võib kahju jääda maksja kanda. Norra õiguse eripära seisneb selles, et need erandid on seaduses selgemalt astmestatud.

Norra kohtupraktika kinnitab lisaks, et finansavtaleloven § 4-30 kohaldamise eelduseks on maksetehingu kvalifitseerimine autoriseerimata maksetehinguks. Norra kohus on rõhutanud, et kui tehing liigitub autoriseerituks, ei kohaldu finansavtaleloven § 4-30 tõendamiskoormise regulatsioon ning maksja peab tuginema eraldi hoolsuskohustuse rikkumisele, mille lävend on kõrge.[73] Sellise nõude lävend on kõrgem, sest vaidlus ei puuduta enam seda, kas maksetehing oli maksjale siduv, vaid seda, kas makseteenuse pakkuja rikkus makse täitmisel eraldiseisvat kohustust. eID omaja seisukohalt on see eristus oluline, sest tehniliselt korrektse eID-kinnituse korral võib vaidlus keskenduda just sellele, kas tegemist oli tegeliku nõusolekuga või pettuse mõjul tehtud autentimistoiminguga.

Norra kohtupraktikas on asjakohane ka varasemale finansavtaleloven'ile tuginev lahend, milles hinnati makseteenuse pakkuja eraldiseisvat hoolsus- ja sekkumiskohustust olukorras, kus autoriseerimata maksetehingute vastutuse regulatsioon ei kohaldunud. Komisjon ei pidanud makseteenuse pakkujat vastutavaks varasemate ülekannete eest, kuna maksjat oli hoiatatud ning tema enda kinnitused raskendasid pettuse tuvastamist. Küll aga vastutas makseteenuse pakkuja kahe hilisema ülekande eest, sest selleks ajaks viitasid asjaolud juba selgelt sellele, et maksja võib olla jätkuvalt pettuse ohver, kuid sarnaseid makseid teise maksekanali kaudu ei takistatud. Hüvitist vähendati 25% maksja enda kaasaaitamise tõttu.[74] Lahend näitab, et tehniliselt autoriseeritud makse ei välista makseteenuse pakkuja vastutust, kuid vastutus eeldab konkreetset alust pettust kahtlustada ja sekkuda.

Kavandatav PSR säilitab autoriseerimata maksetehingute puhul VÕS § 733[2] ja PSD2 artikliga 73 sarnase üldreegli. PSR artikli 56 lõike 1 kohaselt tuleb autoriseerimata maksetehingu summa maksjale tagastada viivitamata ja hiljemalt järgmise tööpäeva lõpuks. Tagastamist võib edasi

[73] Høyesterett. HR-2024-990-A, p 81. – https://lovdata.no/dokument/HRSIV/avgjorelse/hr-2024-990-a?q=HR-2024-990-A (14.04.2026).
[74] Finansklagenemnda Bank, FinKN 2026-5, 06.01.2026, Nordea Bank Abp, filial i Norge, „Investeringssvindel – omsorgsplikt – erstatningskrav", lk 9-12.

lükata üksnes juhul, kui makseteenuse pakkujal on mõistlik põhjus kahtlustada maksja pettust ning ta teavitab sellest kirjalikult asjakohast riigiasutust. PSR-i lisandväärtus võrreldes kehtiva VÕS § 733^2 lõikega 4 seisneb artikli 56 lõikes 2 sätestatud menetluslikus täpsustuses, mille kohaselt peab makseteenuse pakkuja pettusekahtluse korral kümne tööpäeva jooksul kas summa tagastama või esitama põhjenduse tagastamisest keeldumise kohta koos teabega vaidlustamisvõimaluste kohta. Seega ei muuda PSR autoriseerimata makse korral tagastamiskohustuse põhimõtet, kuid muudab maksjapoolse pettuse kahtluse erandi ajaliselt ja menetluslikult selgemaks.

PSR artikli 59 tähendus seisneb selle piiratud kohaldamisalas. Säte ei hõlma kõiki sotsiaalse manipulatsiooni või kehastamispettuse juhtumeid, vaid üksnes olukordi, kus pettur esineb makseteenuse pakkuja töötajana ja kasutab õigusvastaselt makseteenuse pakkuja nime, e-posti aadressi või telefoninumbrit. Piirang on põhjendatud, sest sellisel juhul põhineb pettus otseselt makseteenuse pakkuja identiteedi ja usaldusväärsuse ärakasutamisel ning makseteenuse pakkujal on paremad võimalused riski vähendada. Kui pettur esineb näiteks politsei või muu riigiasutuse esindajana, ei ole pettuse lähtepunkt makseteenuse pakkuja identiteedi kuritarvitamine. Seetõttu ei nihuta PSR artikkel 59 vastutust makseteenuse pakkujale iga kehastamispettuse korral, vaid üksnes tema enda identiteedi väärkasutuse juhtudel.

eID omaja jaoks tähendab see, et PSR artikkel 59 tugevdab kaitset eelkõige olukorras, kus ta kinnitab makse küll ise eID abil, kuid teeb seda ekslikus usus, et suhtleb oma pangaga. Sellisel juhul ei ole määrav üksnes tehniliselt korrektne autentimine, vaid ka see, et makse kinnitamiseni viis makseteenuse pakkuja identiteedi kuritarvitamine. Kui pettur esineb aga mõne muu isikuna, näiteks politsei või riigiasutusena, ei pruugi PSR artikkel 59 kohalduda ning eID omaja kaitse sõltub jätkuvalt üldistest autoriseerimise ja vastutuse reeglitest.

Kokkuvõttes on kehtiva õiguse lähtekoht see, et autoriseerimata makse korral lasub makseteenuse pakkujal kiire ja esmane tagastamiskohustus ning maksja võimalik vastutus tuleb hinnata eraldi VÕS § 733^8 alusel. eID-põhiste pettuste puhul ei pruugi see raamistik siiski anda piisavalt selget kaitset olukorras, kus makse on tehniliselt korrektselt autenditud, kuid eID omaja tegutses pettuse või manipulatsiooni mõjul. Sellised juhtumid võivad jääda autoriseeritud ja autoriseerimata makse piirile. PSR artikkel 59 parandaks eID omaja kaitset panga nimel esinemisega seotud pettuste korral, luues eraldi tagasimaksemehhanismi ka pettuse teel autoriseeritud maksetehingutele. Samas ei lahenda see kõiki sotsiaalse manipulatsiooni juhtumeid, vaid üksnes neid, mis mahuvad artikli 59 kohaldamisalasse.

2.1.2. MAKSETEENUSE PAKKUJA TÕENDAMISKOORMIS

Käesolevas alapeatükis hinnatakse, milliseid asjaolusid peab makseteenuse pakkuja tõendama, kui ta soovib VÕS § 733[8] alusel jätta autoriseerimata maksega seotud kahju täielikult või osaliselt maksja kanda, ning millised on selle tõendamiskoormise piirid.

Makseteenuse pakkuja jaoks on VÕS § 733[8] oluline eelkõige seetõttu, et see sätestab alused, mille esinemisel võib autoriseerimata maksega seotud kahju jääda täielikult või osaliselt maksja kanda. Lõike 1 kohaselt kannab maksja kahju piiratud ulatuses juhul, kui autoriseerimata makse on tehtud kadunud või varastatud makseinstrumenti kasutades või kui makseinstrumenti on kasutatud muul õigustamatul viisil. Maksja vastutus on sellisel juhul piiratud 50 euroga. Lõike 2 järgi ei kohaldu 50-eurone piirmäär aga juhul, kui tegemist on maksjapoolse pettusega või kui maksja on rikkunud oma kohustusi tahtlikult või raske hooletuse tõttu. Seega on makseteenuse pakkuja vastutusest vabanemise seisukohalt keskne küsimus, milliseid asjaolusid peab ta tõendama selleks, et tugineda maksja piiratud või täielikule vastutusele.

Tõendamiskoormise ulatuse hindamisel tuleb seega eristada kahte küsimust. Esiteks peab makseteenuse pakkuja suutma tõendada, et maksetehingu tegemisel kasutati kokkulepitud makseinstrumenti ja autentimisviisi. Teiseks peab ta juhul, kui ta soovib tugineda VÕS § 733[8] lõikele 2, tõendama ka maksja pettust, tahtlust või rasket hooletust. Seega ei saa makseteenuse pakkuja tõendamiskoormis piirduda pelgalt tehniliste logidega.

Õiguskirjanduses on osutatud, et PSD2 raamistik jätab liikmesriikide praktikas ruumi erinevatele tõendamisstandarditele, mistõttu on kohtupraktikas tekkinud lahknevusi selles, kas ja millises ulatuses tuleb makseteenuse pakkujal lisaks autentimislogidele esitada täiendavaid tõendeid.[75] Ühelt poolt toetab PSD2 artikli 72 lõige 2 järeldust, et makseteenuse pakkuja ei saa maksja vastutuse tõendamisel piirduda üksnes makseinstrumendi kasutamise dokumenteerimisega. Teisalt on vastukaaluks sellele õiguskirjanduses Hollandi kohtupraktika näitel märgitud, et makseteenuse pakkuja ei ole üldjuhul kohustatud iga autoriseeritud tehingut enne selle täitmist sisuliselt analüüsima, v.a õigusaktidest tulenevatest nõuetest, näiteks rahapesu tõkestamise eesmärgil.[76] Samuti on rõhutatud, et kui makseteenuse pakkujalt nõuda

[75] Van Praag jt, lk 4-5.
[76] Van Praag jt, lk 10-11.

iga vaidlustatud tehingu puhul detailse käitumusliku analüüsi tõendamist, võiks see praktikas eeldada oluliselt intensiivsemat tehinguseiret ja seeläbi riivata maksjate eraelu puutumatust.[77] Seetõttu tuleb autori hinnangul tõendamiskoormise ulatust piiritleda proportsionaalselt. Makseteenuse pakkuja tõendamiskoormis peaks ulatuma eelkõige nende konkreetsete asjaoludeni, mis on tema valduses või mõistlikult kättesaadavad ja millele ta maksja pettuse, tahtluse või raske hooletuse väitmisel tugineb. Sellised asjaolud võivad puudutada näiteks tehingu aega, summat ja saajat, kasutatud seadet või tavapärasest erinevat maksekäitumist. Küll aga ei peaks makseteenuse pakkujalt nõudma iga vaidlustatud makse puhul kogu kliendi varasema maksekäitumise ammendavat analüüsi ega kõigi võimalike pettusstsenaariumide välistamist. Selline nõue oleks liiga ebamäärane ning võiks praktikas viia ebaproportsionaalselt ulatusliku tehinguseireni.

Norra õiguse võrdlus toetab samuti järeldust, et makseinstrumendi tehnilise kasutamise fakt ei ole piisav maksja vastutuse tõendamiseks. Finansavtaleloven § 3-7 lõike 3 kohaselt ei piisa makseteenuse pakkuja juures registreeritud makseinstrumendi kasutamise faktist iseenesest selle tõendamiseks, et maksetehing oli kliendi poolt heaks kiidetud või et klient tegutses pettuslikult, tahtlikult või raske hooletusega. Tarbijate puhul läheb Norra õigus veelgi kaugemale, nähes finansavtaleloven § 3-7 lõikes 4 teatud asjaolude, sealhulgas tarbija nõusoleku ning pettusliku või tahtliku kohustuse rikkumise tõendamiseks ette kõrgema veenvusastme. Eesti õiguses sellist sõnaselget kõrgendatud tõendamisstandardit ei ole, kuid VÕS § 733[4] lõige 2 täidab sarnast funktsiooni ulatuses, milles välistab autentimislogide käsitamise iseseisvalt piisava tõendina.

Eesti õiguse seisukohalt tähendab Norra võrdlus, et VÕS § 733[8] kohaldamisel tuleb autentimislogisid hinnata koos muude asjaoludega. Kuigi eID kasutamise fakt võib olla oluline tõend, ei saa sellest automaatselt järeldada, et eID omaja tegutses pettuslikult, tahtlikult või raske hooletuse tõttu. Eriti oluline on see pettusejuhtumites, kus autentimissüsteem võib tehniliselt toimida veatult, kuid vaidlus puudutab seda, kas maksja käitumine oli konkreetseid asjaolusid arvestades niivõrd etteheidetav, et kahju tuleks jätta tema kanda.

Kavandatav PSR eelnõu tugevdab sama lähenemist. PSR artikli 55 lõige 2 sätestab sõnaselgelt, et makseinstrumendi kasutamise registreerimine, sealhulgas tugeva kliendi autentimise kohaldamine, ei ole iseenesest piisav tõendamaks, et maksetehing oli maksja poolt

[77] *Ibid*, lk 18.

autoriseeritud. See kinnitab VÕS § 733[4] lõike 2 loogikat ning muudab Euroopa Liidu tasandil selgemaks, et autentimisandmed on üks osa tõendikogumist, mitte lõplik tõend maksja nõusoleku või etteheidetava käitumise kohta.

PSR artikkel 83 ei ole otseselt tõendamiskoormise norm, kuid võib tõendamispraktikat kaudselt mõjutada. Säte kohustab makseteenuse pakkujaid rakendama tehinguseiremehhanisme pettuseriski avastamiseks ja ennetamiseks. Seetõttu võib PSR-i jõustumisel suureneda ootus, et makseteenuse pakkuja suudab vaidluse korral esitada tema valduses olevaid konkreetseid andmeid tehingu ebatavalisuse, teadaolevate petuskeemide, seadme kasutuse või muude riskinäitajate kohta. See ei tähenda siiski kohustust tõendada iga vaidlustatud maksetehingu täielikku käitumuslikku analüüsi.

Tõendamiskoormise seisukohalt on oluline ka PSR artikli 59 lõige 4, mille kohaselt peab makseteenuse pakkuja kehastamispettuse korral tõendama tarbija pettuse või raske hooletuse, kui ta soovib tagastamiskohustusest vabaneda. See kinnitab sama üldist suunda: olukorras, kus makseteenuse pakkuja soovib vältida kahju jäämist enda kanda, peab ta tõendama konkreetsed asjaolud, mis õigustavad kahju kandmist maksjale.

Kokkuvõttes tuleb VÕS § 733[8] kohaldamisel eristada kahte tõendamistasandit. Esiteks peab makseteenuse pakkuja tõendama makseinstrumendi kasutamise ja autentimisega seotud tehnilised asjaolud, sealhulgas seda, et kasutati kokkulepitud autentimisviisi. Teiseks peab ta juhul, kui soovib jätta kahju täielikult või osaliselt maksja kanda, tõendama VÕS § 733[8] kohaldamise eeldused, eelkõige maksja pettuse, tahtluse või raske hooletuse. eID kasutamise fakt ja autentimislogid võivad olla olulised tõendid, kuid neist ei piisa iseenesest maksja vastutuse tuvastamiseks.

Kehtiv õigus ei nõua makseteenuse pakkujalt iga vaidlustatud maksetehingu täieliku käitumusliku või riskianalüüsi tõendamist. Küll aga peab makseteenuse pakkuja esitama need konkreetsed tema valduses olevad andmed, millele ta maksja vastutuse väitmisel tugineb. Norra õiguse võrdlus ja PSR eelnõu toetavad sama üldist suunda: tehniline autentimine ei ole vastutuse jaotamisel lõplik tõend ning järjest olulisemaks muutub tehingu asjaolude, pettuseriski ja maksja käitumise sisuline hindamine.

2.2. eID OMAJA VASTUTUS JA ERANDID

2.2.1. eID OMAJA ÜLDINE VASTUTUS

Käesolevas alapeatükis käsitletakse eID omaja üldisi kohustusi makseinstrumendi ja isikustatud turvaelementide kasutamisel. Need kohustused moodustavad lähtekoha eID omaja võimaliku vastutuse hindamisel, sest autoriseerimata maksetehingu korral sõltub maksja vastutuse ulatus mh sellest, kas ta on täitnud makseinstrumendi kasutamise, turvaelementide hoidmise ja makseteenuse pakkuja teavitamise kohustust. Seetõttu analüüsitakse esmalt kohustuste sisu ning alles järgmistes alapeatükkides nende rikkumise tagajärgi piiratud või piiramatu vastutuse vormis.

Digitaalsete finantsteenuste ja eID vahendite toimimine eeldab, et eID omaja täidab teatud tehnilisi ja käitumuslikke hoolsuskohustusi. eID vahendite eripära seisneb selles, et autentimiseks kasutatav seade ja selle kasutamist võimaldavad isikustatud turvaelemendid, sealhulgas PIN-koodid, on üldjuhul eID omaja valduses ja kontrolli all. Seetõttu on eID omaja käitumisel oluline roll selles, kas kolmandal isikul on võimalik makseinstrumenti või selle kasutamist võimaldavaid andmeid väärkasutada.

Maksja peamised kohustused seoses makseinstrumendi, sh eID vahendite omamise ja kasutamisega, on Eesti õiguses sätestatud VÕS §-s 733^{10}. VÕS § 733^{10} punkti 1 kohaselt on makseinstrumendi omaja kohustatud kasutama makseinstrumenti vastavalt selle väljastamise ja kasutamise tingimustele ning tegema alates makseinstrumendi saamisest kõik vajaliku, et hoida makseinstrument ja selle kasutamist võimaldavad abivahendid kaitstuna. VÕS-i kommenteeritud väljaandes märgitakse, et makseinstrumendi omaja peab arvestama võimalusega, et makseinstrumendi või selle kasutamiseks vajalike abivahendite, näiteks PIN-koodide, kaotamise või varastamise korral võivad kolmandad isikud kasutada makseinstrumendiga seotud kontol olevaid rahalisi vahendeid või krediidilimiiti ning tekitada seeläbi kahju.[78] Seetõttu peetakse mõistlikuks käitumiseks seda, et makseinstrumendi omaja ei jäta makseinstrumenti ega selle turvaelemente järelevalveta, ei avalda neid kolmandatele isikutele ega talleta neid kergesti äratuntavas vormis.[79]

Hoolsuskohustuse oluline osa on ka makseteenuse pakkuja teavitamine. VÕS § 733^{10} punkti 2 kohaselt peab makseinstrumendi omaja pärast teadasaamist viivitamata teavitama

[78] Ulp, M. VÕS § 733^{10}, komm 3.2.1.
[79] *Ibid.*

makseinstrumendi väljastanud makseteenuse pakkujat või tema määratud kolmandat isikut makseinstrumendi kadumisest, vargusest ning autoriseerimata või valest kasutamisest. Teavitamiskohustuse eesmärk on võimaldada makseteenuse pakkujal kiiresti sekkuda, näiteks makseinstrument blokeerida. Mida kiiremini eID omaja reageerib ja autentimisvahendid blokeerib, seda tõhusamalt täidab ta kahju suurenemise vältimisele suunatud hoolsuskohustust. Teavitamisega viivitamine võib seevastu kujutada endast iseseisvat hoolsuskohustuse rikkumist.

Eesti kohtupraktika on eID vahendite hoidmise kohustust käsitlenud eelkõige digitaalallkirja andmise kontekstis. Kuigi viidatud praktika ei puuduta otseselt autoriseerimata maksetehingut, on see käesoleva alapeatüki jaoks asjakohane osas, milles see aitab sisustada eID omaja üldist hoolsuskohustust. Riigikohus on leidnud, et kuna ID-kaardi ja selle PIN-koodide abil on võimalik anda omakäelise allkirjaga samasuguse õigusliku tähendusega digitaalallkiri, lasub ID-kaardi omanikul selle hoidmisel kõrge hoolsuskohustus.[80] Kohus tõi analoogia volituse andmisega, leides, et kui isik annab digitaalse allkirja andmise vahendid vabatahtlikult kolmanda isiku valdusesse, võtab ta endale riski, et kolmas isik võib tegutseda antud piiridest väljaspool.[81] Magistritöö seisukohalt kinnitab lahend, et eID vahendite ja PIN-koodide hoidmise kohustus ei ole üksnes tehniline turvanõue, vaid õiguslikult oluline hoolsuskohustus. Seda, millise vastutuse sellise kohustuse rikkumine konkreetsel juhul kaasa toob, tuleb hinnata eraldi rikkumise raskust ja juhtumi asjaolusid arvestades.

Euroopa Liidu tasandil tuleneb makseinstrumendi kasutaja hoolsuskohustuse alus PSD2 artiklist 69, mille lõike 1 kohaselt peab makseteenuse kasutaja kasutama makseinstrumenti kooskõlas selle väljastamise ja kasutamise tingimustega ning teavitama makseteenuse pakkujat liigse viivituseta makseinstrumendi kaotamisest, vargusest või autoriseerimata kasutamisest. Lisaks kohustab PSD2 artikkel 69 lõige 2 makseteenuse kasutajat astuma kohe pärast makseinstrumendi kättesaamist kõik vajalikud sammud isikustatud turvavolituste turvaliseks hoidmiseks. Seega vastab VÕS § 733[10] sisuliselt PSD2 artiklis 69 sätestatud kohustustele. Nii siseriikliku kui ka Euroopa Liidu regulatsiooni eesmärk on tagada, et makseinstrumendi kasutaja rakendaks mõistlikke abinõusid oma isikustatud turvaelementide kaitsmiseks ning võimaldaks makseteenuse pakkujal väärkasutuse korral kiiresti sekkuda.

[80] RKTKo 16.12.2019, 2-16-124450/77, p 23.
[81] *Ibid*, p-d 23-24.

Euroopa Kohus on selgitanud, et maksjal lasub seejuures kahetasandiline teavitamiskohustus: makseteenuse pakkujat tuleb teavitada põhjendamatu viivituseta pärast autoriseerimata tehingu avastamist ning igal juhul hiljemalt 13 kuu jooksul alates debiteerimisest.[82] See tähendab, et 13-kuuline tähtaeg on lõpptähtaeg ega anna maksjale õigust jääda pärast tehingust teadasaamist passiivseks, vaid pärast tehingu avastamist tuleb tegutseda põhjendamatu viivituseta.

Norra õiguses on eID omaja hoolsuskohustused sätestatud finansavtaleloven §-s 3-19. Sätte lõike 1 kohaselt peab isik, kellel on õigus kasutada finantsteenuse lepingu sõlmimiseks elektroonilist allkirja, kasutama elektroonilise allkirja loomise andmeid vastavalt nende väljastamise ja kasutamise tingimustele ning rakendama kohe pärast andmete saamist kõiki mõistlikke ettevaatusabinõusid nendega seotud isikustatud turvateabe kaitsmiseks. Samuti peavad väljastamise ja kasutamise tingimused olema objektiivsed, mittediskrimineerivad ja eesmärgiga proportsionaalsed. Lõike 2 järgi peab õigustatud isik elektroonilise allkirja loomise andmete väärkasutusest teada saades teavitama sellest teenusepakkujat või allkirja väljastajat põhjendamatu viivituseta määratud korras. Lõige 3 seob teavitamiskohustuse rikkumise vastutuse piiramisega: õigustatud isik kaotab õiguse tugineda §-s 3-20 sätestatud vastutuse piiramisele, kui ta ei teavita väärkasutusest põhjendamatu viivituseta pärast sellest teadasaamist või hiljemalt 13 kuu jooksul ajast, mil ta oleks pidanud väärkasutusest aru saama. Kui teenusepakkuja ei ole aga andnud õigustatud isikule tehingu või lepingu kohta seaduses nõutavat asjakohast teavet, ei kao vastutuse piiramise õigus enne 13 kuu möödumist väärkasutusest teadasaamisest.

Norra regulatsioon on sisult sarnane VÕS § 733^{10} punktides 1 ja 2 sätestatud makseinstrumendi kasutamise, turvaelementide kaitsmise ja teavitamise kohustustega, kuid seob need otsesemalt eID ja elektroonilise allkirja loomise andmete väärkasutuse riskiga. Kuigi Eesti säte on sõnastatud üldisemalt, tuleb ka eID omaja hoolsust hinnata objektiivse mõistliku isiku standardi, mitte absoluutse hoolsuse alusel. Seega ei saa eID omajalt nõuda igasuguse pettuse ärahoidmist, vaid üksnes kasutustingimuste järgimist, turvaelementide kaitsmist, väärkasutuse kahtlusest viivitamata teavitamist ja olukorras mõistlike ettevaatusmeetmete rakendamist. See toetab juhtumipõhist hindamist, sest pelk eID tehniline kasutamine ei tõenda veel kohustuste rasket rikkumist.

[82] EKo 13.03.2025, C-665/23, IL v Veracash SAS, p 41–45.

Kavandatav PSR ei muuda eID omaja üldiste hoolsuskohustuste põhisisu. PSR artikkel 52 säilitab PSD2 artikliga 69 sarnase loogika, nähes punktis PSR artikli 52 punktis a ette makseteenuse kasutaja kohustuse kasutada makseinstrumenti kooskõlas selle väljastamise ja kasutamise tingimustega ning pärast makseinstrumendi kättesaamist peab makseteenuse kasutaja tegema kõik vajalikud toimingud oma isikustatud turvavolituste turvaliseks hoidmiseks. PSR artikli 52 punkti b kohaselt tuleb makseteenuse kasutajal teavitada makseteenuse pakkujat või makseteenuse pakkuja määratud üksust põhjendamatu viivituseta, kui ta on saanud teadlikuks makseinstrumendi kadumisest, varastamisest, väärkasutamisest või autoriseerimata kasutamisest. Eesti õiguse seisukohalt ei too PSR selles küsimuses kaasa sisulist muudatust, kuivõrd VÕS § 733[10] näeb samad põhikohustused juba ette.

Eeltoodust tuleneb, et eID omaja üldist vastutust ei saa mõista absoluutse vastutusena igasuguse eID väärkasutuse eest. eID omajal lasub küll kõrge hoolsuskohustus, kuna eID vahendite abil on võimalik teha õiguslikult siduvaid toiminguid, kuid selle kohustuse rikkumist tuleb hinnata konkreetse juhtumi asjaolude põhjal. Oluline ei ole üksnes see, kas eID vahendit või PIN-koode kasutati, vaid ka see, kas eID omaja järgis mõistlikult eeldatavaid ettevaatusabinõusid, kas tal oli võimalik väärkasutuse ohtu ära tunda ning kas ta teavitas makseteenuse pakkujat võimalikust väärkasutusest õigeaegselt. PSD2, PSR ja Norra õiguse võrdlus toetab sama lähtekohta: eID omaja kohustused on küll ranged, kuid need peavad jääma proportsionaalseks ja juhtumipõhiselt hinnatavaks. Seega tuleb eID omaja üldist hoolsuskohustust mõista kõrge, kuid proportsionaalse kohustusena, mille rikkumise tagajärjed sõltuvad järgnevates alapeatükkides analüüsitavast rikkumise raskusest.

2.2.2. PIIRATUD OMAVASTUTUS AUTORISEERIMATA MAKSETE KORRAL

Käesolevas alapeatükis analüüsitakse VÕS § 733[8] lõikest 1 tulenevat piiratud omavastutust olukorras, kus eID omaja on autoriseerimata maksetehinguga seoses rikkunud oma hoolsus- või teavitamiskohustust hooletusest, kuid tema käitumine ei ulatu raske hooletuse, tahtliku rikkumise ega pettuseni. Sellisel juhul on maksja vastutus piiratud 50 euroga ning ülejäänud kahju jääb üldreeglina makseteenuse pakkuja kanda.

Eesti õiguses on piiratud omavastutuse keskseks normiks VÕS § 733[8] lõige 1, mille kohaselt kannab maksja autoriseerimata maksetehingust tulenevat riisikot juhul, kui makse on tehtud kadunud või varastatud makseinstrumenti kasutades või kui makseinstrumenti on kasutatud

muul õigustamatul viisil. Maksja vastutus on sellisel juhul piiratud makseinstrumendi väljastajaga kokkulepitud piirsumma ulatusega, kuid mitte rohkem kui 50 euroga. Kui eID omaja käitumine kvalifitseerub raskeks hooletuseks, tahtlikuks kohustuste rikkumiseks või pettuseks, ei kohaldu VÕS § 733[8] lõike 2 alusel 50-eurone piirmäär. Seetõttu sõltub piiratud omavastutuse praktiline tähendus eelkõige sellest, kuidas eristatakse tavapärast hooletust raskest hooletusest.

Piiratud omavastutus väljendab tarbijakaitselist riskijaotust, mille kohaselt kannab maksja väikese osa kahjust juhul, kui talle saab ette heita makseinstrumendi või isikustatud turvaelementide ebapiisavat kaitsmist, kuid rikkumine ei ole piisavalt raske, et õigustada kogu kahju tema kanda jätmist. VÕS kommenteeritud väljaande kohaselt on selle lähtekoha aluseks arusaam, et tarbijalt ei saa nõuda maksevahendite kasutamisel ebaproportsionaalselt kõrgeid turvameetmeid, sest see kahjustaks makseteenuste kasutusmugavust ja muudaks kasutaja kohustused ülemääraseks.[83]

Piiratud omavastutuse tegelik kaitsefunktsioon sõltub sellest, kuidas eristatakse tavapärast hooletust raskest hooletusest. Seetõttu ei tohiks 50-eurose piiri välistamine toimuda üksnes eID tehnilise kasutamise, PIN-koodi sisestamise või autentimistoimingu fakti alusel; raske hooletuse sisuline piiritlemine on järgmise alapeatüki keskne küsimus.

Eeltoodud lähtekohta toetab ka Eesti kohtupraktika. Riigikohus on leidnud, et ID-kaardi PIN-koodide üleskirjutamine ja nende hoidmine kodus teistele pereliikmetele kättesaadavas kohas võib küll olla hooletu, kuid ei tähenda iseenesest rasket hooletust. Lahendis oli oluline, et ID-kaarti ja PIN-koode hoiti eraldi, märkmikus ei olnud märgitud, et tegemist on ID-kaardi PIN-koodidega, ning kolmas isik pidi koodide leidmiseks isiku asju korduvalt ja süstemaatiliselt läbi otsima. Samuti ei pidanud isik ette nägema elukaaslase sihipärast ebausaldusväärset käitumist, kui varasem käitumine ei andnud selliseks eelduseks alust.[84] Lahend näitab, et vastutuse astme hindamisel ei piisa üksnes turvaelementide ebapiisava hoidmise tuvastamisest, vaid hinnata tuleb ka nende seostatavust makseinstrumendiga, leitavust ja väärkasutuse ettenähtavust.

VÕS § 733[8] põhineb PSD2 artiklil 74, mis reguleerib maksja vastutust autoriseerimata makse korral. Artikli 74 lõike 1 kohaselt võib maksja vastutus kadunud, varastatud või väärkasutatud

[83] Ulp, M. VÕS § 733[8], komm 3.2.
[84] RKTKo 3-2-1-23-15, p 15.

makseinstrumendi korral olla piiratud kuni 50 euroga. See vastutus on välistatud, kui maksja ei olnud väärkasutusest enne makse tegemist teadlik, välja arvatud pettuse korral, või kui kahju tulenes makseteenuse pakkuja töötaja, agendi, filiaali või tegevuse edasiandmisel kaasatud isiku tegevusest või tegevusetusest. 50-eurone piirmäär ei kohaldu juhul, kui maksja on tegutsenud pettuslikult või rikkunud artiklist 69 tulenevaid kohustusi tahtlikult või raske hooletuse tõttu. Lisaks välistab artikkel 74 maksja vastutuse üldjuhul olukorras, kus makseteenuse pakkuja ei nõudnud tugevat kliendi autentimist või kahju tekkis pärast seda, kui maksja oli väärkasutusest teavitanud. Seega vastab Eesti regulatsioon üldjoontes PSD2 artikli 74 riskijaotusele.

PSD2 artikli 74 ülevõtmisel vähendati ka Eesti õiguses VÕS § 733[8] alusel maksja omavastutuse ülemmäära varasemalt 150 eurolt 50 eurole. Seletuskirja kohaselt oli muudatuse eesmärk piirata maksja rahalist riski autoriseerimata maksetehingute korral.[85] Selline lahendus väljendab riskijaotust, mille järgi ei peaks juhuslikest olukordadest või tavapärasest hooletusest tulenev kahju jääma valdavalt tarbija kanda. Eriti seetõttu, et makseteenuse pakkujad kujundavad makseteenuste tehnoloogilise ülesehituse ning otsustavad, milliseid autentimis- ja turvameetmeid teenuse kasutamisel rakendatakse. Õiguskirjanduses on samamoodi rõhutatud, et PSD2 seob maksja ulatuslikuma vastutuse selgemalt tema süü astme ja makseteenuse pakkuja kohustustega.[86] Samas ei kao maksja finantsrisk täielikult, sest raske hooletuse korral võib tema vastutus olla piiramatu. Seetõttu sõltub 50-eurose omavastutuse tegelik funktsioon sellest, kui kitsalt või laialt sisustatakse raske hooletuse mõistet.

Piiratud omavastutuse riskijaotuslik põhjendus seisneb selles, et autoriseerimata makse kahju ei ole tavalise hooletuse korral üksnes eID omaja isiklik eksimus, vaid ka digitaalse maksekeskkonna pettuseriski realiseerumine. Kuna petturilt kahju tagasisaamine on praktikas sageli keeruline, tuleb hinnata, kas see risk peab jääma tarbija või finantsasutuse kanda. Kui eID omaja ei ole tegutsenud raskelt hooletult ega tahtlikult, on põhjendatud piirata tema

[85] Võlaõigusseaduse ja teiste seaduste muutmise seaduse eelnõu seletuskiri, lk 64, p 6.3.11. – https://www.koda.ee/sites/default/files/content-type/content/2017-02/SELETUSKIRI_I_ring_01_0_0.pdf (14.01.2026).
[86] Steennot, R. Reduced payer's liability for unauthorized payment transactions under the second Payment Services Directive (PSD2). – Computer Law & Security Review 2018/34(4), lk 959–960. - https://www.sciencedirect.com/science/article/pii/S0267364918301924?via%3Dihub (17.03.2026)

vastutus seaduses sätestatud omavastutusega, et süsteemne pettuserisk ei kanduks ebaproportsionaalselt üksikule tarbijale.[87]

PSD2 raamistik ei anna siiski ammendavaid kriteeriume selleks, millal tuleb eID omaja käitumist pidada tavapäraseks hooletuseks ja millal raskeks hooletuseks. See piir jääb suuresti siseriikliku õiguse ja kohtupraktika kujundada. Eesti õiguses võib see tekitada teatavat ebakindlust, sest VÕS § 733[8] ei sisalda näidisloetelu asjaoludest, mis viitaksid tavapärasele hooletusele või raskele hooletusele. Samas on juhtumipõhine hindamine vajalik, kuna eID väärkasutuse ja sotsiaalse manipulatsiooni olukorrad võivad olla väga erinevad. Euroopa Kohus on selgitanud, et vastutuse jaotuse hindamisel tuleb arvestada kõiki asjaolusid kogumis, sealhulgas tehingu konteksti ja pettuse veenvust - mis viitab, et raske hooletuse mõistet ei tohi sisustada pelgalt PIN-koodi sisestamise või autentimistoimingu fakti põhjal.[88]

Norra õiguse võrdlus näitab, et piiratud vastutuse süsteemi on võimalik kujundada astmelisemalt. Uue finantsavtaleloven'i ettevalmistavatest materjalidest nähtub, et PSD2 ülevõtmisel lähtuti selgelt tarbijakaitselisest riskijaotusest, mille kohaselt on autoriseerimata maksete korral lähtekohaks makseteenuse pakkuja vastutus, maksja piiratud omavastutus ning erikaitse olukorras, kus teenuse pakkuja ei nõua tugevat kliendi autentimist.[89] Finansavtaleloven § 3-20 lõike 2 kohaselt on eID-vahendite väärkasutuse korral eID omaja vastutus hooletuse korral piiratud 450 Norra krooniga. Olulisem kui summade võrdlus on aga see, et Norra õigus seob vastutuse sõnaselgelt ka ettenähtavuse kriteeriumiga: eID omaja ei vastuta isegi nimetatud piiratud ulatuses, kui väärkasutus ei olnud talle ette nähtav ja ta ei tegutsenud pettuslikult.

Norra õiguses on eID-vahendite väärkasutuse korral vastutuse jaotus finansavtaleloven § 3-20 lõigetes 2–5 üles ehitatud selge astmelise süsteemina. Hooletuse korral on eID omaja vastutus piiratud 450 Norra krooniga ning see vastutus puudub, kui väärkasutus ei olnud talle ette nähtav. Raske hooletuse korral on vastutuse ülempiir 12 000 Norra krooni (ligikaudu 1000

[87] Kjørven, M.E. 'Who Pays When Things Go Wrong? Online Financial Fraud and Consumer Protection in Scandinavia and Europe', (2020), 31, European Business Law Review, Issue 1, pp. 77-109. - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3583369 (19.02.2026)

[88] EKo 13.03.2025, C-665/23, IL v Veracash SAS, p 41–45.

[89] Prop. 92 LS (2019–2020). Act on Financial Agreements (Financial Agreements Act) and consent to the approval of the EEA Joint Committee's decisions no. 125/2019 and 130/2019 of 8 May 2019 on the incorporation into the EEA Agreement of Directive 2014/17/EU on credit agreements for consumers relating to residential immovable property (the Mortgage Loan Directive) and Commission Delegated Regulation (EU) No. 1125/2014 . Ministry of Justice and Public Security. - https://www.regjeringen.no/no/dokumenter/prop.-92-ls-20192020/id2700119/ (06.04.2026).

eurot), kui kahju tekkis seetõttu, et eID omaja rikkus raskelt hooletult § 3-19 sätestatud kohustusi. Täielik vastutus on ette nähtud üksnes tahtliku kohustuste rikkumise korral. Lisaks välistab § 3-20 lõige 5 eID omaja vastutuse kahju eest, mille on põhjustanud teenusepakkuja ise või tema nimel tegutsev isik; selles osas on Norra lahendus sisuliselt võrreldav VÕS § 733[8] lõikes 4 sätestatud põhimõttega. Käesoleva alapeatüki seisukohalt on oluline eelkõige see, et Norra õiguses on piiratud omavastutus paigutatud selgelt astmelisse vastutussüsteemi, kus maksja rahalise vastutuse ulatus sõltub rikkumise raskusest ja väärkasutuse ettenähtavusest.

Norra lahendus kinnitab seega, et piiratud omavastutuse eesmärk ei ole panna tarbijat vastutama igasuguse väärkasutuse eest, vaid üksnes olukordades, kus talle saab ette heita makseinstrumendi või isikustatud turvaelementide ebapiisavat kaitsmist. Eesti õiguses täidab sarnast funktsiooni VÕS § 733[8] lõikes 1 sätestatud 50-eurone piirmäär. Erinevus seisneb selles, et Norra regulatsioonis on ettenähtavuse kriteerium ja vastutuse astmed seaduse tasandil sõnaselgemalt väljendatud, samas kui Eesti õiguses tuleb need tuletada hoolsuskohustuse üldisest sisust, VÕS § 733[10] kohustustest ja VÕS § 733[8] eesmärgipärasest tõlgendamisest. Eesti õiguses kujuneb piiratud omavastutuse ja ulatuslikuma vastutuse vaheline piir seetõttu suurel määral kohtupraktika kaudu, mis võib muuta õigusliku olukorra eID omaja jaoks vähem ettenähtavaks.

Hooletuse ja raske hooletuse vahelise piiri illustreerimiseks võib võrdlevalt Norra kohtupraktikale. Kuigi tegemist oli tarbijakrediidilepingu, mitte otseselt maksetehinguga, on lahend käesolevas kontekstis asjakohane, sest see käsitles BankID kasutamist autentimisvahendina ning finantsasutuse enda riskivaliku tähendust kliendi hooletuse hindamisel. Kaasuses varastas endine töötaja kliendi BankID koodigeneraatori, mis asus kontoris lukustamata sahtlis, ning võttis kliendi nimel tarbimislaenu.[90] Norra Ülemkohus leidis, et kuigi klienti sai kritiseerida koodigeneraatori ebapiisava turvamise eest, ei olnud tema käitumisest tulenev risk piisav kahju hüvitamise vastutuse tekkimiseks.[91] Oluline oli ka see, et Easybank otsustas sõlmida ulatusliku lepingu üksnes BankID-põhise identifitseerimise alusel, tegemata täiendavaid kontrolle.[92]

Eeltoodud Norra kohtulahendit ei saa Eesti makseõigusesse automaatselt üle kanda, kuid võrdleva argumendina toetab see seisukohta, et autentimisvahendi ebapiisav kaitsmine või selle

[90] Norra Ülemkohus (*Høyesterett*), HR-2020-2021-A, 22.10.2020, p-d 3 ja 76.
[91] *Ibid*, p 103.
[92] HR-2020-2021-A, p 104.

sattumine kolmanda isiku valdusesse ei peaks iseenesest välistama piiratud omavastutuse kohaldamist. Hinnata tuleb ka seda, kas kahju tekkimisele aitas kaasa finantsasutuse enda riskivalik või ebapiisav kontrolliprotsess. Selline lähenemine on kooskõlas piiratud omavastutuse eesmärgiga, mille kohaselt ei tohiks tavalise hooletuse korral tehnilise autentimise fakt muuta tarbijat kogu kahju kandjaks.

Norra õiguse kõige olulisem lisandväärtus võrreldes Eesti kehtiva regulatsiooniga seisneb finansavtaleloven § 3-21 sätestatud vastutuse vähendamise võimaluses. Kuigi seda mehhanismi käsitletakse põhjalikumalt järgmises alapeatükis, on selle tähendus piiratud omavastutuse kontekstis selles, et ka seaduses ette nähtud vastutuse määra ei käsitata täielikult jäigana. Sätte kohaselt võib § 3-20 lõigetes 2 ja 3 ette nähtud eID omaja vastutust vähendada, kui see on konkreetse juhtumi asjaolusid arvestades mõistlik. Hinnata tuleb eelkõige väärkasutusega seotud isikustatud turvaelementide iseloomu, väärkasutamise toimepanemise asjaolusid ning teenusepakkuja võimalikku hooletust või muid kahju tekkimisele kaasa aidanud asjaolusid. Eesti õiguses puudub selline eraldi sõnaselge vastutuse vähendamise alus, mistõttu saab sarnase tulemuse saavutamine tugineda pigem üldpõhimõtetele, eelkõige hea usu põhimõttele, või vastutuse astme juhtumipõhisele hindamisele.

Kavandatav PSR säilitab piiratud omavastutuse põhimõtte. PSR artikli 60 lõike 1 kohaselt võib maksja olla kohustatud kandma autoriseerimata maksetehingust tulenevat kahju kuni 50 euro ulatuses, kui kahju tuleneb kadunud või varastatud makseinstrumendi kasutamisest või makseinstrumendi omastamisest. Eesti õiguse seisukohalt ei too see kaasa põhimõttelist muudatust, kuna VÕS § 733^8 lõige 1 näeb sama 50-eurose piirmäära juba ette.

Kokkuvõttes on 50-eurone omavastutuse piir mõeldud katma olukordi, kus eID omajale saab ette heita makseinstrumendi või isikustatud turvaelementide ebapiisavat kaitsmist, kui tema käitumine jääb tavapärase hooletuse tasemele. Piiratud omavastutuse eesmärk on vältida seda, et juhuslikust või kergemast hooletusest tulenev väärkasutuse risk kanduks valdavas ulatuses tarbijale. Eesti õiguses on piiratud omavastutuse ja ulatuslikuma vastutuse piir vähem selgelt seaduses piiritletud kui Norra õiguses, mistõttu sõltub 50-eurose piiri praktiline tähendus eelkõige raske hooletuse mõiste sisustamisest. Seda küsimust käsitletakse järgmises alapeatükis.

2.2.3. PIIRAMATU VASTUTUS PETTUSE JA RASKE HOOLETUSE KORRAL

Kui eID omaja käitumine ületab tavapärase hooletuse taseme ning kvalifitseerub pettuseks, tahtlikuks kohustuse rikkumiseks või raskeks hooletuseks, ei kohaldu VÕS § 733[8] lõikes 1 sätestatud 50-eurone omavastutuse piir. Käesolevas alapeatükis analüüsitakse seetõttu piiramatu vastutuse eeldusi, eelkõige raske hooletuse mõistet ja selle tõendamist eID-põhiste pettuste kontekstis. Alapeatüki keskne küsimus on, millal võib eID omaja käitumist pidada sedavõrd etteheidetavaks, et autoriseerimata maksetehingust tekkinud kahju jääb täies ulatuses tema kanda.

eID omaja hoolsuskohustuse keskseks sisuks eID vahendite kasutamisel on isikustatud turvaelementide, sealhulgas PIN1 ja PIN2 koodide, saladuses hoidmine ning makseinstrumendi kasutamine selle väljastamise ja kasutamise tingimuste kohaselt, nagu on sätestatud VÕS § 733[10] lõikes 1. VÕS § 733[8] lõike 2 ei kohaldu 50-eurone omavastutuse piir juhul, kui autoriseerimata maksetehing on seotud maksja pettusega või kui maksja on makseinstrumendi kasutamisega seotud kohustusi rikkunud tahtlikult või raske hooletuse tõttu.[93] Eesti õiguses puudub raske hooletuse korral seadusjärgne vastutuse ülempiir, mistõttu võib raske hooletuse tuvastamine kaasa tuua kogu kahju kandmise maksja poolt.

Raske hooletuse mõiste tuleneb VÕS § 104 lõikest 4, mis defineerib raske hooletuse käibes vajaliku hoole olulise määral järgimata jätmisena. Riigikohus on mõistet sisustanud selliselt, et hooletuse ja raske hooletuse eristamine toimub objektiivsete kriteeriumide alusel: tuleb anda hinnang, kuidas oleks samal tegevusalal keskmine hoolas isik vastavas olukorras käitunud ning kas kahju tekkimine oli objektiivselt ettenähtav ja välditav.[94] Maksetehingute kontekstis tähendab see, et maksja käitumist tuleb hinnata selle põhjal, kuidas oleks samas olukorras käitunud mõistlik ja hoolas eID omaja.

Õiguskirjanduses on rõhutatud, et raske hooletuse mõistet tuleks sisustada kitsalt ja põhjendatult. Raske hooletus ei tohiks kujuneda laialt kasutatuks praktikaks, mille abil makseteenuse pakkuja saab iga pettusejuhtumi puhul vastutuse maksjale üle kanda. Samuti on õiguskirjanduses öeldud, et raske hooletus ei saa seisneda pelgas hoolsuskohustuse rikkumises. Raske hooletus eeldab tavalise hooletusega võrreldes oluliselt suuremat etteheidetavust ehk käitumist, mis väljendab märkimisväärset hoolimatust makseinstrumendi või isikustatud

[93] Ulp, M. VÕS § 733[8], komm 3.3.
[94] RKTKo 26.09.2006, 3-2-1-53-06, p 12.

turvaelementide kaitsmisel. Kui raske hooletus samastada iga olulise eksimuse või tehniliselt korrektse autentimistoiminguga, kaotaks piiratud omavastutuse regulatsioon suure osa praktilisest tähendusest ning autoriseerimata maksete kaitse muutuks tarbija jaoks näiliseks.[95] Seetõttu ei tohiks eID-põhiste pettuste puhul üksnes asjaolu, et petturil õnnestus saada ligipääs PIN-koodile või autentimisvahendile, automaatselt viia järelduseni, et eID omaja tegutses raskelt hooletult.

Kehtiv seadus ei loetle ammendavalt, milline käitumine kujutab endast rasket hooletust eID kasutamisel. PSD2 artikkel 74 jätab raske hooletuse täpse sisustamise suuresti siseriikliku õiguse ja kohtupraktika ülesandeks. Samas ei tähenda see, et raske hooletuse sisustamine võiks toimuda üksnes formaalsete tunnuste alusel. Raske hooletuse tuvastamiseks peab maksja käitumine oluliselt erinema sellest, mida võib mõistlikult eeldada keskmiselt hoolikalt makseinstrumendi kasutajalt.

Eesti kohtupraktikas ei ole raske hooletuse mõistet eID abil tehtud autoriseerimata maksete kontekstis seni sisuliselt käsitletud.[96] See tähendab, et raske hooletuse sisustamisel ei saa tugineda väljakujunenud siseriiklikule makseteenuste kohtupraktikale, vaid lähtuda tuleb VÕS § 733[8] eesmärgist, PSD2 süsteemist ning õiguskirjanduses kujundatud arusaamast, et raske hooletus eeldab tavalise hooletusega võrreldes oluliselt suuremat etteheidetavust. Seetõttu ei tohiks VÕS § 733[8] lõike 2 kohaldamisel keskenduda üksnes tehnilise kinnitustoimingu tegemisele, vaid hinnata tuleb tehingu konteksti, pettuse veenvust, eID omaja tegelikku arusaama ning seda, kas tema käitumine kaldus konkreetseid asjaolusid arvestades oluliselt kõrvale mõistlikult oodatavast hoolsusest. Asjakohane võib olla ka see, kas makseteenuse pakkujal oli konkreetsete ohumärkide põhjal võimalik pettust tuvastada või selle realiseerumist takistada.

Euroopa Kohus on rõhutanud, et maksja vastutuse hindamisel tuleb arvesse võtta kõiki konkreetse juhtumi asjaolusid kogumis. eID-põhiste pettuste puhul tähendab see, et raske hooletuse tuvastamine ei saa põhineda üksnes PIN-koodi sisestamise või autentimistoimingu tehnilisel toimumisel. Hinnata tuleb ka pettuse toimepanemise viisi, tehingu konteksti,

[95] Braithwaite, J. Gross Negligence in Bank Payments Law. - Oxford Journal of Legal Studies 2026, lk 957-958. - https://academic.oup.com/ojls/advance-article/doi/10.1093/ojls/gqag002/8454854 (07.02.2026).

[96] eID väärkasutust on Eesti kohtupraktikas käsitletud võõra eID abil sõlmitud tarbijakrediidilepingute kontekstis, kuid need lahendid ei puuduta makseteenuste regulatsiooni ega VÕS § 733[8] lõike 2 kohast vastutust autoriseerimata maksetehingu eest. Seetõttu ei käsitleta neid käesolevas töös eraldi.

makseinstrumendi kasutamise tingimusi ning seda, kas maksja käitumine kaldus oluliselt kõrvale mõistlikult oodatavast hoolsusest.[97]

Norra kohtupraktika analüüsimisel tuleb arvestada, et osa alljärgnevatest lahenditest on tehtud enne 1. jaanuari 2023, st varasemalt kehtinud finansavtaleloven'i alusel. Varasema regulatsiooni kohaselt võis makseteenuse kasutaja raske hooletuse korral vastutada autoriseerimata maksetehingust tekkinud kahju eest ulatuslikumalt kui kehtiva õiguse järgi. Uue finansavtaleloven'i vastuvõtmisel peeti vajalikuks tarbija kaitset tugevdada ja vastutuse piire täpsustada, mistõttu ei saa varasema seaduse alusel tehtud lahendite tulemusi automaatselt üle kanda kehtivale Norra õigusele ega Eesti VÕS-ile. Samas on need lahendid võrdlevalt asjakohased osas, milles need aitavad sisustada raske hooletuse ja tahtliku kohustuse rikkumise piiri eID-vahendite väärkasutuse olukorras.

Esimeses Norra kohtupraktikas (mis tehti eelmise finansavtaleloven'i alusel) käsitleti juhtumit, kus maksja sisestas oma BankID kasutajanime ja parooli SMS-pettuse teel loodud võltslehele.[98] Kohus leidis, et maksja tegutses raske hooletusega, kuna ta jättis kontrollimata lehekülje autentsuse enne isiklike autentimisandmete sisestamist, hoolimata sellest, et BankID kasutustingimused keelavad seda selgesõnaliselt.[99] Kuna lahend tehti varasema seaduse alusel, jäi kahju kliendi kanda ulatuses, mis ei ole automaatselt ülekantav kehtiva Norra õiguse konteksti.[100] Lahend on siiski võrdlevalt oluline osas, milles see näitab, et isikustatud turvaelementide sisestamist kontrollimata keskkonda võib pidada raskeks hooletuseks ka siis, kui maksja ei mõistnud, et tegemist on pettusega.

Teises Norra Ülemkohtu lahendis (mis on samuti tehtud eelmise finansavtaleloven'i alusel) selgitati põhjalikumalt sotsiaalse manipulatsiooni teel toime pandud pettuse ning raske hooletuse ja tahtliku kohustuse rikkumise vahelist piiri. Kaasuses peteti eakat pensionäri telefoni teel andma oma BankID paroolid ja koodid isikutele, kes esinesid panga töötajatena ning väitsid, et kliendi konto on ohus.[101] Maksja andis koodid välja, kuna ta oli veendunud, et aitab pangal pettust ära hoida.[102] Norra Ülemkohus leidis, et kuigi klient rikkus BankID kasutustingimusi ja tegutses objektiivselt hinnates raske hooletusega, ei tegutsenud ta tahtlikult

[97] EKo 13.03.2025, C-665/23, IL v Veracash SAS, p 60-61.
[98] Agder lagmannsrett, LA-2021-136209, 07.01.2022, p-d 4-7.
[99] *Ibid*, p-d 38-39 ja 44-45.
[100] *Ibid,* p *50.*
[101] Norra Ülemkohus (*Høyesterett*), HR-2022-1752-A, 13.09.2022, p 4.
[102] *Ibid*, p 33.

kohustust rikkudes ning ta ei soovinud panka kahjustada ega mõistnud, et tegutseb oma kohustuste vastaselt, vaid uskus heas usus, et aitab panka pettuse tõkestamisel.[103] Seetõttu piirati kliendi vastutus raske hooletuse seadusjärgse ülemmääraga ning ülejäänud kahju jäi panga kanda.[104]

Samas kohtuasja varasemas lahendis analüüsiti põhjalikumalt tahtluse subjektiivset elementi. Kohus rõhutas, et finantsteenuste valdkonnas ei piisa tahtluse tuvastamiseks üksnes kohustuse objektiivsest rikkumisest. Vajalik on tuvastada, et klient oli teadlik sellest, et tema tegevus rikub kohustust, ning tegutses sellele vaatamata.[105] See eristus on oluline ka Eesti õiguse jaoks VÕS § 733[8] lõike 2 tõlgendamisel. Kui raske hooletus võib põhineda objektiivsel hoolsusstandardi olulisel rikkumisel, siis tahtlik kohustuse rikkumine eeldab kliendi teadlikkuse ja tahte sisulist hindamist.

Kolmandas Norra Ülemkohut lahendis (mis on tehtud kehtiva finansavtaleloven'i alusel), käsitleti olukorda, kus pangaklient avaldas oma BankID kasutajanime, parooli ja ühekordse koodi isikutele, kes esinesid politsei ja prokuratuuri esindajatena ning väitsid, et klient on seotud rahapesu uurimisega.[106] Norra Ülemkohus leidis, et klient tegutses raske hooletusega, kuna BankID kasutustingimused keelavad selgesõnaliselt autentimisandmete avaldamise kolmandatele isikutele ning see kohustus on elementaarne ega sõltu sellest, kelle esindajana andmeid küsiv isik esineb.[107] Samas rõhutas kohus, et raske hooletuse hindamisel tuleb arvesse võtta ka kliendi isiklikke asjaolusid, sealhulgas vanust, haridust ja üldist võimet mõista, et ükski ametiasutus ega pank ei tohiks kunagi kliendi autentimisandmeid küsida.[108]

Neljas näide Norra kohtupraktikast illustreerib tahtliku kohustuse rikkumise ja raske hooletuse vahelist piiri. Kaasuses langes pangaklient armastuspettuse ohvriks ning kandis petturile märkimisväärses ulatuses raha, avaldades talle ka oma BankID kasutajanime, isikliku parooli ja ühekordse koodi.[109] Kohus leidis, et klient oli teadlik kohustusest mitte avaldada BankID andmeid kolmandatele isikutele, sest pank oli teda sellest otseselt teavitanud ning oli

[103] *Ibid,* p-d 33 ja 50-51.
[104] HR-2022-1752-A*,* p-d 33 ja 51.
[105] *Eidsivating lagmannsrett*, LE-2021-70115, 27.11.2021, p-d 169–170 ja 176–177. Tegemist on sama asja apellatsioonikohtu lahendiga, mille peale esitati kassatsioonkaebus ning mille Norra Ülemkohus jättis HR-2022-1752-A lahendis rahuldamata.
[106] Norra Ülemkohus, HR-2024-990-A, 31.05.2024, p-d 4-7.
[107] *Ibid*, p-d 38-39.
[108] HR-2024-990-A, p-d 48-49.
[109] *Nord-Troms og Senja tingrett*, TNTS-2024-30271, 01.11.2024, p-d 14, 17 ja 18

väljendanud kavatsust kliendisuhte lõpetada, kui ülekanded jätkuvad.[110] Seetõttu leidis kohus, et kliendi käitumine liigitus tahtlikuks kohustuse rikkumiseks, mille korral kohaldus täielik vastutus.[111] Lahend eristub teise näitena toodud Norra kohtupraktikast just seetõttu, et viimases uskus klient heauskselt, et suhtleb pangaga ega mõistnud oma kohustuse rikkumist.

Norra kohtulahendeid ei saa Eesti õiguse tõlgendamisele otse üle kanda, kuna Norra ja Eesti vastutuse jaotuse reeglid erinevad, eelkõige raske hooletuse korral kohaldatava vastutuse ülempiiri poolest. Need lahendid on magistritöös kasutatavad üksnes võrdlusmaterjalina, näitamaks, kuidas eID-vahendite väärkasutuse juhtumites on eristatud rasket hooletust ja tahtlikku kohustuse rikkumist. Eesti õiguse seisukohalt jääb määravaks VÕS § 733^4 lõige 2, mille kohaselt ei tõenda makseinstrumendi kasutamise dokumenteerimine iseenesest maksja rasket hooletust. Seetõttu saab Norra praktika üksnes illustreerida, milliseid asjaolusid võib sotsiaalse manipulatsiooni olukorras arvesse võtta; lõplik hinnang peab aga tuginema VÕS § 733^8 lõike 2 kohaldamisele.

50-eurose omavastutuse piiri välistamine ei toimu automaatselt ning tõendamiskoormis lasub ka piiramatu vastutuse kontekstis makseteenuse pakkujal. VÕS § 733^4 lõike 2 kohaselt ei tõenda ainuüksi autentimisvahendi kasutamise dokumenteerimine iseenesest ei autoriseerimist ega maksja rasket hooletust. Makseteenuse pakkuja peab näitama, et kliendi käitumine kaldus oluliselt kõrvale sellest, mida mõistlik maksja samades tingimustes oleks teinud.

Norra õiguses on tõendamiskoormis piiramatu vastutuse kontekstis selgemalt reguleeritud. Finansavtaleloven § 3-7 lõige 3 sätestab, et makseteenuse pakkuja peab esitama dokumentatsiooni tõendamaks, et klient on tegutsenud pettuslikult, tahtlikult või raske hooletusega. Sama paragrahvi lõige 4 kehtestab tarbijate puhul teatud asjaolude tõendamiseks kõrgendatud veenvusastme. Eesti õiguses sellist sõnaselget kõrgendatud tõendamisstandardit ei ole, kuid VÕS § 733^4 lõike 2 eesmärgipärane tõlgendus PSD2 valguses toetab sisuliselt sama järeldust: üksnes autentimislogid ei ole piisavad tõendamaks rasket hooletust ega tahtlikku kohustuse rikkumist.

Raske hooletuse hindamisel on oluline arvestada ka makseteenuse pakkuja enda kohustuste täitmist. VÕS § 711 lõike 1 punkti 14 kohaselt on makseteenuse pakkuja kohustatud teavitama kliente makseteenuse osutamisega seotud andmete väärkasutamisest ning võimalikest

[110] *Ibid*, p 108.
[111] *Ibid*, p-d 166, 172 ja 178.

pettustest.[112] Kui makseteenuse pakkuja on teavitamiskohustuse täitnud üksnes vormiliselt ega ole klienti tegelikest riskidest sisuliselt teavitanud, ei saa kliendi käitumist hinnata teadmise põhjal, mida tal tegelikkuses ei olnud. Vastutuse jaotus peab seega olema proportsionaalne mõlema poole panusega.

Norra õiguse oluline eripära on finansavtaleloven § 3-21, mis võimaldab vähendada § 3-20 lõigetes 2 ja 3 ette nähtud eID omaja vastutust, kui see on konkreetse juhtumi asjaolusid arvestades mõistlik. Hinnata tuleb muuhulgas isikustatud turvaelementide iseloomu, väärkasutamise asjaolusid ning teenusepakkuja võimalikku hooletust või muud kahju tekkimisele kaasa aidanud asjaolu. Säte on eriti oluline sotsiaalse manipulatsiooni juhtumites, kus eID omaja on küll objektiivselt oma kohustusi rikkunud, kuid teinud seda pettuse mõjul. Eesti õiguses sellist eraldi vastutuse vähendamise alust ei ole, mistõttu saab sarnane tulemus tulla üksnes üldpõhimõtete või raske hooletuse juhtumipõhise sisustamise kaudu.

Kavandatav PSR tugevdab sama suunda, mille kohaselt ei piisa vastutuse jaotamisel üksnes tehnilisest autentimisest. PSR artikli 55 lõige 2 sätestab, et makseinstrumendi kasutamise registreerimine, sealhulgas tugeva kliendi autentimise kohaldamine, ei tõenda iseenesest, et maksetehing oli maksja poolt autoriseeritud, ega seda, et maksja tegutses pettuslikult või raske hooletusega. PSR artikkel 59 täiendab vastutuse välistamise süsteemi kehastamispettuste puhul, kuid selle kohaldamisala on piiratud makseteenuse pakkuja identiteedi kuritarvitamisega ning see ei hõlma kõiki sotsiaalse manipulatsiooni juhtumeid.

Raske hooletuse mõiste täpsustamise vajadust on tunnistatud ka PSR eelnõu ettevalmistamisega seotud aruteludes. Sidusrühmad on rõhutanud, et uus regulatsioon peaks sisaldama konkreetsemaid näiteid käitumisest, mis võib kvalifitseeruda raskeks hooletuseks.[113] Selliste näidetena on esile toodud eelkõige isikustatud turvaelementide, sealhulgas Smart-ID PIN-koodide teadlik jagamine kolmandatele isikutele, oma seadme või biomeetriliste andmete kasutamise võimaldamine autoriseerimata isikutele ning olukorrad, kus maksja kinnitab autentimise käigus maksetehingu, mille saaja või summa ei vasta ilmselgelt sellele, mida ta enda arvates teeb.[114] Selliste näidete väärtus seisneks eelkõige selles, et need vähendaksid

[112] Ulp, M. VÕS § 711, komm 3.14.
[113] European Commission. Impact Assessment accompanying the Proposal for a Payment Services Regulation. SWD(2023) 231 final, 28.06.2023, lk 47–49.
[114] Euroopa Komisjon. Impact Assessment, lk 47–49.

tõlgendusruumi olukordades, kus vastutuse ulatus sõltub hooletuse ja raske hooletuse piiri sisustamisest.

Autori hinnangul on põhjendatud kaaluda, kas Eesti õiguses peaks raske hooletuse korral maksja vastutusele kehtima seadusjärgne ülempiir. Sellise lahenduse kasuks räägib eelkõige asjaolu, et eID-põhistes pettustes võib hooletuse ja raske hooletuse piir olla ebaselge, samas kui VÕS § 733[8] lõige 2 toob raske hooletuse tuvastamisel kaasa väga järsu tagajärje: 50-eurone piir kaob ning kogu kahju võib jääda maksja kanda. Sotsiaalse manipulatsiooni juhtumites võib selline tulemus olla ebaproportsionaalne, kui klient tegutses küll objektiivselt hooletult, kuid heauskselt ja petturi loodud eksitavas olukorras.

Norra mudel näitab, et raske hooletuse korral vastutuse piiramine ei tähenda maksja vastutusest vabastamist. 12 000 Norra krooni suurune ülempiir säilitab kliendi isikliku vastutuse, kuid väldib kogu kahju kandumist kliendile olukorras, kus tema süü ei ulatu tahtluseni. Samas ei saa Norra lahendust üle võtta üksikute elementidena, sest vastutuse ülempiiri täiendavad seal vastutuse vähendamise võimalus ja kõrgem tõendamisstandard.

2.3. eID OMAJA VASTUTUSE VÄLISTAMINE

Eelnevates alapeatükkides käsitleti eID omaja vastutuse kujunemist ning olukordi, kus tema vastutus võib raske hooletuse, tahtliku kohustuste rikkumise või pettuse korral ulatuda üle 50-eurose piiratud omavastutuse. Käesolev alapeatükk käsitleb seevastu olukordi, kus eID omaja ei kanna autoriseerimata maksetehingust tulenevat kahju. Eelkõige analüüsitakse tugeva kliendi autentimise kohaldamata jätmist, pärast nõuetekohast teavitamist toimunud tehinguid ning olukordi, kus kahju tekkimine on seotud makseteenuse pakkuja enda kohustuste rikkumisega. Nende erandite eesmärk on suunata makseteenuse pakkujaid rakendama piisavaid turva- ja kontrollimeetmeid ning vältida olukorda, kus süsteemne risk kandub tarbijale üksnes tehnilistele formaalsustele tuginedes.[115]

Eesti õiguses on eID omaja vastutuse välistamise keskne säte VÕS § 733[8] lõige 4, mis näeb ette mitu alternatiivset alust, mille esinemisel eID omaja ei kanna autoriseerimata maksetehingust tulenevat riisikot. Esiteks on maksja vastutus välistatud juhul, kui makseteenuse pakkuja ei ole taganud VÕS § 733[11] lõike 1 punktis 3 sätestatud tasuta tehnilist

[115] Ulp, M. VÕS § 733[8], komm 3.5.

võimalust teatada makseinstrumendi kadumisest, vargusest või makseinstrumendi autoriseerimata või valesti kasutamisest. Teiseks ei kanna maksja kahju juhul, kui kahju põhjustas makseteenuse pakkuja või tema agendi tegevus või tegevusetus. Kolmandaks on vastutus välistatud juhul, kui maksja ei olnud enne autoriseerimata makse tegemist teadlik makseinstrumendi kaotusest või vargusest. Neljandaks ei kanna maksja kahju juhul, kui makseteenuse pakkuja ei nõudnud tugevat kliendi autentimist, välja arvatud juhul, kui maksja tegutses pettuse teel.

Käesoleva magistritöö kontekstis on nimetatud alustest keskse tähendusega eelkõige tugeva kliendi autentimise nõude rikkumine, sest eID-põhiste maksete puhul sõltub vastutuse jaotus sageli sellest, kas makseteenuse pakkuja on nõutud autentimis- ja turvameetmeid korrektselt rakendanud. Tegemist on ulatusliku vastutuse välistamise alusega, mis on otseses sõltuvuses makseteenuse pakkuja enda kohustuste täitmisest.[116] Sätte eesmärk on suunata tugeva kliendi autentimise rakendamata jätmisest tulenev risk makseteenuse pakkujale.[117]

Eraldiseisev vastutuse jaotuse alus on sätestatud VÕS § 733[8] lõikes 3, mis reguleerib olukorda pärast seda, kui maksja on nõuetekohaselt teavitanud makseteenuse pakkujat makseinstrumendi või selle turvaelementide kadumisest, vargusest või muul viisil kaotusest. Nimetatud sätte kohaselt lasub kõigi pärast teavitamist toimunud autoriseerimata tehingute eest vastutus täies ulatuses makseteenuse pakkujal. Selle sätte eesmärk on motiveerida makseteenuse pakkujaid viivitamata reageerima kliendi teavitusele ning tagama reaalajas toimivad tehingute peatamise süsteemid.[118]

VÕS § 733[8] lõike 3 kohaldamine eeldab kahe eelduse täitmist. Esiteks peab maksja olema täitnud teavitamiskohustuse nõuetekohaselt, st teavitanud makseteenuse pakkujat makseinstrumendi kadumisest, vargusest või autoriseerimata kasutamisest pärast sellest teadasaamist vastavalt VÕS § 733[10] punktile 2. Teiseks peavad sätte kohaselt vaidlustatud tehingud olema toimunud pärast teavituse jõudmist makseteenuse pakkujani. Mõlema eelduse täitmisel ei saa makseteenuse pakkuja tugineda maksja varasemale hooletusele nende tehingute osas, mis toimusid pärast teavitust. Sätte praktiline tähendus avaldub näiteks olukorras, kus maksja teavitab makseteenuse pakkujat maksevahendi kaotamisest või eID-vahendi võimalikust kuritarvitamisest, kuid makseteenuse pakkuja ei blokeeri vahendit või ei peata

[116] Ulp, M. VÕS § 733[8], komm 3.5; vt ka PSD2 art 74 lg 2.
[117] PSD2, põhjenduspunkt 72.
[118] Ulp, M. VÕS § 733[8], komm 3.4.3.

tehinguid piisavalt kiiresti. Sellisel juhul jääb pärast teavitust toimunud tehingutest tulenev kahju makseteenuse pakkuja kanda.

Eeltoodud vastutust välistavad alused sobituvad PSD2 üldise vastutussüsteemiga. PSD2 artikli 74 lõige 2 näeb ette, et juhul kui maksja makseteenuse pakkuja ei nõua tugevat kliendi autentimist, ei kanna maksja üldjuhul autoriseerimata maksetehingust tulenevat rahalist kahju, välja arvatud juhul, kui ta on toime pannud pettuse. Kui tugevat kliendi autentimist ei kasuta makse saaja või makse saaja makseteenuse pakkuja, peab ta hüvitama maksja makseteenuse pakkujale tekkinud kahju. Seega seob PSD2 tugeva kliendi autentimise nõude eelkõige makseteenuse pakkujate turva- ja vastutuskohustustega. Sellest ei saa aga teha vastupidist järeldust, et tehniliselt korrektne tugev autentimine oleks alati samastatav maksja tegeliku ja teadliku nõusolekuga konkreetse maksetehingu tegemiseks.

PSD2 süsteemi seisukohalt on oluline ka tagastamiskohustuse ja vastutuse välistamise vahekord. PSD2 artikkel 73 lõige 1 kohustab makseteenuse pakkujat tagastama autoriseerimata maksetehingu summa viivitamata ja hiljemalt järgmise tööpäeva lõpuks. See kohustus on kehtiva regulatsiooni lähtepunkt, kuid selle kõrval tuleb hiljem hinnata, kas esineb alus maksja vastutuseks või vastutuse välistamiseks. Seetõttu ei tohiks makseteenuse pakkuja raske hooletuse pelga kahtluse alusel automaatselt keelduda autoriseerimata makse summa tagastamisest.

Seda kinnitab ka kohtujuristi ettepanek Euroopa Kohtu asjas. Kohtujurist on asunud seisukohale, et makseteenuse pakkuja ei tohi keelduda autoriseerimata makse summa viivitamatust tagastamisest pelgalt seetõttu, et tal esineb kahtlus kliendi raske hooletuse osas. Teisisõnu on tagastamiskohustus esmane ning vastutuse jaotuse küsimus lahendatakse hilisemas etapis.[119] Siinkohal tuleb siiski rõhutada, et tegemist on kohtujuristi ettepanekuga, mitte Euroopa Kohtu siduva otsusega. Kõnealuses lahendis ei ole veel magistritöö kirjutamise seisuga kohtuotsust tehtud. Kohtujuristi seisukoht võib anda suunise PSD2 tõlgendamiseks ja selle alusel Eesti õiguspraktika kujundamiseks, kuid sellele ei saa tugineda sama kindlusega kui lõplikule kohtuotsusele.

Autori hinnangul tuleks kohtujuristi seisukohaga sisuliselt nõustuda. Esiteks toetab seda PSD2 artikli 73 lõike 1 sõnastus, mis kohustab makseteenuse pakkujat tagastama autoriseerimata

[119] C-70/25, *Tukowiecka*, kohtujuristi A. Rantos ettepanek p 17.

makse summa viivitamata ja hiljemalt järgmiseks tööpäevaks. Säte ei näe ette erandit üksnes raske hooletuse korral. Teiseks vastab see PSD2 süsteemsele loogikale, mille kohaselt lasub autoriseerimise ja maksja raske hooletuse tõendamise koormis makseteenuse pakkujal. Kolmandaks tagab selline tõlgendus, et tagastamiskohustuse erand piirdub üksnes põhjendatud pettusekahtlusega, mitte laiema raske hooletuse kahtlusega. Seega ei saa makseteenusepakkuja kasutada raske hooletuse kahtlust tagastamise peatamise alusena, v.a juhul, kui tal on põhjendatud kahtlus maksja enda pettuse kohta.

Võrdlus Norra õigusega näitab, et vastutuse välistamise alused võivad olla sõnastatud laiemalt kui Eesti õiguses. Norra õiguses on teavitamise roll vastutuse välistamisel sätestatud finansavtaleloven § 3-20 lõike 5 punktis a, mis on sisuliselt võrreldav VÕS § 733^8 lõikega 3. Norra regulatsioon sisaldab siiski olulist täiendust, millele Eesti õiguses otsene vaste puudub. Nimelt näeb finansavtaleloven § 3-19 lõige 3 ette, et eID omaja ei kaota kaitset üksnes seetõttu, et ta jättis teavitamiskohustuse täitmata, kui makseteenuse pakkuja ise ei ole täitnud oma kohustust edastada kliendile teavet tehtud tehingute kohta. Sellisel juhul saab vastutuse piirangule tugineda alles 13 kuu möödumisel ajast, mil eID omaja sai väärkasutusest teada, ning sedagi üksnes tingimusel, et makseteenuse pakkuja on oma tehingute teavitamise kohustuse nõuetekohaselt täitnud. See on eriti oluline sotsiaalse manipulatsiooni juhtumites, kus pettuse ohver ei pruugi kohe aru saada, et tema nimel on tehing tehtud, eriti juhul, kui makseteenuse pakkuja ei ole tehinguteavitusi korrektselt edastanud.

Norra õiguses on vastutuse välistamise alused sõnastatud mõnevõrra laiemalt. Finansavtaleloven § 3-20 lõige 5 välistab eID omaja vastutuse muu hulgas juhul, kui kahju on põhjustanud teenusepakkuja või tema nimel tegutsev isik, kui teenusepakkuja ei ole taganud väärkasutusest teavitamise võimalust, kui elektrooniline allkirjastamine ei olnud piisavalt turvaline või kui teenusepakkuja ei nõudnud tugevat kliendi autentimist. Eesti VÕS § 733^8 lõige 4 sisaldab sarnaseid konkreetseid välistamisaluseid, kuid Norra regulatsiooni eripära on üldisem riskijaotuslik alus, mis võimaldab arvestada, kas väärkasutuse risk peaks asjaolusid arvestades jääma teenusepakkuja kanda. eID omaja jaoks tähendab see, et Eesti õiguses sõltub vastutusest vabanemine rohkem sõnaselgelt nimetatud aluste esinemisest, samas kui Norra õigus võimaldab paindlikumat juhtumipõhist riskijaotust.

eID omaja jaoks tähendab see, et Eesti õiguses on vastutusest vabanemine tihedalt seotud VÕS § 733^8 lõikes 4 sõnaselgelt nimetatud alustega. Kui makseteenuse pakkuja on nõudnud tugevat kliendi autentimist, taganud teavitamisvõimaluse ning kahju ei ole otseselt põhjustatud

makseteenuse pakkuja või tema agendi tegevusest või tegevusetusest, on eID omaja vastutusest vabastamine keerulisem ning sõltub pigem hooletuse, raske hooletuse või pettuse hindamisest. Norra regulatsiooni puhul on eID omaja kaitse ulatus potentsiaalselt laiem, sest lisaks konkreetsetele välistamisalustele saab arvestada ka seda, kas asjaolud viitavad väärkasutuse riski jäämisele teenusepakkuja kanda. Seega on Eesti õiguses eID omaja jaoks keskne küsimus see, kas ta suudab näidata mõne VÕS § 733^8 lõikes 4 nimetatud konkreetse aluse esinemist, samas kui Norra õiguses on võimalik suurem rõhk panna ka juhtumi üldisele riskijaotusele.

Kavandatav PSR säilitab autoriseerimata maksetehingute vastutuse välistamise põhiloogika. Artikli 60 lõike 2 järgi ei kanna maksja kahju, kui makseteenuse pakkuja ei ole nõudnud tugevat kliendi autentimist, välja arvatud maksjapoolse pettuse korral. Artikli 60 lõige 4 välistab maksja vastutuse ka pärast makseinstrumendi kaotusest, vargusest või väärkasutusest teatamist ning juhul, kui makseteenuse pakkuja ei taga selleks sobivaid teavitamisvahendeid. Seega ei loo PSR Eesti õiguse seisukohalt sisuliselt uut vastutuse välistamise süsteemi, vaid koondab senised põhimõtted selgemalt vahetult kohaldatavasse määrusesse.

Töö seisukohalt on eraldi oluline PSR artiklis 59 kavandatav kehastamispettuse regulatsioon. See puudutab olukorda, kus tarbijat manipuleeritakse makseteenuse pakkuja identiteedi kuritarvitamise kaudu ning tarbija teeb makse ise. Kuigi säte ei hõlma kõiki sotsiaalse manipulatsiooni juhtumeid, näitab see reformisuunda: vastutuse hindamisel ei piirduta üksnes tehnilise autentimistoiminguga, vaid arvestatakse ka pettuse konteksti ja makseteenuse pakkuja ennetuskohustusi. eID maksete puhul toetab see järeldust, et PIN-koodi sisestamine ei tõenda iseenesest eID omaja vaba ja teadlikku tahet konkreetset maksetehingut teha. Kuna PSR ei ole veel lõplikult jõustunud, tuleb seda käsitada arengusuunana, mitte kehtiva õigusena.

Lisaks artiklis 60 sätestatud autoriseerimata maksetehingute vastutuse reeglitele on käesoleva töö seisukohalt oluline ka PSR artiklis 59 kavandatav kehastamispettuse eriregulatsioon. Nimetatud säte ei käsitle klassikalist autoriseerimata maksetehingut, vaid olukorda, kus tarbijat manipuleeritakse makseteenuse pakkuja identiteedi kuritarvitamise kaudu ning tarbija teeb makse pettuse mõjul ise. Artikli 59 tähendus seisneb selles, et vastutuse jaotamisel ei keskenduta üksnes tehnilisele autentimistoimingule, vaid arvestatakse ka pettuse konteksti ja makseteenuse pakkuja ennetuskohustusi. Samas on selle kohaldamisala piiratud ning see ei hõlma kõiki sotsiaalse manipulatsiooni juhtumeid.

Sama järeldust toetab ka pettuse mõjul tehtud maksekorralduste käsitlus, sest sellistes juhtumites on makse tehniliselt kinnitatud, kuid maksja tegutseb sotsiaalse manipulatsiooni mõjul.[120] Käesoleva magistritöö seisukohalt on see oluline ka eID abil kinnitatud maksete puhul: PIN-koodi sisestamise fakt ei näita iseenesest, et eID omaja tegi vaba ja teadliku otsuse konkreetse maksetehingu tegemiseks. Seega toetab PSR-i kehastamispettuse artikkel 59, et eID omaja vastutuse hindamisel tuleb lisaks tehnilisele autentimistoimingule arvestada ka pettuse konteksti ja makseteenuse pakkuja ennetuskohustusi.

PSR reformi 2025. aasta poliitilise kokkuleppe valguses tuleb neid muudatusi käsitada reformisuunana, mitte veel lõpliku kehtiva õigusena. Kokkuleppe kohaselt tugevdatakse makseteenuse pakkujate ennetavaid pettusetõrjekohustusi, sealhulgas saaja nime ja unikaalse tunnuse kontrolli, tehinguseire, kululimiitide ja blokeerimismeetmete kasutamist.[121] Käesoleva töö seisukohalt näitab see arengusuund, et vastutuse jaotuse raskuskese liigub üksnes maksja autentimistoimingult laiemale küsimusele, kas makseteenuse pakkuja rakendas piisavaid ennetus-, kontrolli- ja sekkumismeetmeid.

Samas ei tähenda makseteenuse pakkuja ennetavate kohustuste rõhutamine seda, et pank peaks iga maksetehingu puhul tegema põhjaliku käitumusliku analüüsi. Õiguskirjanduses on osutatud, et selline nõue võiks viia ebaproportsionaalselt ulatusliku tehinguseireni ning riivata maksjate eraelu puutumatust.[122] Seetõttu peaks makseteenuse pakkuja kohustus piirduma eelkõige tema valduses olevate konkreetsete riskinäitajate hindamisega, näiteks ebatavaline makse summa, uus saaja, uus seade, tavapärasest erinev maksekäitumine või hiljutised muudatused kliendi kontaktandmetes või autentimisvahendites. Selline lähenemine võimaldab arvestada makseteenuse pakkuja paremat positsiooni pettuseriski tuvastamisel, muutmata teda samas iga pettuse automaatseks kandjaks.

Autori hinnangul ei ole VÕS § 733[8] lõigete 3 ja 4 peamine probleem nende sätete sisus, vaid nende võimalikus liiga formaalses kohaldamises. Kui kahju tekkimist või suurenemist mõjutas makseteenuse pakkuja enda kohustuse rikkumine, ei tohiks eID omaja vastutust hinnata üksnes tema autentimistoimingu kaudu. Vastutust välistavaid aluseid tuleks tõlgendada koostoimes

[120] Wold, V. En kritisk oversikt over det privatrettslige forbrukervernet. – Kritisk juss 2024/2–4, lk 174. - https://opphevet.juridika.no/tidsskrifter/kritisk-juss/2024/2-4/artikkel/wold-59178?utm (07.03.2026)
[121] European Parliament. Payment services deal: More protection from online fraud and hidden fees. Press release, 27.11.2025. - https://www.europarl.europa.eu/news/en/press-room/20251121IPR31540/payment-services-deal-more-protection-from-online-fraud-and-hidden-fees (19.12.2025)
[122] European Parliament. Payment services deal: More protection from online fraud and hidden fees. Press release, 27.11.2025, lk 18.

makseteenuse pakkuja autentimis-, teavitamis- ja väärkasutuse tõkestamise kohustustega. Sellist lähenemist toetab ka Woldi käsitlus eraõiguslikust tarbijakaitsest, mille kohaselt peaks tarbijakaitse suunama professionaalsete turuosaliste käitumist, mitte piirduma üksnes konkreetse vaidluse tagantjärele lahendamisega.[123]

Samuti võiks kaaluda Norra finansavtaleloven § 3-19 lõike 3 eeskujul sõnaselget normi, mille kohaselt ei kaota maksja kaitset teavitamiskohustuse rikkumise tõttu juhul, kui makseteenuse pakkuja ise ei ole andnud talle nõuetekohast teavet tehingu kohta. Selline täpsustus oleks oluline eelkõige sotsiaalse manipulatsiooni juhtumites, kus ohver ei pruugi väärkasutusest aru saada, kui makseteenuse pakkuja teavitamissüsteem ei toimi nõuetekohaselt. Samas tuleb säilitada teavitamiskohustuse preventiivne tähendus, mistõttu ei tohiks selline erand kujuneda üldiseks vabanduseks kliendi passiivsusele.

Kokkuvõttes annavad VÕS § 733^8 lõiked 3 ja 4 eID omajale olulised vastutust välistavad kaitsemehhanismid olukordades, kus kahju tekkimine või suurenemine on seotud makseteenuse pakkuja enda kohustuste rikkumisega, tugeva kliendi autentimise nõudmata jätmisega või pärast nõuetekohast teavitamist toimunud väärkasutusega. Nende sätete praktiline tähendus sõltub aga sellest, kas neid tõlgendatakse üksnes formaalselt või arvestatakse ka makseteenuse pakkuja tegelikku rolli makseteenuse turvalisuse ja väärkasutuse tõkestamise korraldamisel. Samas ei tohi vastutuse välistamise aluseid tõlgendada nii laialt, et eID omaja hoolsuskohustus kaotaks praktilise tähenduse. Seetõttu peab tasakaal seisnema selles, et eID omaja vastutab oma hoolsuskohustuse rikkumise eest, kuid makseteenuse pakkuja kannab riski olukorras, kus kahju tekkimist mõjutas tema enda autentimis-, teavitamis- või väärkasutuse tõkestamise kohustuse rikkumine.

Autori hinnangul ei vaja VÕS § 733^8 lõiked 3 ja 4 vältimatult ümberkirjutamist, kui kohtupraktika tõlgendab neid eesmärgipäraselt. Kui praktika jääb aga liiga formaalseks, võiks kaaluda kahte täpsustust. Esiteks võiks VÕS § 733^8 lõike 4 kohaldamisala olla selgemalt piiritletud tugeva kliendi autentimise nõudmata jätmise korral, sest kliendilt ei saa mõistlikult eeldada makseteenuse pakkuja autentimissüsteemi tehnilise vastavuse hindamist. Teiseks võiks kaaluda Norra finansavtaleloven § 3-19 lõike 3 eeskujul normi, mille kohaselt ei kaota maksja kaitset teavitamiskohustuse rikkumise tõttu juhul, kui makseteenuse pakkuja ise ei ole

[123] Wold, V. En kritisk oversikt over det privatrettslige forbrukervernet. – Kritisk juss 2024/2–4, lk 181.

andnud talle nõuetekohast teavet tehingu kohta. Mõlemal juhul tuleb siiski säilitada eID omaja hoolsus- ja teavitamiskohustuse preventiivne tähendus.

KOKKUVÕTE

Käesoleva magistritöö eesmärk oli analüüsida, kuidas jaotub vastutus makseteenuse pakkuja ja eID omaja vahel olukorras, kus eID-d kasutatakse pettuse tulemusel makse tegemiseks, ning hinnata, kas kehtiv Eesti õigus tagab sellistes olukordades tasakaalustatud vastutuse jaotuse. Töö keskne probleem seisnes selles, milline õiguslik tähendus tuleb omistada eID abil tehtud tehnilisele autentimistoimingule juhul, kui maksja tegelik tahe konkreetset maksetehingut teha on pettuse või manipulatsiooni tõttu vaieldav.

Töö tulemusel selgus esmalt, et autoriseerimata makse eID kasutamise kontekstis ei ole määratletav üksnes selle järgi, kas maksetehing kinnitati tehniliselt nõuetekohase autentimisvahendiga. VÕS § 724^1 lõike 1 järgi on maksetehing autoriseeritud üksnes juhul, kui maksja on andnud selleks nõusoleku. eID kasutamine võib olla VÕS § 724^1 lõike 2 tähenduses poolte vahel kokku lepitud viis sellise nõusoleku väljendamiseks, kuid see ei tähenda, et iga tehniliselt korrektne autentimistoiming oleks automaatselt samastatav maksja materiaalõigusliku nõusolekuga. Seetõttu tuleb eID abil kinnitatud maksetehingu autoriseeritust hinnata kahel tasandil: ühelt poolt tuleb kontrollida, kas maksetehing kinnitati kokkulepitud tehnilise autoriseerimisviisi abil, ning teiselt poolt tuleb hinnata, kas eID omaja tegelik ja teadlik tahe oli suunatud just konkreetse maksetehingu tegemisele.

Selline eristus on eriti oluline pettuseolukordades. Kui pettur kasutab eID vahendeid eID omaja teadmata, puudub eID omaja tahteavaldus täielikult. Keerulisem on olukord siis, kui eID omaja sisestab PIN-koodi ise, kuid teeb seda pettuse mõjul, arvates näiteks, et ta kinnitab mõnda muud toimingut või takistab pettust. Sellisel juhul ei piisa autoriseerituse jaatamiseks sellest, et PIN-kood sisestati või tugev kliendi autentimine läbiti. Hinnata tuleb ka seda, kas maksja mõistis autentimistoimingu tegelikku tähendust, kas talle oli arusaadav kinnitatava makse summa ja saaja ning kas tema tahe oli suunatud maksetehingu tegemisele. Seega on tehniline autentimine oluline tõend, kuid see ei ole iseseisvalt piisav alus järeldamaks, et maksetehing oli maksja poolt autoriseeritud.

Nimetatud järeldusele jõuti VÕS § 724^1 ja § 724^6, TsÜS § 67 ning PSD2 artiklite 64, 97 ja 98 koosmõjus. VÕS § 724^1 ja PSD2 artikkel 64 reguleerivad maksja nõusolekut kui maksetehingu siduvuse materiaalõiguslikku eeldust. VÕS § 724^6 ning PSD2 artiklid 97 ja 98 reguleerivad aga tugevat kliendi autentimist kui elektrooniliste maksete turvalisuse nõuet. Nende sätete süsteemne eristamine näitab, et tugev autentimine võib olla nõusoleku väljendamise tehniline

viis, kuid ei asenda nõusoleku materiaalõiguslikku olemasolu. Sama toetab VÕS § 733[4] lõige 2, mille kohaselt ei tõenda makseinstrumendi kasutamise dokumenteerimine iseenesest ei maksetehingu autoriseerimist ega maksja pettust, tahtlust või rasket hooletust.

Kehtiva õiguse kohaselt lasub autoriseerimata maksetehingu korral esmane vastutus makseteenuse pakkujal. VÕS § 733[2] lõike 2 järgi peab makseteenuse pakkuja autoriseerimata maksetehingu summa maksjale viivitamata tagastama. See väljendab PSD2 tarbijakaitselist lähtekohta, mille kohaselt ei tohi autoriseerimata makse risk jääda esmalt tarbija kanda. Samas ei tähenda makseteenuse pakkuja esmane tagastamiskohustus, et kahju jääb alati lõplikult tema kanda. Kahju lõplik jaotus sõltub eID omaja käitumise etteheidetavuse astmest.

Kui eID omaja on rikkunud makseinstrumendi või isikustatud turvaelementide kasutamisega seotud kohustusi üksnes tavapärase hooletuse tõttu, piirdub tema vastutus VÕS § 733[8] lõike 1 järgi üldjuhul 50 euroga. Selline piiratud omavastutus väljendab tarbijakaitselist riskijaotust. Selle eesmärk on vältida olukorda, kus digitaalse maksekeskkonna juhuslik või süsteemne pettuserisk kandub valdavas ulatuses üksikule tarbijale. See on põhjendatud eelkõige seetõttu, et makseteenuse pakkuja kujundab autentimis- ja turvasüsteemid, kontrollib makseteenuse tehnilist ülesehitust ning on üldjuhul paremas positsioonis pettuseriske ennetama ja tuvastama.

Kui eID omaja tegutseb pettuslikult, rikub kohustusi tahtlikult või raske hooletuse tõttu, ei kohaldu 50-eurone vastutuse piir. Eesti õiguses puudub raske hooletuse korral seadusjärgne vastutuse ülempiir, mistõttu võib raske hooletuse tuvastamine tuua kaasa kogu kahju kandmise maksja poolt. Seetõttu on raske hooletuse mõiste sisustamine eID-põhiste pettuste puhul vastutuse jaotuse seisukohalt määrava tähtsusega. Töö tulemusel jõuti järeldusele, et rasket hooletust ei tohi samastada iga olulise eksimuse, PIN-koodi sisestamise või autentimistoimingu tehnilise toimumisega. Raske hooletus peab tähendama tavapärase hooletusega võrreldes oluliselt suuremat etteheidetavust.

Raske hooletuse hindamine peab olema juhtumipõhine. Arvesse tuleb võtta pettuse toimepanemise viisi, manipulatsiooni veenvust, maksjale autentimise hetkel kuvatud teavet, maksja tegelikku arusaama toimingu tähendusest ning seda, kas makseteenuse pakkujal oli konkreetsete riskisignaalide põhjal võimalik pettust tuvastada või selle realiseerumist takistada. VÕS § 733[4] lõige 2 toetab sellist lähenemist, sest välistab autentimisandmete dokumenteerimise käsitamise piisava tõendina raske hooletuse kohta. Seega peab

makseteenuse pakkuja eID-põhises vaidluses esitama lisaks autentimislogidele ka muid asjaolusid, millest nähtuks maksja käitumise tegelik raskusaste.

Töö tulemusel selgus ka, et eID omaja vastutus peab olema välistatud olukordades, kus kahju tekkimine või suurenemine on seotud makseteenuse pakkuja enda kohustuse rikkumisega. Sellisteks olukordadeks on eelkõige tugeva kliendi autentimise nõudmata jätmine, nõuetekohase teavitamisvõimaluse tagamata jätmine või tehingute toimumine pärast seda, kui maksja on makseteenuse pakkujat makseinstrumendi või eID-vahendi võimalikust väärkasutusest teavitanud. Nendes olukordades ei ole põhjendatud jätta kahju eID omaja kanda, sest tegemist on riskidega, mille maandamine kuulub eeskätt makseteenuse pakkuja kontrolli alla.

Norra õiguse ja kohtupraktika võrdlus näitas, et eID-vahendite väärkasutuse korral on vastutuse jaotust võimalik kujundada astmelisemalt kui Eesti õiguses. Norra õiguses eristatakse hooletuse korral piiratud vastutust, raske hooletuse korral kõrgemat, kuid siiski piiratud vastutust, ning täielikku vastutust tahtliku kohustuse rikkumise korral. Norra lahendeid ei saa Eesti õigusele otse üle kanda, sest vastutusreeglid on sisuliselt erinevad. Küll aga näitab Norra võrdlusmaterjalina, et eID-vahendite väärkasutuse puhul on oluline eristada objektiivset hoolsuskohustuse rikkumist ja kliendi teadlikku tahet kohustust rikkuda. Sama eristus on oluline ka Eesti õiguses, sest VÕS § 733^{8} lõike 2 kohaldamisel tuleb eristada rasket hooletust, tahtlikku kohustuse rikkumist ja pettust.

Töö autor ei järelda, et Eesti õiguses tuleks esmase lahendusena kehtestada Norra eeskujul raske hooletuse korral vastutuse ülempiir. Esmalt tuleks olemasolevat regulatsiooni tõlgendada sisulisemalt. Kohtupraktika peaks VÕS § 733^{4} lõike 2 ja VÕS § 733^{8} kohaldamisel vältima formaalset lähenemist, mille kohaselt PIN-koodi sisestamine või tehniliselt korrektne autentimine viib automaatselt maksja täieliku vastutuseni. Seadusandlik sekkumine oleks põhjendatud eelkõige juhul, kui kohtupraktika jääb liiga formaalseks või kui raske hooletuse tuvastamine toob praktikas ebaproportsionaalselt sageli kaasa kogu kahju kandmise tarbija poolt.

PSD3 ja PSR kavandatavad muudatused tugevdavad tarbijakaitselist suunda, kuid ei lahenda kõiki eID-põhiste pettustega seotud probleeme. PSR eelnõu kinnitab mitut juba kehtivast PSD2-st ja Eesti õigusest tulenevat põhimõtet: makseteenuse pakkuja viivitamatu tagastamiskohustus autoriseerimata maksetehingu korral, 50-eurone piiratud omavastutus ning

vastutuse välistamine juhul, kui makseteenuse pakkuja ei nõua tugevat kliendi autentimist või kui kahju tekib pärast maksja nõuetekohast teavitust. Uue regulatsiooni tähtsus seisneb eelkõige selles, et need põhimõtted koondatakse vahetult kohaldatava määruse tasandile ja muudetakse Euroopa Liidu üleselt ühtlasemaks.

PSR eelnõu kõige olulisem panus eID-põhiste maksete kontekstis seisneb autentimisandmete tõendusliku tähenduse täpsustamises. PSR artikli 55 lõige 2 sätestab sõnaselgelt, et makseinstrumendi kasutamise registreerimine, sealhulgas tugeva kliendi autentimise kohaldamine, ei tõenda iseenesest maksetehingu autoriseerimist ega maksja pettust või rasket hooletust. See põhimõte on sisuliselt kooskõlas VÕS § 733^4 lõikega 2, kuid PSR-i sõnastus muudab veel selgemaks, et ka edukalt läbitud tugev autentimine ei ole lõplik tõend maksja nõusoleku ega raske hooletuse kohta.

Oluline areng on ka PSR artiklis 59 kavandatav kehastamispettuse regulatsioon. See käsitleb olukorda, kus tarbija teeb makse ise, kuid teeb seda makseteenuse pakkuja identiteedi kuritarvitamise tõttu tekkinud eksimuse mõjul. Selline regulatsioon näitab, et Euroopa Liidu õiguse arengusuund ei keskendu enam üksnes sellele, kas maksja kinnitas tehingu tehniliselt ise, vaid arvestab ka pettuse konteksti ja makseteenuse pakkuja ennetuskohustusi. Samas on artikli 59 kohaldamisala piiratud, sest see ei hõlma kõiki sotsiaalse manipulatsiooni juhtumeid. Seetõttu ei kõrvalda PSR vajadust hinnata eID omaja nõusolekut ja vastutust juhtumipõhiselt ka üldiste autoriseerimise ja vastutuse reeglite alusel.

PSR ja PSD3 reformi laiem tähendus seisneb selles, et vastutuse jaotuse raskuskese liigub järk-järgult maksja üksikult autentimistoimingult makseteenuse pakkuja ennetus-, kontrolli- ja sekkumismeetmete poole. Kavandatavad reeglid saaja nime ja unikaalse tunnuse kontrolli, tehinguseire, limiitide ja blokeerimismeetmete kohta näitavad, et makseteenuse pakkujalt oodatakse aktiivsemat rolli pettuste ennetamisel. Samas peab selline kohustus jääma proportsionaalseks. Makseteenuse pakkuja ei peaks kandma automaatselt iga pettuse riski ega tegema iga maksetehingu puhul põhjalikku käitumuslikku analüüsi, kuid tal peab olema kohustus arvestada konkreetseid tema valduses olevaid riskinäitajaid.

Kokkuvõttes sisaldab kehtiv Eesti õigus eID omaja kaitseks olulisi mehhanisme, kuid nende tõhusus sõltub sellest, kas neid tõlgendatakse sisuliselt või formaalselt. Autoriseerimise tasandil tuleb eristada tehnilist autentimist ja tegelikku nõusolekut. Tõendamise tasandil ei tohi autentimislogisid käsitada iseseisvalt piisava tõendina. Vastutuse tasandil tuleb eristada

tavapärast hooletust, rasket hooletust, tahtlikku kohustuse rikkumist ja pettust. Vastutuse välistamise tasandil tuleb arvestada, kas kahju tekkimist mõjutas makseteenuse pakkuja enda kohustuse rikkumine.

Magistritöö keskne järeldus on, et eID kasutamise tehniline fakt ei tohiks üksi otsustada ei maksetehingu autoriseeritust ega eID omaja vastutust. Vastutuse jaotus peab sõltuma kolmest asjaolust: kas maksja tegelik tahe oli suunatud konkreetse maksetehingu tegemisele, milline oli tema käitumise etteheidetavuse aste ning kas makseteenuse pakkuja täitis talle pandud autentimis-, tõendamis-, teavitamis- ja pettusetõrjekohustused. PSD3 ja PSR kavandatavad muudatused liiguvad samas suunas, kuid ei asenda vajadust Eesti õiguse eesmärgipärase ja juhtumipõhise tõlgendamise järele.

LIABILITY OF THE eID HOLDER IN THE EVENT OF AN UNAUTHORISED PAYMENT

Summary

The use of electronic identity solutions has become an essential part of digital banking and payment services in Estonia. ID-card, Mobile-ID and Smart-ID are commonly used not only for identifying a person but also for accessing payment accounts, confirming payment orders and giving legally relevant declarations of intent. This creates a specific legal problem in fraud cases. A payment transaction may appear technically correct in the payment service provider's system because it has been confirmed by means of an eID solution and strong customer authentication. At the same time, the payer may claim that they did not have a genuine intention to make the payment, because the authentication act was performed as a result of fraud, manipulation or misuse of authentication credentials.

The central problem examined in this master's thesis is therefore whether the technical use of an eID solution is sufficient to conclude that a payment transaction was authorised and binding on the payer, or whether the payer's actual consent must be assessed separately. This issue is particularly important in social engineering fraud cases, where the payer may personally enter the PIN code or otherwise complete the authentication process, but does so under the influence of deception, for example believing that they are preventing fraud, confirming another operation or communicating with their bank.

The aim of this thesis is to analyse how liability is allocated between the payment service provider and the eID holder when an eID has been used as a result of fraud to initiate or confirm a payment transaction. The thesis seeks to determine whether the current Estonian legal framework provides a balanced allocation of risk and whether the forthcoming PSD3 and PSR framework may change or clarify that allocation.

The thesis addresses three research questions. First, it asks what an unauthorised payment means in the context of eID use and under what conditions a payment transaction confirmed by eID can be considered binding on the payer. Secondly, it analyses how liability is allocated under current law between the payment service provider and the eID holder when the payment has been made using the person's eID as a result of fraud. Thirdly, it examines how the proposed Payment Services Directive 3 and Payment Services Regulation may affect the allocation of liability between the eID holder and the payment service provider.

The thesis uses an analytical and comparative legal method. The analysis is based primarily on Estonian law, in particular the provisions of the Law of Obligations Act concerning payment services, authorisation of payment transactions, unauthorised payments, the payer's liability and the payment service provider's burden of proof. Since Estonian payment services law is based on the second Payment Services Directive, the relevant national provisions are interpreted in the light of PSD2. The thesis also analyses the proposed PSD3 and PSR framework. Norwegian law and case law are used as comparative material, because Norway has extensive experience with BankID-related fraud cases and has adopted a more detailed statutory model for allocating liability in cases involving misuse of electronic signature creation data. Norwegian law is not treated as a direct interpretative source for Estonian law, but as comparative material illustrating possible approaches to negligence, gross negligence and intentional breach in eID-related fraud cases.

The first conclusion of the thesis is that a payment transaction confirmed by eID cannot be regarded as authorised solely because the technical authentication process was successfully completed. Under Estonian law, a payment transaction is authorised only if the payer has given consent to its execution. The parties may agree on the manner and procedure for giving such consent, and eID may serve as the agreed technical means of expressing consent. However, the use of an authentication tool does not in itself replace the substantive legal requirement of consent. Consent requires a declaration of intent directed at bringing about the legal consequence of executing a specific payment transaction.

This distinction is particularly important in two types of fraud scenarios. In the first scenario, a fraudster uses the eID holder's authentication credentials without the eID holder's knowledge or participation. In such a case, the eID holder's declaration of intent is absent altogether. In the second scenario, the eID holder enters the PIN code personally but does so under the influence of fraud. This is legally more difficult, because the payment service provider's systems may show a technically correct authentication act. Nevertheless, the mere fact that the PIN code was entered or that strong customer authentication was completed is not sufficient to prove that the payer intended to make that particular payment. It must also be assessed whether the payer understood the meaning of the authentication act, including the amount, the payee and the legal effect of the transaction.

This conclusion is supported by the structure of PSD2. Article 64 of PSD2 regulates authorisation through the payer's consent, whereas Articles 97 and 98 regulate strong customer

authentication as a security requirement for electronic payments. These provisions serve different legal functions. Strong customer authentication may be the technical means through which consent is expressed, but it is not an independent substantive basis for consent. Therefore, strong customer authentication and consent must not be treated as identical legal concepts.

The second conclusion concerns the burden of proof. Under Estonian law, where a payment transaction is disputed, the payment service provider must prove that the transaction was authenticated, properly recorded and entered in the accounts, and that it was not affected by a technical breakdown or other deficiency. However, the mere recording of the use of a payment instrument is not sufficient to prove that the payment transaction was authorised or that the payer acted fraudulently, intentionally or with gross negligence. In eID-based payment disputes, authentication logs may therefore prove that a technical act was performed, but they do not by themselves prove the payer's actual consent or the degree of culpability of the payer's conduct.

The thesis therefore concludes that the payment service provider cannot rely solely on authentication logs. It must present additional evidence and circumstances that allow an assessment of whether the payer actually authorised the transaction or whether the payer's conduct amounted to fraud, intentional breach of obligations or gross negligence. Such circumstances may include the information displayed to the payer during authentication, the payee, the amount, the device used, whether the payment was made to a new beneficiary, whether the transaction differed from the payer's usual payment behaviour and whether there were other indications of fraud.

The third conclusion is that, under current law, the payment service provider bears the primary responsibility in the event of an unauthorised payment transaction. The payment service provider must refund the amount of the unauthorised transaction without undue delay. This reflects the consumer-protective logic of PSD2, according to which the risk of an unauthorised payment should not initially be borne by the payer. However, this primary refund obligation does not mean that the payment service provider always bears the final loss. Depending on the conduct of the payer, liability may be shifted partly or fully to the payer.

If the eID holder has breached obligations relating to the use of the payment instrument or personalised security credentials merely through ordinary negligence, the payer's liability is

limited to 50 euros. This limited liability reflects a consumer-protective allocation of risk. It is not reasonable to place the main burden of digital payment fraud on the individual consumer where the consumer's conduct does not exceed ordinary negligence, particularly because payment service providers design and control the technical infrastructure, authentication systems and fraud prevention mechanisms used in payment services.

If the eID holder has acted fraudulently, intentionally breached their obligations or acted with gross negligence, the 50-euro liability limit does not apply. In Estonian law, there is no statutory maximum liability cap for gross negligence. Therefore, a finding of gross negligence may result in the payer bearing the entire loss. The thesis finds that this makes the interpretation of gross negligence crucial in eID-related fraud cases. Gross negligence should not be interpreted broadly or inferred automatically from the fact that the payer entered a PIN code or that the transaction was technically authenticated. It must involve a substantially higher degree of blameworthiness than ordinary negligence.

The assessment of gross negligence must be case-specific. Relevant factors include the manner in which the fraud was committed, how convincing the manipulation was, what information was displayed to the payer during authentication, whether the payer understood that they were confirming a payment transaction, and whether the payment service provider had concrete risk indicators that could have allowed it to detect or prevent the fraud. The rule that authentication logs are not sufficient proof of gross negligence supports this approach and prevents payment service providers from transferring liability to the payer solely on the basis that the eID tool was technically used.

The comparison with Norwegian law demonstrates that liability in eID-related fraud cases can be structured in a more graduated manner. Norwegian law distinguishes between limited liability in cases of negligence, higher but still capped liability in cases of gross negligence, and full liability in cases of intentional breach. Norwegian case law also illustrates the importance of distinguishing between an objective breach of a duty of care and the payer's subjective awareness that they are breaching their obligations. This distinction is particularly relevant in social engineering cases, where the payer may objectively breach the rules for using authentication credentials but may nevertheless act in good faith, believing that they are communicating with the bank or preventing fraud. Although Norwegian law cannot be directly transferred to Estonian law, it provides useful comparative material for assessing whether

Estonian law should develop a more nuanced approach to gross negligence and intentional breach.

The thesis does not conclude that Estonian law must immediately adopt a statutory liability cap for gross negligence similar to the Norwegian model. Instead, the primary solution should be a more substantive and less formal interpretation of the existing rules. Estonian courts and dispute resolution bodies should avoid an approach where the entry of a PIN code or successful authentication automatically leads to a finding of gross negligence. A statutory amendment introducing a liability cap for gross negligence could become justified if case law remains overly formal or if the current system results too often in consumers bearing the entire loss in situations where their conduct, although negligent, falls short of intentional wrongdoing.

The thesis also concludes that the eID holder's liability must be excluded where the loss was caused or increased by the payment service provider's own failure to comply with its obligations. This includes cases where the payment service provider failed to require strong customer authentication, failed to provide an effective means for notifying the loss or misuse of the payment instrument, or failed to prevent further transactions after being duly notified by the payer. These are risks that lie primarily within the control of the payment service provider. The eID holder cannot reasonably assess whether the payment service provider's authentication system, notification channels or fraud prevention mechanisms comply with legal and technical requirements.

The proposed PSD3 and PSR framework strengthens the consumer-protective direction of payment services law, but does not resolve all problems related to eID-based fraud. Several principles already present in PSD2 and Estonian law are retained: the immediate refund obligation for unauthorised payments, the 50-euro limited liability rule, and the exclusion of payer liability where strong customer authentication was not required or where the loss occurred after proper notification by the payer. The significance of the PSR lies partly in the fact that these rules would be consolidated in a directly applicable EU regulation, contributing to greater uniformity across Member States.

A particularly important development is Article 55(2) of the proposed PSR, which expressly states that the recording of the use of a payment instrument, including the application of strong customer authentication, is not in itself sufficient to prove that the payment transaction was authorised or that the payer acted fraudulently or with gross negligence. This confirms and

strengthens the evidentiary principle already reflected in PSD2 and Estonian law. In eID-related fraud cases, it makes clear that the payment service provider cannot rely solely on the fact that strong customer authentication was successfully completed.

Another important development is the proposed special rule on impersonation fraud in Article 59 of the PSR. This provision addresses situations where a consumer is manipulated into making a payment as a result of the fraudulent misuse of the payment service provider's identity. Its significance lies in the fact that the allocation of liability would no longer depend solely on whether the consumer technically confirmed the payment. Instead, the legal assessment would also take into account the context of the fraud and the preventive obligations of the payment service provider. However, the scope of Article 59 is limited. It does not cover all types of social engineering fraud, but primarily situations involving misuse of the payment service provider's identity. Therefore, the general rules on consent, burden of proof and liability remain important even under the proposed framework.

The overall conclusion of the thesis is that Estonian law already contains important mechanisms for protecting the eID holder, but their effectiveness depends on substantive and purpose-oriented interpretation. At the level of authorisation, technical authentication must be distinguished from actual consent. At the level of proof, authentication logs must not be treated as sufficient evidence on their own. At the level of liability, ordinary negligence, gross negligence, intentional breach and fraud must be clearly distinguished. At the level of liability exclusions, the payment service provider's own failures must be taken into account.

The central conclusion of the thesis is therefore that the mere technical use of eID should not determine either the authorisation of a payment transaction or the liability of the eID holder. The allocation of liability must depend on whether the payer's actual intention was directed at making the specific payment, the degree of blameworthiness of the payer's conduct, and whether the payment service provider complied with its duties relating to authentication, proof, notification and fraud prevention. The proposed PSD3 and PSR framework moves in the same direction, but it does not remove the need for Estonian law to be interpreted in a case-specific and substantively balanced manner.

KASUTATUD ALLIKATE LOETELU

KASUTATUD KIRJANDUS

1. Braithwaite, J. Gross Negligence in Bank Payments Law. – Oxford Journal of Legal Studies 2026. – https://academic.oup.com/ojls/advance-article/doi/10.1093/ojls/gqag002/8454854 (07.02.2026).
2. Council of the European Union. Council adopts regulation on instant payments. 26.02.2024. - https://www.consilium.europa.eu/et/press/press-releases/2024/02/26/council-adopts-regulation-on-instant-payments/ (16.03.2026).
3. Eesti Pank. Maksepettuste ülevaade 2025. Eesti Pank, 2025. – https://haldus.eestipank.ee/sites/default/files/2025-12/ep_maksepettuste-ulevaade-2025_0.pdf (14.04.2026).
4. Eesti Pangaliit. Pettuste ennetamine. – https://pangaliit.ee/pettuste-ennetamine (09.04.2026).
5. Eesti Pangaliit. Uue Smart-ID loomisega seotud pettused põhjustavad miljonikahju - inimesed ei teadvusta ohumärke. - https://pangaliit.ee/uudised-ja-teated/uue-smart-id-loomisega-seotud-pettused-pohjustavad-miljonikahjusid-inimesed-ei-teadvusta-ohumarke (16.01.2026).
6. ERR. Kelmid on tänavu Eesti inimeste kontodelt varastanud 23 miljonit eurot. ERR, 13.01.2026. – https://www.err.ee/1609865229/kelmid-on-tanavu-eesti-inimeste-kontodelt-varastanud-23-miljonit-eurot (14.04.2026).
7. Euroopa Komisjon. Kiiremad ja turvalisemad eurovälkmaksed toimivad nüüd kogu euroalal. 09.10.2025. - https://estonia.representation.ec.europa.eu/uudised/kiiremad-ja-turvalisemad-eurovalkmaksed-toimivad-nuud-kogu-euroalal-2025-10-09_et (21.03.2026).
8. Euroopa Komisjoni ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, milles käsitletakse makseteenuseid ja e-raha teenuseid siseturul ning millega muudetakse direktiivi 98/26/EÜ ja tunnistatakse kehtetuks direktiivid 2015/2366/EL ja 2009/110/EÜ. - COM(2023) 366 final, 28.06.2023.
9. Euroopa Komisjoni ettepanek: Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse makseteenuseid siseturul ning millega muudetakse määrust (EL) nr 1093/2010. - COM(2023) 367 final, 28.06.2023.

10. Euroopa Liidu Nõukogu. Küberturvalisus: sotsiaalne manipulatsioon. Euroopa Liidu Nõukogu. https://www.consilium.europa.eu/et/policies/cybersecurity-social-engineering/ (10.01.2026).
11. European Banking Authority. EBA Consumer Trends Report 2024/25. European Banking Authority, 26.03.2025. – https://www.eba.europa.eu/sites/default/files/2025-03/514b651f-091b-42d3-b738-1fae79264044/Consumer%20Trends%20Report%202024-2025.pdf (14.04.2026).
12. European Banking Authority. Opinion on new types of payment fraud and possible mitigations, European Banking Authority, 2024. – https://www.eba.europa.eu/sites/default/files/2024-04/363649ff-27b4-4210-95a6-0a87c9e21272/Opinion%20on%20new%20types%20of%20payment%20fraud%20and%20possible%20mitigations.pdf (02.04.2026).
13. European Commission. Impact Assessment accompanying the Proposal for a Payment Services Regulation. SWD(2023) 231 final, 28.06.2023.
14. European Commission. Questions and answers: Strong Customer Authentication and open banking. European Commission, 16.09.2019. – https://ec.europa.eu/commission/presscorner/detail/et/qanda_19_5555 (14.03.2026).
15. German Banking Industry Committee (GBIC). Payment Services Regulation: Comments on EP and Council mandates with a view on the upcoming trilogue. Berlin, 28.08.2025. - https://bankenverband.de/sites/default/files/medien/3/dokumente/2025-08-28-trilogue-psr-psd3-comments-gbic-versand.pdf (23.02.2026).
16. Kalamees, P. „Näita käppa“ ehk minu digiallkiri, järelikult minu tehtud tehing. - Juridica 2024 nr 9-10.
17. Kjørven, M. E. 'Who Pays When Things Go Wrong? Online Financial Fraud and Consumer Protection in Scandinavia and Europe', (2020), 31, European Business Law Review, Issue 1, pp. 77-109. - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3583369 (19.02.2026).
18. Kjørven, M. E., Høgberg, A. P., Woxholth, G. The customer's liability for fraud-induced use of BankID and payment instruments. Oslo Law Review, 2024, 11(2). – https://www.scup.com/doi/10.18261/olr.11.2.3#sec-4 (12.03.2026).
19. Naabel, K. Esindusõigus näivusvolituse alusel ja selle isikuline piiritlus, sealhulgas eID kasutamise mõju esindusõiguse kehtivusele. Magistritöö. Juhendaja Piia Kalamees. Tartu Ülikool 2024. - https://dspace.ut.ee/server/api/core/bitstreams/7df28517-7669-4a43-9397-755c9cd22e62/content (03.12.2025).

20. Politsei- ja Piirivalveamet. Kelmid petsid Eesti inimestelt välja 29 miljonit eurot. - https://www.politsei.ee/et/uudised/kelmid-petsid-eesti-inimestelt-vaelja-29-miljonit-eurot-13196 (20.01.2026).
21. Politsei- ja Piirivalveamet. Politseis registreeritud sündmused. 05.12.2025. – https://www.politsei.ee/et/uudised/politseis-registreeritud-suendmused-473cb3-13111 (05.03.2026).
22. Rink, R. Autoriseerimata maksetehing elektroonilise maksevahendiga. Magistritöö. Juhendaja Urmas Volens. Tartu Ülikool 2012. - https://dspace.ut.ee/server/api/core/bitstreams/0d6468c2-e626-40b3-9de5-9d4cd3c75d00/content (02.12.2025).
23. SEB Pank AS. Rahvusvahelise deebetkaardi lepingu tingimused. Kehtivad alates 26.06.2025. - https://www.seb.ee/sites/default/files/tac/rahvusvahelise_deebetkaardi_lepingu_tingimused_20250626_est.pdf (26.03.2026).
24. Soosalu, T. Välkmakse saab normiks kogu euroalal. Eesti Pank, 03.02.2025. – https://www.eestipank.ee/blogi/valkmakse-saab-normiks-kogu-euroalal (19.03.2026).
25. Steennot, R. Reduced payer's liability for unauthorized payment transactions under the second Payment Services Directive (PSD2). – Computer Law & Security Review 2018/34(4). - https://www.sciencedirect.com/science/article/pii/S0267364918301924?via%3Dihub (15.03.2026).
26. Swedbank AS. Deebetkaardi kasutamise lepingu tingimused. Kehtivad alates 01.11.2023. - https://www.swedbank.ee/static/pdf/private/d2d/cards/conditions_debitcard_est_01112023.pdf (26.03.2026).
27. Van Praag, E. jt, „Authorised Push Payment Fraud: Suggestions for the Draft Payment Services Regulation", EBI Working Paper Series 2025, nr 190.
28. Wold, V. En kritisk oversikt over det privatrettslige forbrukervernet. – Kritisk juss 2024/2–4. - https://opphevet.juridika.no/tidsskrifter/kritisk-juss/2024/2-4/artikkel/wold-59178?utm (07.03.2026).
29. Wold, V., Kalamees, P. Identity Theft in Consumer Finance: Consent, Contract and Liability: Analysing Rules on Loss Allocation in Norwegian, Estonian and EU Law. – Oslo Law Review 2025/11(2). - https://www.scup.com/doi/epdf/10.18261/olr.11.2.3 (13.12.2025).

KASUTATUD ÕIGUSAKTID

EESTI ÕIGUSAKTID

30. Eesti Panga Presidendi 11.05.2010 määrus nr 4 „Maksejuhiste aktsepteerimise tingimused". - RTL 2010, 25, 446. - https://www.riigiteataja.ee/akt/13312807 (15.03.2026).
31. Tsiviilseadustiku üldosa seadus. - RT I, 31.12.2024, 48.
32. Võlaõigusseadus. - RT I, 11.11.2025, 16.

NORRA ÕIGUSAKTID

33. Lov om finansavtaler (finansavtaleloven) 18.12.2020 nr 146. - Lovdata. - https://lovdata.no/dokument/NL/lov/2020-12-18-146 (01.03.2026).

EUROOPA LIIDU ÕIGUSAKTID

34. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/2366, 25. november 2015, makseteenuste kohta siseturul, direktiivide 2002/65/EÜ, 2009/110/EÜ ning 2013/36/EL ja määruse (EL) nr 1093/2010 muutmise ning direktiivi 2007/64/EÜ kehtetuks tunnistamise kohta. – ELT L 337, 23.12.2015.
35. Euroopa Parlamendi ja nõukogu määrus (EL) 2024/886, 13. märts 2024, millega muudetakse määrusi (EL) nr 260/2012 ja (EL) 2021/1230 ning direktiive 98/26/EÜ ja (EL) 2015/2366 eurodes välkkreeditkorralduste osas (EMPs kohaldatav tekst). - ELT L, 2024/886, 19.3.2024.

SELETUSKIRJAD JA KOMMENTAARID

36. Võlaõigusseaduse ja teiste seaduste muutmise seaduse eelnõu seletuskiri. - https://www.koda.ee/sites/default/files/content-type/content/2017-02/SELETUSKIRI_I_ring_01_0_0.pdf (14.01.2026).

37. Võlaõigusseaduse ja krediidiasutuste seaduse muutmise seadus (finantspettuste ennetamine ja tõkestamine) seletuskiri. - https://eelnoud.valitsus.ee/main/mount/docList/4fb857a3-e037-492d-9d32-7c88e95b4151#MSHX5Up3 (05.04.2026).
38. Varul, P. jt (koost). Võlaõigusseadus IV. 8. osa 40. ptk – 10. osa (§-d 703–1067). Kommenteeritud väljaanne. Tallinn: Juura 2020.
39. Varul. P. jt (koost). Tsiviilseadustiku üldosa seadus. Kommenteeritud väljaanne. Tartu: Juura 2023.
40. Prop. 92 LS (2019–2020). Act on Financial Agreements (Financial Agreements Act) and consent to the approval of the EEA Joint Committee's decisions no. 125/2019 and 130/2019 of 8 May 2019 on the incorporation into the EEA Agreement of Directive 2014/17/EU on credit agreements for consumers relating to residential immovable property (the Mortgage Loan Directive) and Commission Delegated Regulation (EU) No. 1125/2014. Ministry of Justice and Public Security. - https://www.regjeringen.no/no/dokumenter/prop.-92-ls-20192020/id2700119/ (06.04.2026).

KASUTATUD KOHTUPRAKTIKA

EESTI KOHTUTE PRAKTIKA:

41. RKTKo 16.12.2019, 2-16-124450/77.
42. RKTKo 08.04.2015, 3-2-1-23-15.
43. RKTKo 26.09.2006, 3-2-1-53-06.

EUROOPA KOHTU PRAKTIKA:

44. EKo C-351/21, *ZG vs. Beobank SA*, ECLI:EU:C:2023:215.
45. EKo C-665/23, IL v Veracash SAS, ECLI:EU:C:2025:598.
46. EK C-70/25, *N. O. versus PKO BP S.A.*, ECLI:EU:C:2026:153, kohtujuristi A.Rantos ettepanek.

NORRA KOHTUPRAKTIKA:

47. Norra Ülemkohus (Norges Høyesterett). Rt-2011-410.
48. Norra Ülemkohus (Norges Høyesterett). HR-2024-990-A.
49. Norra Ülemkohus (Høyesterett), HR-2020-2021-A, 22.10.2020.
50. Norra Ülemkohus (Høyesterett), HR-2022-1752-A, 13.09.2022.
51. Agder lagmannsrett, LA-2021-136209, 07.01.2022.
52. Eidsivating lagmannsrett, LE-2021-70115, 27.11.2021.
53. Nord-Troms og Senja tingrett, TNTS-2024-30271, 01.11.2024.
54. Finansklagenemnda Bank, FinKN 2026-5, 06.01.2026, Nordea Bank Abp, filial i Norge, „Investeringssvindel – omsorgsplikt – erstatningskrav“.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Elisabeth Okk ,
(autori nimi)

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

eID OMAJA VASTUTUS AUTORISEERIMATA MAKSE KORRAL
(lõputöö pealkiri)

mille juhendaja(d) on Piia Kalamees ,
(juhendaja nimi)

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 Commonsi 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.

Elisabeth Okk
29.04.2026