TARTU ÜLIKOOL

ÕIGUSTEADUSKOND

Karistusõiguse osakond

Stina Veek

ISIKUSAMASUSE TUVASTAMISE KOHUSTUSE EDASIANDMISE OSAPOOLTE VASTUTUS MASINTEKKELISEL RIKKUMISEL

Magistritöö

Juhendaja

Marko Kairjak, PhD

Tallinn

2022

Sisukord

Sissejuhatus

Isikusamasuse tuvastamine on finants- ja krediidiasutusele hoolsusmeetmeks rahapesu ja terrorismi rahastamise tõkestamisel. Selle eesmärgiks on takistada kuritegelikult saadud vara varjamist või moondamist ja tõkestada rahapesu toimepanemist. Nende meetmete järgimine tagab ettevõtluskeskkonna läbipaistvust ning usaldusväärsust. Hoolsusmeetmeid loetakse täidetuks, kui asutusel tekib veendumus, et kohustus on täidetud vastavalt nõutavale. Isikusamasuse tuvastamiseks loetakse isiku tuvastamist isikustatud unikaalse ja personaalse informatsiooni abil. Selliseks teabeks on isiku nimi, isikukood (selle puudumisel sünnikoht ja -aeg ning asu- või elukoht) ning vajadusel ka isiku tegevus- või kutseala. Isiku tuvastamisel on lubatavad dokumendid näiteks seaduse alusel välja antud isikut tõendav dokument, välisriigis välja antud kehtiv reisidokument, juhiluba, sünnitõend või notariaalselt tõestatud/ametlikult kinnitatud ärakiri.[1] Käesolevas töös käsitletakse isikusamasuse tuvastamiseks kohustatud osapoolena peamiselt jaekliente teenindavaid krediidiasutusi krediidiasutuste seaduse mõistes.

Isikusamasuse tuvastamine krediidiasutuse poolt kannab mitmeid eesmärke. Kliendi isikusamasuse tuvastamisel kehtib põhimõte „tunne oma klienti." Selle põhimõtte sisuks ei ole ainult isikusamasuse tuvastamine, vaid ka kindlaks tegemine, mis on kliendi tegevusprofiil, tegevuse eesmärk, vahendite päritolu ja allikas, millega tehakse tehinguid, ning muu vajalik ning oluline informatsioon, mis võib ärisuhte loomiseks vajalikuks osutuda.[2] Lisaks kliendi kohta maksimaalse informatsiooni kogumise eesmärgile ning kontrollimisele, et tegemist on isikuga, kellena klient ennast esitleb, tuleb krediidiasutusele isikusamasuse tuvastamise kohustus ka Eesti seadusandlusest, täpsemalt rahapesu ja terrorismi rahastamise tõkestamise seadusest. Krediidiasutus on rahapesuvastase võitluse osas rahapesu ja terrorismi rahastamise tõkestamise seaduse (edaspidi RahaPTS) mõistes kohustatud isik kohaldamaks olulisi

[1] Finantsinspektsioon. Finantsinspektsiooni soovituslik juhend „Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks ". Finantsinspektsiooni koduleht 26.11.2018. Arvutivõrgus: https://www.fi.ee/sites/default/files/2018-11/FI_AML_Soovituslik_juhend.pdf (02.04.2022)

[2] Finantsinspektsioon. Finantsinspektsiooni soovituslik juhend „Rahapesu ja terrorismi rahastamise tõkestamise meetmed krediidi- ja finantseerimisasutuses". Finantsinspektsiooni koduleht 03.07.2013. Arvutivõrgus: https://www.fi.ee/failid/Soovituslik_juhend_Rahapesu_tokestamine.pdf (27.02.2022)

hoolsusmeetmeid oma igapäevatöös. Krediidiasutus on kohustatud jälgima teatud hoolsusmeetmeid, sh tuvastama tehingus osaleva isiku isikusamasuse ja esitatud teabe õigsust usaldusväärsest ja sõltumatust allikast hangitud teabe põhjal. RahaPTS sätestab täiendavad juhendid, nõuded ning tingimused, millega arvestada, et hoolsusmeetme järgimist saaks lugeda täidetuks. Seda ka juhul kui kasutatakse e-identimist ning e-tehinguid.[3]

21. sajandil on tendents digitaliseerumise suunas ning aina suuremat rolli mängib infotehnoloogia ka finantsmaailmas, seega krediidiasutused kujundavad oma ärimudeleid ümber, et selliste tehnoloogiatega kohalduda. Kõige enam antakse edasi teenuseid, mis on seotud infotehnoloogiaga, kuigi see võib endast kujutada turvariski ning muuta keerukaks seadusandluse, järelevalve ning andmekaitse.[4] Finantsasutustel lasub ulatuslik administratiivne koormus selleks, et nad oleksid võimelised järgima erinevaid seadusest tulenevaid nõudeid rahapesu tõkestamiseks. See nõuab krediidiasutustelt olulisi investeeringuid nende kohustuste täitmiseks. See on lisaks isikusamasuse tuvastamisele oluline ka tehingute monitooringu puhul, kus klientide, kontode ning tehingute maht on niivõrd suur, et vaid inimeste poolt manuaalselt piisavat ning täpset analüüsi tagada on keeruline. Seetõttu on krediidiasutused võtnud rahapesu tõkestamiseks kasutusele infotehnoloogia, seda nii informatsiooni mahu kui ka süsteemi järjepidevuse tõttu, vähendades inimfaktorit ning sellega kaasnevaid nõrkusi.[5]

Üheks oluliseks faktoriks infotehnoloogia implementeerimisel krediidiasutuste igapäevatöös on kuluefektiivsus. Selleks, et erinevaid seadusest tulenevaid nõudeid täita, on krediidiasutustele pandud mitmesuguseid kohustusi, mille täitmine vajab ressursse. Kuigi saab väita, et seaduste järgimine ning nende täitmine ülima täpsusega tagab selle, et krediidiasutus ei ole kohustatud maksma rikkumistest tulenevaid trahve ning maine on laitmatu, siis selline tegevus lisatulu ei genereeri ning ülesannete ebaefektiivsel täitmisel võib tekkida ülimalt suur kulu. Selleks, et turumajanduses maksimeerida oma tulu, on oluline hoida igapäevategevuste kulu võimalikult madalal. Infotehnoloogia ei asenda küll asutuses töötavaid inimesi täielikult,

[3] RT I, 12.03.2022, 19.

[4] EBA. Guidelines on outsourcing arrangements. European Banking Authority koduleht 25.02.2019.Arvutivõrgus: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1 (20.02.2019)

[5] Chau, D. Dijck Nemcsik, M. Anti-money laundering transaction monitoring systems implementation. Finding anomalies. *Sine loco*: Wiley 2020, lk 3-4.

ent võimaldab asutusel standardsetes olukordades vähendada kulukama inimfaktori kasutamist ning teha ülesandeid automatiseeritud kujul odavamalt.[6] Lisaks infotehnoloogiliste lahenduste kuluefektiivsusele ning kasumi suurendamise võimalusele, aitab digitaliseerimine tagada paremini teenuste paindlikkust ja efektiivsust.[7] Infotehnoloogia kasutuse ning osakaalu muutumist, tähtsuse suurenemist ning uute teenuste ja ärimudelite loomist, nimetatakse väljendiga *FinTech*, mis tähendab innovaatilise ning automatiseeritud tehnoloogia kasutamist finantsteenustes.[8]

Krediidiasutuse kohustus tuvastada klientide isikusamasus on üks nendest valdkondadest, milles nähakse võimalust rakendada *FinTech* lahendusi saavutamaks rahaline kokkuhoid ning suurenenud efektiivsus ja võimalus krediidiasutustel keskenduda rohkem oma põhifunktsioonidele. Selleks on Euroopa Liidu üleselt välja kujundatud protsess, mille alusel on krediidiasutustel võimalik taoliste kohustuste täitmisel kasutusele võtta infotehnoloogilisi lahendusi ning nende kohustuste täimine anda edasi osapoolele, kes taolist infotehnoloogilist lahendust omab. Infotehnoloogia kasutamisel isikusamasuse kohustuse täitmisel tekivad aga ohud, mis varasemalt kasutusel olnud alternatiivsete lahendustega tõusetunud ei ole. Olukorras, kus on kasutusele võetud infotehnoloogilised lahendused krediidiasutuse enda kohustuse täitmiseks viisil, mis tagab asutusele kuluefektiivsuse ja suurema ligipääsu rohkematele klientidele, on vajalik tagada, et klient ei oleks eelnimetatud lahenduste kasutusele võtmisega halvemas olukorras, kui varasemalt. Seetõttu nähakse vajadust valdkonda reguleerida ja ühtlustada.

FinTech areng on kiirenenud alles viimastel aastakümnetel koos üldiste infotehnoogiliste arengutega ning sellest tulenevalt, et tagada klientide ning üldise finantssüsteemi kaitse, on käesolevat valdkonda pidanud oluliseks reguleerida nii Eesti seadusandja kui ka Euroopa Liidu institutsioonid. Sellises kiiresti arenevas sektoris on aga oht olukorra tekkeks, kus õiguslikud regulatsioonid ei ole võimelised ajaga niivõrd kiires tempos kaasas käima ning sätete kohaldumine esinevatele olukordadele võib osutuda keeruliseks. Samuti võivad tekkida

[6] Chau, D. Dijck Nemcsik, lk 10-11.

[7] EBA/GL/2019/02

[8] OECD. Digital disruption in Bankind and its impact on competition. OECD koduleht. 2020. Arvutivõrgus: https://www.oecd.org/competition/digital-disruption-in-banking-and-its-impact-on-competition-2020.pdf (26.04.2022)

põhimõttelised vastuolud ja kaalutlused valdkonna reguleerimisel, kuna seadusandlusel ning õigusorganite poolt kehtestatud põhimõtetel on, arvestades valdkonna spetsiifikat, oht takistada valdkonna edasist arengut ja innovatsiooni.

Magistritöö eesmärk on analüüsida isikusamasuse tuvastamise tegevuse edasiandmise olemust valdkonnale kehtivate suuniste, juhendite ja õigusaktide põhjal ning sellele kehtivaid nõudeid ning erisusi kontekstis, kus tagatakse isikusamasuse tuvastamine läbi tegevuse edasiandmise kasutades infotehnoloogiliste lahendusi. Vajalik on teha kindlaks isikusamasuse tuvastamise kohustuse edasiandmise täitmise osapooled ning nendevahelised õiguslikud suhted selleks, et töö hilisemas etapis oleks võimalik teha järeldusi vastutuse olemasolu, selle jagunemise ning aluste kohta poolte vahel tekkinud õiguslikes suhetes. Lisaks sellele on eesmärgiks tuvastada infotehnoloogilised lahendused, mida on kasutusele võetud isikusamasuse tuvastamiseks teenusepakkujate poolt, kellele isikusamasuse tuvastamise tegevus edasi antakse, selleks, et mõista kasutusel olevatest infotehnoloogilistest lahendustest tulenevaid õiguslikke raamistikke, põhimõtteid ja tagajärgi. See võimaldab tuvastada teenusepakkuja vastutuse olemasolu tekkinud õiguslikes suhetes, selle paiknemise ja ulatuse. Eeltoodu võimaldab jõuda järeldustele selle osas, kuidas jaguneb vastutus isikusamasuse tegevuse edasiandmise osapoolte vahel olukorras, kui on toimunud rikkumine ning rikkumine on tekkinud masintekkelistel põhjustel infotehnoloogilise lahenduse poolt isikusamasuse tuvastamise kohustuse edasiandmise olukorras.

Magistritöös esitatud analüüsi raames antakse vastus järgnevatele küsimustele: Milliste tingimuste täitmisel on võimalik isikusamasuse tuvastamise tegevus anda edasi teenusepakkujale, sh elektroonseks täitmiseks? Milliste eritingimustega peab krediidiasutus arvestama isikusamasuse tuvastamise tegevuse edasiandmisel? Millised ohud kaasnevad infotehnoloogiliste lahenduste kasutamisel isikusamasuse tuvastamisel? Kes on isikusamasuse tuvastamise kohustuse edasiandmise täitmise osapooled ning millised õiguslikud suhted nende vahel tekivad? Millist tehnoloogilist lahendust kasutatakse peamiselt isikusamasuse tuvastamiseks teenusepakkujate poolt ning milline on sellekohane üldine ja vastutuse regulatsioon Eestis ja Euroopa Liidu üleselt juhul, kui toimub rikkumine infotehnoloogiast tulenevalt? Kuidas ja mille alusel jaguneb isikusamasuse tuvastamise osapoolte vahel vastutus

juhul, kui isikusamasuse tuvastamise tegevus on teenusepakkujale edasi antud ning toimub rikkumine, mis on masintekkeline?

Tegevuse edasiandmist isikusamasuse tuvastamise kohustuse kontekstis ei ole põhjalikult ja laiahaardeliselt käsitletud ei Eesti õiguses ega Euroopa Liidu õigusaktidest ja juhenditest tulenevalt. On ebaselge, millised erisused ja nõuded tulenevalt tegevuse edasiandmise reeglistikust kohalduvad isikusamasuse tuvastamise tegevuse edasiandmisele. Samuti puudub sellekohane kohtupraktika. Lisaks sellele puudub Eestis tehisintellekti käsitlev seadusandlus ja kohtupraktika ning Euroopa Liidu ülestes jõustatud õigusdokumentides on tehisintellekti käsitlev raamistik alles algusjärgus. Vastutuse olemasolu tehisintellekti poolt põhjustatud rikkumise korral ja selle paiknemist käsitlevaid õigusakte ei ole ei Eesti ega Euroopa Liidu tasandil. Samuti puudub ühene kohtupraktika, mida oleks võimalik käesoleva töö osas relevantseks pidada. Taoline olukord on eriti oluline krediidiasutuse kliendi kaitse seisukohast, kuna puudub õigusraamistik, mis võimaldab töös käsitletud rikkumise korral rikkumise eest vastutuse siduda konkreetse tehisintellekti ja selle välja töötanud või omava ettevõttega. Kuigi isikusamasuse tuvastamise kohustuse rikkumisel on seaduse alusel krediidiasutus vastutav riigi ees, on ebaselge, millistele alustele saab klient sellise rikkumise tagajärgede tekkimisel tugineda. Pole ka selge, kas vastutuse osas võib tekkida erisusi või saab krediidiasutus tugineda enda vastutuse puudumisele, kui tegemist on infotehnoloogiliste lahenduste poolt tekitatud rikkumistega.

Töö koosneb neljast peatükist, mis jagunevad alapeatükkideks. Esimene peatükk käsitleb krediidiasutuse võimalusi tuvastada klientide isikusamasus kasutades elektroonseid vahendeid, selle eeliseid, ohte ning riske ja tingimusi selle rakendamiseks. Esimene peatükk analüüsib isikusamasuse tuvastamise tegevuse edasiandmist ja seda käsitlevat reeglistikku. Lisaks annab esimene peatükk vastuse selle osas, milliste juhenditest ja suunistest tulenevate erisuste ja nõuetega peab krediidiasutus arvestama juhul, kui edasiantav teenus on isikusamasuse tuvastamine. Lisaks sellele selgub millistel järelevalveasutustel on pädevus ja õigus anda valdkonda reguleerivaid juhendeid ja suuniseid ning nende õiguslik siduvus.

Teine peatükk tuvastab isikusamasuse tuvastamise kohustuse edasiandmise osapooled analüüsib nende vahel tekkivaid õiguslikke suhteid. Teise peatüki analüüsist selgub, milliste õigussuhete raames ja mille alusel vastutusküsimused saavad rikkumise korral tekkida.

Kolmas peatükk analüüsib turul pakutavaid infotehnoloogilisi lahendusi isikusamasuse tuvastamiseks ning teeb järeldusi enimlevinud lahenduse kohta selleks, et välja selgitada selle lahenduse kasutust ja olulisust üldises finantssektoris. Tuvastanud enim kasutatud lahenduse, analüüsib kolmas peatükk selle lahenduse õigusraamistikku ja senist reguleerimist Eesti ja Euroopa Liidu tasandil, pöörates erilist tähelepanu lahenduse vastutusküsimuste lahendamisele eelnimetatud õigusaktides ja dokumentides. Kolmandas peatükis tuvastatakse olemasolevate õiguslike allikate ning valdkonna spetsialistide arvamuste alusel teenusepakkuja poolt pakutava lahenduse poolse rikkumise tagajärjel tekkinud vastutuse paiknemine suhtes teise osapoolega ning, tulenevalt lahenduse iseloomust, lahendusega seotud isikute ja teenusepakkuja vahel.

Neljandas peatükis analüüsitakse isikusamasuse tuvastamise kohustuse edasiandmise osapoolte vastutuse olemasolu, ulatust, jagunemist ja vastutuse tekkimise aluseid juhul, kui on toimunud isikusamasuse tuvastamise kohustuse rikkumine ning rikkumine on toimunud masintekkeliselt. Esmalt käsitletakse võimalikke rikkumise vorme, mis võivad isikusamasuse tuvastamisel masintekkeliselt tekkida ning millest tulenevalt vastutus tekib. Seejärel analüüsib neljas peatükk krediidiasutusele seadusega pandud isikusamasuse tuvastamise kohustuse rikkumisest tulenevat vastutust seaduse alusel, millega eelnimetatud kohustus krediidiasutusele tekitati. Järgmisena käsitletakse krediidiasutuse vastutust kliendi ees, kellega on krediidiasutus lepingulistes suhetes ning kelle isikusamasuse tuvastamisel on masintekkelistel põhjustel toimunud rikkumine. Lisaks sellele analüüsib neljas peatükk infotehnoloogilist lahendust pakkuva teenusepakkuja või lahendust kontrolliva isiku vastutust osapoole ees, kellega ollakse lepingulistes suhetes, ning võimalikku vastutust muudel alustel isiku ees, kelle isikusamasuse tuvastamisel masintekkeline rikkumine toime pandi.

Magistritöös on kasutatud peamiselt kvalitatiivset ning induktiivset ehk sünteetilist meetodit. Seda seetõttu, et töö on põhistatud peamiselt teoreetilisele ning sisulisele analüüsile ning käsitledes õigusakte, juhendeid ning Swedbank AS ning AS SEB üldtingimusi, tehakse töös järeldusi ning luuakse analoogse olukorra lahendamise teooria ning ettepanekud. Kirjandusena

on peamiselt kasutatud tegevuse edasiandmist käsitlevaid suuniseid ja juhendeid, millega vastavad järelevalveorganid valdkonda reguleerivad, Eesti ning Euroopa Liidu seadusakte, Euroopa Liidu institutsioonide jõustamata ettepanekuid, käsitlusi ning raporteid tehisintellekti vallas, õiguskirjandust ning avalikult saadaolevaid allikaid isikusamasuse tuvastamiseks kasutusel olevate infotehnoloogiliste lahenduste ning teenusepakkujate kohta.

Magistritööd iseloomustavad märksõnad: rahapesu, isikusamasuse tuvastamine, tegevuse edasiandmine, tehisintellekt, masintekkeline rikkumine.

1. Isikusamasuse tuvastamine elektroonselt, isikusamasuse tuvastamise edasiandmine ning sellega seotud riskid

1.1 Isikusamasuse tuvastamine elektroonselt ning sellest tulenevad kohustused krediidiasutustele

Isikusamasuse tuvastamiseks elektroonselt on mitmeid erinevaid võimalusi. Üheks võimaluseks on kasutada videosilla loomise võimalust, kus teostatakse identimist sooviva isikuga videokõne, mille viib krediidiasutuse poolt läbi väljaõppe läbinud töötaja. See annab võimaluse rakendada inimelementi, mis võib kanda suurt rolli kahtlase käitumise tuvastamiseks. Teiseks võimaluseks on kasutada täisautomaatseid lahendusi, mille puhul on välistatud inimteguri erapoolikus ning hinnanguliselt samaväärne efektiivsus. Kuigi täisautomaatne lahendus võib mitmetel põhjustel olla efektiivsem, siis sellel on suurem risk kogu süsteemi rikkeks.[9]

Eesti seadusandlus kohustab muuhulgas RahaPTS § 31 alusel teostada isikusamasuse tuvastamine ja andmete kontrollimine infotehnoloogiliste vahendite abil juhul, kui ärisuhte loomisel ei kohaldata hoolsusmeetmeid isikuga samas kohas viibides ja kui on täidetud muud tingimused. Nendeks tingimusteks on kui klient on pärit Euroopa Majanduspiirkonna välisest riigist või tema elu- või asukoht on sellises riigis või kui tehinguga või teenuse osutamise lepinguga seotud väljaminevate maksete kogusumma ühes kalendrikuus ületab 15 000 eurot füüsilisest isikust kliendi puhul või 25 000 eurot juriidilisest isikust kliendi puhul. Selleks, et võtta kasutusele infotehnoloogilisi vahendeid isikusamasuse tuvastamiseks ja andmete kontrollimiseks, peab isik omama seaduse nõuetele vastavat isikut tõendavat dokumenti ning

[9] Euroopa Komisjon. Report on existing remote on-boarding solutions in the banking sector. Assessment of risks and associated mitigationg controls, including interoperability of the remote solutions. Euroopa Komisjoni koduleht. 12.2019. Arvutivõrgus: https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf (20.02.2022)

krediidiasutus peab sellele lisaks kasutama usaldusväärsest ja sõltumatust allikast pärit teavet.[10] Vastavat seadust täpsustab valdkonna ministri määrus. Rahandusministri määrus sätestab täiendavaid tingimusi krediidiasutustele, sh kohustust kasutada kõrge usaldusväärsuse tasemega tehnilisi lahendusi. Sealjuures jätab määrus krediidiasutustele ka valikuvõimalusi, näiteks on lubatud kasutada biomeetriliste andmete võrdlemist. Nõuded infosüsteemidele on vastavas määruses ulatuslikud. Infosüsteemidele on esitatud miinimumnõudeid nii heli, infovoo kvaliteedi, salvestamise ja salvestise taasesitatavusele kui ka isiku näo ja dokumendi kadreerimisele. Krediidiasutus peab kehtestama asutusesiseselt protseduurireeglid infotehnoloogiliste vahendite abil isikusamasuse tuvastamiseks ja andmete kontrollimiseks. Määruses on kehtestatud nõuded ka isikule või tema esindajale, kes soovib e-identimislahendust kasutada, st nõuded dokumendile või süsteemile, millega oma identiteeti tuvastada soovitakse.[11]

Krediidiasutuste jaoks on elektroonsed isikusamasuse tuvastamise lahendused olulised, et omada ligipääsu Euroopa Liidu ülesele majandustegevusele, sest see võimaldab nii Euroopa Liidu kui ka kolmandate riikide isikutel osaleda Euroopa Liidu finantsturgudel.[12] Euroopa Komisjon toob välja, et kuigi on oluline järgida rahapesu tõkestamise põhimõtteid elektroonsel isikusamasuse tuvastamisel, siis peab pidama silmas proportsionaalsust, et liigsed meetmed kliendi kasutajakogemusele laastavalt ei mõjuks. Euroopa Komisjon toob välja Eesti seadusandluse rahapesu vallas, mille kohaselt võib teatud olukordades olla piisav vaid riikliku ID-kaardi kasutamine, et mitte igakordselt tuvastada isiku nägu kas video või otsese kontakti abil.[13] Teisest küljest rõhutab Euroopa Komisjon, et digitaalne isikute identifitseerimine võib muuta isikusamasuse tuvastamise protsessi hõlpsamaks ning suurendab teenuste paindlikkust, kuna teenuste saamiseks ei ole vajalik enam füüsiliselt pöörduda teenusepakkujate poole nende lahtiolekuaegadel.[14]

[10] RT I, 13.03.2022, 19.

[11] RT I, 04.12.2020, 9.

[12] EBA/GL/2019/02

[13] *Ibid*

[14] Euroopa Komisjon, eGovertnment Benchmark 2018: the digitaal efforts of European countries are visibly paying off. Euroopa Komisjoni koduleht, 22.11.2018. Arvutivõrgus: https://digital-strategy.ec.europa.eu/et/node/2424 (16.04.2022)

1.2 Elektroonse isikusamasuse tuvastamisega seotud riskid ja ohud

Euroopa Komisjon koostas aastal 2019 raporti hindamaks riske, mis tõusetuvad elektroonse isikutuvastuse implementeerimisega. Euroopa Komisjon on võtnud eesmärgiks selle, et Euroopa Liidu kodanikele oleks võimaldatud turvaline piiriülene teenindamine. Juhul, kui füüsiline või juriidiline isik soovib avada pangakontot teises Euroopa Liidu liikmesriigis, on kõige mugavamaks lahenduseks Euroopa Komisjoni hinnangul isikusamasus tuvastada kasutades elektroonseid vahendeid, mis pakuvad kohest madalate riskidega lahendust. Euroopa Komisjoni raporti hinnangul ei ole aga selline tulemus veel saavutatud, kuigi vahendid selleks on olemas.[15]

Kuigi elektroonsete vahenditega isikutuvastus rahapesu ning terrorismi rahastamise vastase võitluse kontekstis omab palju eeliseid, mis on võimaldanud ettevõtetel vähendada nende nõuete täitmise kulu ning suurendada enda klientide arvu, on elektroonse isikutuvastamisega seotud mitmeid riske.

Üheks ohuks, mis võib tekkida inkorporeerides elektroonseid vahendeid isikutuvastamiseks, on inimgrupi tekkimine, kes varasemalt kasutas alternatiivseid lahendusi, ent kellel on infotehnoloogilistele süsteemidele ligipääs erinevatel põhjustel raskendatud või välistatud. See võib viia olukorrani, kus isikud, kes varasemaid lahendusi kasutades omasid ligipääsu vajalike toiminguteni, lõigatakse välja oluliste teenuste kasutamise võimalustest seetõttu, et neil puudub ligipääs elektroonsetele lahendustele või seadmetele või puuduvad vajalikud oskused elektroonsete vahendite kasutamiseks. Üheks sellise olukorra tekke näiteks saab pidada e-hääletamise korraldamist, mille võimaldamine ei tohiks viia olukorrani, kus isikud, kellel puudub taoline võimalus ja ligipääs vajalikele e-lahendustele, jäävad ilma enda kodanikuõigusest hääletada. Kõige tõenäolisem on sellisesse riskirühma kuuluda näiteks puuetega inimestel, rahvusvähemustel, mittekodanikel ning isikutel, kes on tehnoloogiakauged või madala lugemisoskusega.[16]

[15] Euroopa Komisjon. 12.2019.

[16] World Bank. ID4D practitioner's guide: Version 1.0. Washington, 11.2019. Arvutivõrgus: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

Lisaks sellele, et elektroonset isikusamasuse tuvastamist kasutades on oht jätta ilma vajalikest teenustest ja toimingutest inimesed, kellel puuduvad teadmised ja võimalused kasutamaks elektroonseid vahendeid, võib elektroonsete lahenduste kasutamist mõjutada ka isikutest mitteolenevad faktorid ning võib tekkida risk nende kõrvale jäämiseks vajalikest teenustest ja tegevustest. Näiteks arengumaades puudub tegelik ülevaade riigi rahvastikust ning andmed isikute sündide ja surmade kohta on ebatäpsed. See tähendab ka seda, et sünnitunnistuse puudumisel ei pruugi kodanikel tekkida võimalust omada ametlikku isikut tõendavat dokumenti ning isiku kohased andmed võivad olla väga madala kvaliteediga. Samuti on infotehnoloogiliste lahenduste kasutamiseks kodanikele vajalik ligipääs vastavatele seadmetele, nende saadavus ja tehnilised võimalused nende kasutamiseks. Sellega võib tekkida probleem mitmetes regioonides, kus andmeside ja interneti ühenduse võimalus puudub ning ei ole loodud vajalikke infrastruktuure selle võimaldamiseks.[17]

Näost-näkku kontakti asendamine elektroonsete vahenditega võib suurendada ka infotehnoloogilistele lahendustele omaseid riske, mis on valitsevad üldises infotehnoloogilises ruumis. Näiteks küberründed või tehniliste vahendite rikked isikusamasuse tuvastamise süsteemides või isikuandmete väärkasutamine. Ei ole välistatud ka sarnased vead, mille risk on suurem infotehnoloogiliste vahendite mitte kasutamisel nagu näiteks inimlik eksimine või vääralt isiku tuvastamine. Suures osas oleneb riskide realiseerumine ka kasutusel oleva süsteemi kvaliteedist ja efektiivsusest. [18]

1.3 Isikusamasuse tuvastamise tegevuse edasiandmine

Tegevuse edasiandmine (inglise keeles ka *outsourcing*) tähendab Euroopa Pangandusjärelevalve Asutuse (European Banking Authority, edaspidi EBA) tõlgenduse kohaselt ükskõik millises vormis kokkulepet krediidiasutuse ning teenusepakkuja vahel, mille

[17] World Bank, lk 7.

[18] Mahajan, D; Sperling, O; White, O. Digital ID: The opportunities and the risks. McKinsey&Company 2019. Arvutivõrgus: https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/digital-id-the-opportunities-and-the-risks (02.04.2022)

kohaselt teostab teenusepakkuja protsessi, teenust või tegevust, mida mitte edasiandmisel teostaks krediidiasutus ise.[19]

Nagu varasemalt tuvastatud, on krediidiasutuse kohustus isikusamasust tuvastada hoolsusmeetmeks RahaPTS alusel. Eesti seadusandluse alusel on rahapesu ja terrorismi tõkestamise eesmärgil kehtestatud kohustuste ja hoolsusmeetmete, sh isikusamasuse tuvastamise kohustuse kohaldamise edasiandmise õigus sätestatud RahaPTS §-s 24. Käesolev paragrahv on Eesti õiguses aluseks krediidiasutuse õiguse tekkeks anda enda kohustusi edasi teisele osapoolele. Paragrahv sätestab tingimused tegevuse edasiandmiseks ja nõuded teenusepakkujale ning pooltevahelisele tegevuse edasiandmise lepingule. Paragrahv sätestab ka krediidiasutuse kohustuse lepingust teavitada vastavaid järelevalveasutusi. Sättest tuleb kohustus tagada kõikide kohustuste ja hoolsusmeetmete täimine tegevuse edasiandmisel ning nõue pakkuda tegevust sama kvaliteediga kui teeks seda krediidiasutus ise.

Tegevuse edasiandmise sisu ning nõudeid krediidiasutustele sisustavad lisaks RahaPTS-ile Eestis siseriiklik järelevalveorgan finantsinspektsioon ning Euroopa Liidu ühtse arusaama ning riikide sisemise tegevuse edasiandmise kohaldamise praktika ühtlustamise eesmärgil EBA. Finantsinspektsiooni õigus teostada krediidiasutuste tegevuse üle järelevalvet ning suunata ja mõjutada finantsjärelevalve subjekte tuleneb finantsinspektsiooni seadusest. Selleks on finantsinspektsioonil õigus anda välja soovitusliku iseloomuga suuniseid ja juhendeid finantssektori tegevust reguleerivate õigusaktide selgitamiseks või järelevalvesubjektide suunamiseks. Finantsinspektsioon annab välja suunised selgitamaks järelevalvesubjektidele täitmiseks kohustuslikke seadusi ning Euroopa Liidu õigusakte. Lisaks sellele koostab juhendeid, mille üle omab finantsinspektsioon järelevalvekohustust.[20] See tähendab, et finantsinspektsiooni poolt välja antud tegevuse edasiandmise suunised ei ole aluseks krediidiasutuse vastutuseks, vaid selgitavad EBA poolt esitatud suuniseid ja soovitusi. Eelnimetatud suuniste avaldamisega nähtub, et finantsinspektsioon on otsustanud järgida EBA

[19] EBA/GL/2019/02

[20] RT I, 29.03.2022, 8

poolt esitatud suunist.[21] Finantsinspektsiooni tegevuse edasiandmise soovitusliku juhendiga antakse välja EBA „tegevuse edasiandmise suunised".[22]

EBA on Euroopa Liidu asutus, millel on juriidilise isiku staatus ning mis omab kõikides liikmesriikides kõige laialdasemat õigus- ja teovõimet, mis juriidilistel isikutel vastavas liikmesriigis tagatakse. EBA ülesandeks on aidata kaasa liiduüleselt järelevalvestandardite ning -tavade loomisele läbi erinevate Euroopa Liidu finantsinstitutsioonidele esitatud arvamuste ning avaldades seadusandlikel aktidel põhinevaid suuniseid, soovitusi ning eelnõusid.[23] EBA poolt esitatud suunised ei ole oma olemuselt imperatiivsed ega tekita siduvaid õiguslikke tagajärgi. See tähendab, et asutused, kellele on EBA suunised suunatud, ei ole kohustatud suuniseid järgima ja säilib õigus nendest kõrvale kalduda. Euroopa Kohtu hinnangul, kuigi EBA suunised ei ole õiguslikult siduvad liikmesriikide järelevalve organitele ning krediidiasutustele, peavad osapooled tegema endast kõik oleneva, et neid järgida ning järelevalveasutused peavad andma EBA-le selgitusi juhul, kui on võetud vastu otsus suuniseid mitte järgida. Lisaks sellele eeldatakse, et Euroopa Liidu liikmesriikide siseriiklikud kohtud arvestavad EBA suunistega kohtusse jõudnud kaasuste lahendamisel.[24] Käesolevas töös on asjaomane EBA tegevuse edasiandmise suunis, mille on finantsinspektsioon avaldades üle võtnud. EBA suunised tuginevad erinevatele Euroopa Liidu direktiividele ning lisavad täiendavaid selgitusi. Kuigi Euroopa Liidu direktiivid on iga liikmesriigi suhtes siduvad ning võivad liikmesriigi suhtes omada vahetut mõju ka juhul, kui vastavaid sätteid ei ole liikmesriigi õigusesse korrektselt üle võetud[25], annab Euroopa Kohtu otsus võimaluse siseriiklikus kohtus võtta arvesse ka EBA poolt välja antud suuniseid. Käesoleva töö autori hinnangul tähendab see,

---

[21] 24. november 2010. aasta Euroopa Parlamendi ja nõukogu määrus (EL) nr 1093/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Pangandusjärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/78/EÜ. – ELT L 331/12, artikkel 16. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32010R1093&from=en (10.04.2022)

[22] Finantsinspektsioon. Juhatuse otsus, 05.08.2019 nr 1.1-7/92. Arvutivõrgus: https://www.fi.ee/sites/default/files/2019-08/JHO%2CEuroopa%20Pangandusjärelevalve%20Asutuse%20suuniste%20Tegevuse%20edasiandmise%20suunised%20välja%20andmine..pdf (10.04.2022)

[23] Euroopa Parlamendi ja nõukogu määrus (EL) nr 1093/2010, artikkel 8

[24] EKo C-911/19, *Fédération bancaire française (FBF) versus Autorité de contrôle prudentiel et de résolution (ACPR),* ECLI:EU:C:2021:599.

[25] Euroopa Parlament. Euroopa Liidu õiguse allikad ja kohaldamisala. Euroopa Parlamendi koduleht. Arvutivõrgus: https://www.europarl.europa.eu/factsheets/et/sheet/6/euroopa-liidu-oiguse-allikad-ja-kohaldamisala

et tegevuse edasiandmise sisustamisel on võimalik võtta arvesse finantsinspektsiooni juhendit, mille eesmärgiks on avaldada EBA suunised. Kuigi tegemist ei ole õiguslikult siduva õigusaktiga ning kõne all olevad dokumendid ei ole aluseks vastutusele võtmisele või vastutuse jagunemiseks, on võimalik vastavatele suunistele kohtuvaidluse tekkimisel ning vastutusküsimuse lahendamisel tugineda.

Tegevuse edasiandmine on oma olemuselt äripraktika, mille kohaselt antakse teatud tegevus edasi täitmiseks kolmandale osapoolele ehk teatud tegevused või töökohad delegeeritakse osapoolele, kes on võimeline seda funktsiooni täitma kiiremini, paremini ja odavamalt. Finantsinspektsiooni hinnangul on tegevuse edasiandmise eesmärgiks järelevalve subjektil läbi tegevuse edasiandmise saavutada suurem efektiivsus, kontsentreeruda oma põhitegevusele ja kompetentsile ning võimaldab klientidele pakkuda kvaliteetsemat teenust või toodet.[26] Eesti seadusandja ei ole tegevuse edasiandmise mõistele legaaldefinitsiooni andnud. T. Toonela kirjutatud magistritöös jõutud järelduse kohaselt on tegevuse edasiandmise mõiste sisustamise ülesanne ja roll on jäänud järelevalveorganitele. Seda on neil võimalus teha läbi nende poolt koostatavate selgitavate juhendite. Finantsinspektsioon on defineerinud tegevuse edasiandmist Eesti finantssektoris kui „järelevalvesubjekti poolt lepingu alusel, arvestades õigusaktides sätestatud erinõudeid ja piiranguid, kolmanda isiku (teenusepakkuja) teenuste kasutamine, mille sisuks on tegevuste ja toimingute jätkuv teostamine, mis on vajalikud järelevalvesubjekti poolt klientidele tegevus(te) osutamiseks ning mida tavaolukorras teostaks järelevalvesubjekt ise“. Oluline on märkida, et tegevuse edasiandmise definitsioon finantsvaldkonnas ei ole identne teistes valdkondades valitseva arusaamaga tegevuse edasiandmisest, kuna vastavalt finantssektoris kehtestatud normidele käsitletakse tegevuse edasiandmisest tulenevate riskide vastutust ning vastutuse üleandmist mõnevõrra teisiti.[27]

[26] Finantsinspektsioon. Finantsinspektsiooni soovituslik juhend. Nõuded finantsjärelevalve subjekti poolt tegevuse edasiandmisele (outsourcing). 05.08.2019. Arvutivõrgus: https://www.fi.ee/sites/default/files/2019-08/pp%20nr%2004%2005.08.2019%20Tegevuse%20edasiandmise%20FI%20juhend%20uues%20redaktsioonis%20ET_0.pdf (27.02.2022)

[27] Toonela, T. Tegevuse edasiandmise käsitlus finantsvaldkonna õigusaktides. Magistritöö. Juhendaja Kadri Siibak. Tallinn: Tallinna Tehnikaülikool 2019, p 1.1. Arvutivõrgus: https://digikogu.taltech.ee/et/Item/00e6c6da-b6a8-4e66-b2ac-067e2bb4fe0a (02.04.2022)

Funktsiooni täitmise viisi liigitumine tegevuse edasiandmisena eeltoodu alustel omab rolli ning vajab täpset määratlemist finantssektoris seetõttu, et kui on tegemist tegevuse edasiandmisega Euroopa Liidu õigusorganite ning finantsinspektsiooni tõlgenduse kohaselt, peab krediidiasutus arvestama täiendavate kohustustega lepingu sisu ning järelevalveasutuse teavitamise osas. Kuigi krediidiasutus ja tegevust teostav teenusepakkuja astuvad lepingu sõlmimisel võlaõiguslikku suhtesse ning sellele kehtib lepinguvabaduse põhimõte, esineb finantsjärelevalveasutusel alus sekkuda krediidiasutuse ning teenusepakkuja privaatautonoomiasse. Osapool, kes hakkab edasiantud tegevust teostama, ei ole sarnaselt krediidiasutusele läbinud kindlaid järelevalveorgani poolt sätestatud hindamisprotsesse, mille käigus antakse hinnang asutuse majandus- ja kutsetegevuse alustamise lubatavusele. See tähendab, et kohustuste määramist ja nõuete esitamist sellisele osapoolele saab järelevalveorgan sätestada vaid läbi tegevuse edasiandmise lepingule esitatud nõuete. Selle protsessi reguleerimise alusel on võimalik taoline kolmas osapool, antud juhul tegevust osutav teenusepakkuja, allutada läbi lepingutingimustele esitatud nõuete finantsjärelevalvele ning võimaldada kolmandale osapoolele delegeerida ülesandeid, mis seaduse kohaselt on määratud täitma vaid finantsjärelevalve subjektide poolt.[28]

Finantsinspektsiooni tegevuse edasiandmise juhendis sätestatud nõuded tegevuse edasiandmise lepingule sisaldavad üldiseid nõudeid lepingu sisule. Nendeks on edasiantava tegevuse ja selle ulatuse võimalikult täpne määratlemine, õiguste, kohustuste ja tasustamise piisavalt täpne kehtestamine ning tegevuse edasiandmise lepingu koostamine viisil, mis ei takista finantsjärelevalve subjektile pandud kohustuste ning tema üle riikliku järelevalve teostamise täitmist. Muuhulgas on juhendis sätestatud kohustus lepingus kokku leppida tagatistes ja garantiides juhuks, kui lepingulisi kohustusi ei täideta nõuetekohaselt või kui tekib kahju, mida peab hüvitama, täpsustamata seda, kuidas kohustused ja vastutus lepingus osapoolte vahel jagatud olema peaks.[29]

Kui antakse edasi finantsasutuste funktsioone olukorras, kus teenusepakkuja asub väljaspool Euroopa Liitu, on riskid suuremad nii asutustele endale kui järelevalveasutustele. Eriti juhul, kui antakse edasi tegevust, mille eest vastutab juhatus. See võib muuta suhet asutuse ning nende

[28] Toonela, T. P 1.1

[29] Finantsinspektsioon. 05.08.2019.

klientide suhtes, sest krediidiasutusel on lepinguline suhe ja kohustused enda kliendi ees. Tegevuse edasiandmine ei tohiks tekitada olukorda, kus ei ole võimalik omada piisavat kontrolli asutuse tegevuse üle ega vähendada teenuse kvaliteeti. Finantsasutuse juhatuse vastutust oma tegevuse eest ei saa edasi anda. EBA sellekohased suunised sätestavad, et iga krediidiasutuse juhatus jääb vastutavaks asutuse tegevuste ning tegevusega kaasnevate riskide eest eranditeta. Krediidiasutused peavad pidevalt ning efektiivselt kontrollima enda poolt edasiantud tegevuste kvaliteeti ja toimimist ning teostama riskihinnanguid ning pidevat monitoorimist. Ei ole piisav, et ettevõtted annavad vaid formaalseid hinnanguid ning vabanevad vastutusest tagada tegevuse edasiandmise nõudeid.[30] Finantsinspektsiooni juhend viitab tsiviilseadustiku üldosa seaduse § 31 lg-le 3, mille kohaselt ei saa eraõigusliku juriidilise isiku organi pädevust anda üle muule organile või isikule. Krediidiasutustele on sätestatud ulatuslikud nõuded teenusepakkuja taustakontrolli teostamiseks, mis töö kirjutaja hinnangul raskendab krediidiasutuse poolt vastutusest vabanemist, st paneb krediidiasutuse hoolsuskohustuse teenusepakkuja valikul kõrgeks ning raskendab tegevuse edasiandmisel tekkivate rikkumiste korral tuginemist teenusepakkuja poolsele rikkumisele või pakutava teenuse puudujääkidele.[31]

Tegevuse edasiandmiseks on krediidiasutusel vajalik esmalt saada selleks luba vastavate kompetentsete autoriteetide käest kooskõlas Euroopa Liidu seadusandlusega. Riigisisesed järelevalveasutused peavad samuti esmalt kindlaks tegema selle, et krediidiasutustel on piisavad reeglid ja protseduurid paigas vastavalt ajas muutuvatele kohalduvatele reeglitele. [32]

Isikusamasuse tuvastamise tegevuse edasiandmise näol on tegemist krediidiasutuse hoolsusmeetme täitmise edasiandmisega osapoolele, kellel sellist kohustust seadusest ei teki.[33] Isikusamasuse tuvastamise tegevuse edasiandmine võimaldab krediidiasutusel täita oma kohustust olukorras, kus kohustuse täitmist reaalselt korraldab ettevõte, kellele tegevus edasi antakse. Läbi tingimuste, mis on sätestatud osapoolte vahel sõlmitud lepingule järelevalveasutuste poolt, on võimalik anda edasi tegevusi, mida seaduse alusel on määratud

[30] EBA/GL/2019/02

[31] Finantsinspektsioon 05.08.2019.

[32] EBA/GL/2019/02

[33] RT I, 12.03.2022, 19.

täitma vaid krediidiasutused.[34] Seega tähendab isikusamasuse tuvastamise tegevuse edasiandmine, et ettevõte, kellega on krediidiasutus sõlminud lepingu, tagab isikute isikusamasuse tuvastamise samadel tingimustel ja kvaliteedil, kui oleks selleks kohustatud krediidiasutus. Juhul, kui lepingus pole see selgesõnaliselt sätestatud, peab ettevõte oma kohustust täitma võttes muuhulgas arvesse seadustest tulenevaid nõudeid nii isikusamasuse tuvastamisele, tegevuse edasiandmisele kui ka rahapesu ja terrorismi tõkestamise hoolsusmeetmetele.

EBA suunistes eristatakse krediidiasutuse kõikidest funktsioonidest kriitilisi ja olulisi funktsioone. Kriitilised ja olulised funktsioonid on need, millel võib olla suur mõju krediidiasutuse riskiprofiilile ja sisemisele reeglistikule. Seetõttu on nende edasiandmisele sätestatud ka lisanõuded. Finantsinspektsiooni soovituslikus tegevuse edasiandmise nõuete juhendis taolist eristamist funktsioonide olulisuses ning kriitilisuses sellises detailsuses ei ole välja toodud. Samas vastavalt EBA poolt välja antud suunistele, mis on samuti krediidiasutustele ning finantsinspektsioonile enda juhendite sisustamiseks olulised ning mis on siseriiklikult koostatud juhendite aluseks, on funktsioonide tähtsusel tegevuste edasiandmisel erisused ning sellest lähtuvalt nagu eelmainitud, erinevad nõuded selleks, et anda selgust ja luua ühtne tõlgendus Euroopa Liidu ülese arusaama harmoneerimiseks. See tähendab, et lähtudes küll siseriikliku finantsjärelevalve asutuse suunistest, on vajalik arvestada EBA poolt juhistatud nüanssidega. Selleks, et jõuda järeldusele, kas isikusamasuse tuvastamise kohustuse edasiandmisel on tegemist tegevuse edasiandmisega, mis allub olulise või kriitilise funktsiooni edasiandmise erisustele, on vajalik arvestada EBA suunistega. Seejuures tuleb meeles pidada, et EBA peab IT teenuste saamist, ka juhul, kui seda teenuse osutamist kolmanda osapoole poolt ei saa pidada tegevuse edasiandmiseks, suurema riski allikaks.[35]

EBA suunistes ei ole selgesõnaliselt toodud välja isikusamasuse tuvastamise kohustust ega selle tegevuse edasiandmise kvalifitseerimist kriitiliseks või oluliseks funktsiooniks. Selleks tuvastamiseks tuleb välja selgitada, kuidas neid funktsioone defineerib oma suunises EBA. Sellisteks funktsoonideks on situatsioonid kus:

[34] Toonela, T. P 1.1

[35] EBA/GL/2019/02

1. „Viga või katkestus teenuse toimimises toob endaga kaasa olulised rikkumised Euroopa Liidu seadusandlusega, takistab asutuse finantsteenuse toimimist või katkestab nende maksu- ja pangandusteenuse ja -tegevuse jätkusuutlikkuse või usaldatavuse.
2. Antakse edasi sisekontrolli funktsioone.
3. Antakse edasi krediidiasutusele omaseid funktsioone, mis vajavad kompetentsetelt organitelt nõusolekut.“[36]

Selleks, et mõista, millena käsitleb EBA kriitilisi või olulisi funktsioone, on vajalik välja selgitada, mis on kriitiline või oluline funktsioon Euroopa Liidu õiguses. Euroopa Parlamendi direktiivi 2014/59/EU artikkel 2 punkt 1 lõige 35 toob kriitiliste funktsiooni definitsiooniks „teenused või tegevused, mille seiskumine toob ühes või enamas liikmesriigis tõenäoliselt kaasa reaalmajanduse jaoks oluliste teenuste katkemise või häirib tõenäoliselt finantsstabiilsust krediidiasutuse või investeerimisühingu või konsolideerimisgrupi suuruse, turuosa, välise ja sisemise seotuse, keerukuse või piiriülese tegevuse tõttu, pidades eelkõige silmas kõnealuste tegevuste, teenuste või tegevuste asendatavust.“[37] Euroopa Komisjoni määrus omakorda annab kriteeriumid selleks, et määrata kindlaks kriitilised funktsioonid. Funktsioon on kriitiline kahe tingimuse täitumisel: kui krediidiasutus täidab funktsiooni endaga mitteseotud kolmandate isikute jaoks ning kui „funktsiooni täitmise ootamatu katkemine avaldaks tõenäoliselt olulist negatiivset mõju kolmandatele isikutele, põhjustaks finantsraskuste levimist või vähendaks turuosaliste üldist kindlustunnet, sest funktsioon on kolmandatele isikutele süsteemselt oluline ning krediidiasutus või investeerimisühing või konsolideerimisgrupp on funktsiooni täitmisel süsteemselt oluline.“ Selleks, et teha kindlaks, kas kolmandatele isikutele avaldatav mõju on olemas, peab hindama:

1. asutuse ulatust piirkondlikult, st kas asutus tegutseb mõnes piirkonnas, riigis või Euroopa Liidu üleselt,
2. kui palju tehinguid ja millises mahus teeb asutus,

[36] EBA/GL/2019/02

[37] Euroopa Parlamendi ja Nõukogu direktiiv 2014/59/EL, millega luuakse krediidiasutuste ja investeerimisühingute finantsseisundi taastamise ja kriisilahenduse õigusraamistik ning muudetakse nõukogu direktiivi 82/891/EMÜ ning Euroopa Parlamendi ja nõukogu direktiive 2001/24/EÜ, 2002/47/EÜ, 2004/25/EÜ, 2005/56/EÜ, 2007/36/EÜ, 2011/35/EL, 2012/30/EL ja 2013/36/EL ning määruseid (EL) nr 1093/2010 ja (EL) nr 648/2012. ETL L 173/190. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32014L0059&from=EN (02.03.2022)

3. klientide olukorda, st kui palju on krediidiasutusel kliente, kellele on asutus ainsaks panganduspartneriks, kas klient, kes saab funktsioonist mõjutatud, on jaeklient või äriklient jne.[38]

Käesolevas töös käsitleme krediidiasutusena peamiselt jaekliente (Eesti õiguse järgi tarbija) teenindavaid finantsasutusi, kes on isikusamasuse tuvastamise kohustuse täitmiseks võtnud kasutusele teenusepakkuja poolt pakutava elektroonse isikusamasuse tuvastamise lahenduse. Sellises olukorras saab väita, et krediidiasutus täidab funktsiooni kolmandate isikute jaoks, kes ei ole krediidiasutuse endaga seotud. Selleks, et saaks üheselt väita, et isikusamasuse tuvastamise funktsioon on kriitiline funktsioon EBA suunise mõttes, tuleb analüüsida sellise funktsiooni katkemise mõju. Eesti seadusandluse alusel on isikusamasuse elektroonne tuvastamine kohustuslik juhul, kui tehingu maht ületab füüsilise isiku puhul 15 000 eurot ning juriidilise isiku puhul 25 000 euro. Olukorras, kus isikusamasuse tuvastamine on katkenud või töötab ebakorrektselt eelnimetatud mahus tehingute tegemisel, on võimalik väita, et selle tagajärjel võivad tekkida ulatuslikud finantsilised tagajärjed ning tehingu tegemine võib olla kolmandatele isikutele oluline. Seda näiteks juhul, kui tuvastatakse isik valesti. Samuti vähendab klientide usaldust nii vastava asutuse kui ka süsteemi vastu olukord, kus ei ole võimalik kliendi isikusamasuse tuvastamise kohustust täita või ei ole võimalik teostada seda korrektselt. Eeltoodule tuginedes, on töö autor seisukohal, et isikusamasuse tuvastamise funktsioon on kriitiline funktsioon EBA suunise, Euroopa Parlamendi direktiivi 2014/59/EU ning Euroopa Komisjoni delegeeritud määruse (EU) 2016/778 mõistes ning vastavalt EBA suunistele on seda funktsiooni võimalik anda edasi teenusepakkujale, arvestades kriitiliste või oluliste funktsioonide edasiandmisele sätestatud erisustega.

Kriitilise või olulise funktsiooni tuvastamine isikusamasuse tuvastamise edasiandmise kontekstis on oluline juba enne tegevuse edasiandmise kokkuleppe sõlmimist. Seda seetõttu, et vastavalt tegevuse liigitusele, on teatud aspekte, millega peab arvestama juba lepinguliste suhete kujundamisel. Juhul, kui tegemist on kriitilise või olulise funktsiooniga, peab

[38] 2. veebruar 2016. aasta Euroopa Komisjoni delegeeritud määrus (EU) 2016/778, millega täiendatakse Euroopa Parlamendi ja nõukogu direktiivi 2014/59/EL seoses asjaolude ja tingimustega, mille korral võib krediidiasutuse või investeerimisühingu tasutavad erakorralised *ex post* osamaksed täielikult või osaliselt edasi lükata, ja kriitiliste funktsioonidega seotud tegevuste, teenuste ja toimingute kindlaksmääramise ning põhiäriliinide ja nendega seotud teenuste kindlaksmääramise kriteeriumidega. – ELT L 131/41, artikkel 6. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32016R0778&from=EN (10.04.2022)

krediidiasutus selle tuvastama. Samuti tegema kindlaks sellega kaasnevad ohud ning lepingulistesse suhetesse astumise eel need ohud maandama. Üheks võimalikuks tagajärjeks olukorras, kui edasiantav tegevus on kriitiline või oluline, võib olla vajadus tegevus edasi anda mitmele erinevale teenusepakkujale. See tähendab, et ka juhul, kui krediidiasutus on järginud kõiki juhiseid ja soovitusi selleks, et tegevuse edasiandmine oleks võimalik ja õiguspärane, võib kriitilise või olulise tegevuse puhul olla krediidiasutuse poolne tegevuse edasiandmine puudulik seetõttu, et tegevuse täitmine anti edasi vaid ühele teenusepakkujale.[39]

[39] Finantsinspektsioon. 05.08.2019.

2. Isikusamasuse tuvastamise kohustuse edasiandmise täitmise osapooled ning nendevahelised õiguslikud suhted

Selleks, et tuvastada isikusamasuse tuvastamise kohustuse edasiandmise pooltevaheline vastutuse jagunemine, kui toimunud on masintekkeline rikkumine, on esmalt oluline kindlaks teha, millised osapooled kõne all olevas protsessis osalevad ning millistes õiguslikes suhetes osapooled üksteise suhtes on. Sellest tulenevalt on hiljem võimalik teha kindlaks, kas ja milliseid õiguslikke instrumente enda huvide kaitseks on erinevatel osapooltel võimalik rakendada.

2.1 Krediidiasutuse ja teenusepakkuja vahelised õiguslikud suhted

Esmalt peab krediidiasutus välja selgitama, kas kõne all olev kokkulepe kolmanda osapoolega, käesoleval juhul teenusepakkujaga, on oma olemuselt tegevuse edasiandmine finantsinspektsiooni ning EBA suuniste mõistes. Selleks on vajalik analüüs, kas funktsioon, mida soovitakse kolmandale osapoolele edasi anda püsivalt, on tegevus, mis langeb krediidiasutuse enda pädevuse piiridesse ning mida saab pidada omaseks tegevuseks krediidiasutuse toimimiseks, vaatamata sellele, kas krediidiasutus on seda kohustust varasemalt ise täitnud või mitte. Tegevuse edasiandmiseks ei loeta näiteks selliseid tegevusi, mida peavad täitma IT teenuseid pakkuvad ettevõtted seaduse kohaselt, turu-uuringuid ega muid krediidiasutusele mitteomaseid tegevusi (spetsiifilise finantsnõu andmine, klientide esindamine kohtus, krediidiasutuse valduste korrashoid jne).[40] Vastavalt peatükis 1 jõutud järeldusele, on isikusamasuse tuvastamise tegevus funktsioon, mida saab krediidiasutus anda edasi ning on kohustatud alluma kriitiliste või oluliste funktsioonide edasiandmise reeglistikule.

Sarnaselt EBA suunistele, tuleb ka Eesti seadusandluse kohaselt selleks, et funktsiooni täitmist anda teisele osapoolele edasi, krediidiasutusel sõlmida kirjalik leping teenusepakkujaga ning

[40] EBA/GL/2019/02

lepingu sõlmimisest teavitada pädevat järelevalveasutust. Osapoolte vahel sõlmitud lepingu näol on tegemist võlaõigusliku lepinguga, mis reguleerib kahe osapoole omavahelist suhtlust. Tegevuse nõuetele vastava täitmise eest jääb vastutama seaduse mõttes kohustatud isik ehk krediidiasutus olenemata sellest, et funktsiooni täitmist krediidiasutus ise ei teosta või kuidas on vastutust reguleeritud omavahelises lepingus.[41] Eeltoodust nähtub, et poolte vahel sõlmitakse tegevuse edasiandmise leping.

Tegevuse edasiandmise lepingu näol on tegemist küll võlaõigusliku suhtega, mis tähendab, et peaks olema võimalik lähtuda lepinguvabaduse põhimõttest. Tegevuse edasiandmise lepingule ning osapoolte vahelisele õigussuhtele on aga finantsinspektsioon ning EBA oma juhendites sätestanud erinevaid nõudeid krediidiasutustele selleks, et oleks võimalik tagada tegevuse jätkusuutlikus ning järelevalve teostamise võimalikkus. Viidatud juhenditest tulenevad ning need soovitused on krediidiasutustele kohustuslikud täitmiseks.[42]

Enne tegevuse edasiandmist on krediidiasutusel kohustus viia läbi taustauuring teenusepakkuja kohta. Selle eesmärgiks on tagada teenusepakkuja, kes hakkab krediidiasutusele kohustuslikku ülesannet täitma, sobivus ning kaardistada ettevõttega seonduvad riskid. Teenusepakkuja peab olema vastava kvalifikatsiooni, teadmiste ning kogemustega, võimeline oma kohustusi täitma, omama piisavat finantstausta, tema tegevuse üle peab olema võimalus teostada järelevalvet ja kontrolli krediidiasutuse poolt jne.[43]

Enne omavahelise lepingu sõlmimist peab krediidiasutus selgelt tuvastama ohud, mis sellise suhtega kaasnevad ning sellest lähtuvalt riske maandama juba enne tegevuse edasiandmist. Nendeks ohtudeks võivad olla näiteks tegevuse edasiandmise omakordse edasiandmise lubamine kolmandale osapoolele, mitmete tegevuste edasiandmine samale teenusepakkujale ja olulise tegevuse edasiandmine liiga vähestele teenusepakkujatele. Eriti oluline on viimasena mainitut jälgida kriitilise või olulise funktsiooni edasiandmisel.[44]

[41] RT I, 12.03.2022, 19.

[42] *Supra,* lk 17-18.

[43] Finantsinspektsioon. 05.08.2019.

[44] *Ibid*

Finantsinspektsiooni juhendis on esitatud nõuded tegevuse edasiandmise lepingule, mille kohaselt peavad pooled lepingus kokku leppima tegevuse olemuse, ulatuse, poolte õigused, kohustused ja vastutuse. Krediidiasutus peab lepingus määratlema nõuded osutatavale tegevusele ning teenusepakkujale, millele peab teenusepakkuja igal ajahetkel vastama. Juhendis on välja toodud välja vastutuse määratlemine, õiguskaitsevahendite kokkuleppe olemasolu osapoolte vahelises lepingus ning võimaliku kahju hüvitamiseks vajalike garantiide kehtestamine. Vaatamata nimetatule ei ole avatud seda, kas pooltel on lubatud kokku leppida, et tegevuse katkemisel ning sellega seonduvate kahjude tekkimisel, sh krediidiasutusele esitatavate nõuete ning seadusest tulenevate võimalike tagajärgede eest, saab vastutuse kanda omavahelises suhtes teenusepakkujale edasi.[45]

EBA suunised annavad krediidiasutustele täiendavad juhiseid lepingu sõlmimiseks teenusepakkujaga. On oluline, et krediidiasutusele jääks õigus ja kohustus monitoorida tegevuse korrektset toimimist ja leppida kokku tegevuse pakkumise standardid selleks, et teenuse kvaliteedi langemisel viivitamatult tegutseda. Muuhulgas on tähelepanu pööratud ka faktile, et teenusepakkuja ning krediidiasutuse vahelise lepingu sõlmimise hetkel tuleks kaaluda teenusepakkuja poolt kohustusliku kindlustuse sõlmimist teatud riskide vastu ning selle summa ulatust. Oluline on juba lepingus kujundada ka olukorrad, millistel juhtudel on võimalik osapooltel leping lõpetada. Peamiselt on nendeks juhtudeks, kui teenusepakkuja või tema poolt pakutav teenus ei vasta seaduse nõuetele, kokku lepitud nõuetele või krediidiasutuse enda poolsetele tegevuse edasiandmise nõuetele. Juhul, kui antakse edasi kriitiline või oluline funktsioon, on soovituslik krediidiasutusel omada väljumisstrateegiat juhuks, kui lõppeb leping teenusepakkujaga, teenusepakkuja ei ole võimeline tegevust pakkuma, edasiantud tegevuse osutamise kvaliteet on langenud ning sellest võivad tekkida potentsiaalsed rikkumised või on juba tekkinud. Krediidiasutused peavad tegevuse edasiandmisel tagama selle, et juhul, kui tegevuse edasiandmises tekib tagasilangus või sellest loobutakse, on krediidiasutuse tegevus endiselt kooskõlas seadusandluse ja klientide ootusega. Lisaks krediidiasutuse poolse monitoorimise võimaldamisele, on vajalik lepingus sätestada ka järelevalvet teostavate asutuste õigus saada vajalikku teavet ning teostada järelevalvet. Auditi tegemise õigus on ülioluline

[45] Finantsinspektsioon. 05.08.2019.

tagamaks kriitiliste tegevuste edasiandmise nõuete täitmist ning kompetentsete asutuste õigust järelevalveks.[46]

2.2 Krediidiasutuse ning kliendi vahelised õiguslikud suhted

Isikusamasuse tuvastamise kohustuse täitmisel juhul, kui isikusamasuse tuvastamise kohustus on antud edasi täitmiseks teisele osapoolele, st infotehnoloogilist lahendust pakkuvale ettevõttele, on üheks osapooleks klient, kelle isikusamasust krediidiasutus vastavalt seadusandlusele on kohustatud tuvastama. Krediidiasutusel on lisaks tegevuse edasiandmise lepingule lepinguline suhe ka krediidiasutuse kliendiga. See tähendab, et olukord, kus võib tekkida krediidiasutusele täiendav vastutuse dimensioon on juhul, kui temaga lepingulises suhtes kliendil tekib krediidiasutuse poolt täitmata kohustusest kahju. Oluline on märkida, et isikusamasuse tuvastamise kohustuse mittetäitmisel ei pruugi tekkida kahju. Seda olukorras, kus isikusamasuse tuvastamine on nurjunud või kui on isikusamasust tuvastatud valesti, ent kahju ei ole osapooltele tekkinud. Käesolevas alapeatükis käsitletakse olukorda, kus tekib kolmandale osapoolele ehk kliendile kahju ning kahju tekib olukorras, kus krediidiasutus on andnud edasi krediidiasutusele omase funktsiooni, mille täitmise osas on ta kohustatud isik RahaPTS mõistes, teenusepakkujale ning isikusamasuse tuvastamise kohustust on rikutud masintekkelistel põhjustel.

Krediidiasutuste seaduse kohaselt on krediidiasutuse klient iga isik, kes kasutab või on kasutanud krediidiasutuse poolt pakutavat teenust või isik, kes on krediidiasutuse poole pöördunud teenuse kasutamise eesmärgil ja kes on selle krediidiasutuse poolt identifitseeritud. Asutuse suhet kliendiga reguleerivad kirjalikus või kirjalikku taasesitamist võimaldavas või elektroonilises vormis sõlmitud eriliigilised lepingud. Krediidiasutuse ning tema kliendi vahelisi suhteid reguleerivad üldtingimused, mis peavad olema klientidele kättesaadavad. Üldtingimused on kliendi suhtes rakendatavad standardseid tingimusi sisaldav dokument, mis sätestab krediidiasutuse ning kliendi vaheliste suhete põhialuseid, suhtlemise korra ning üldised

[46] EBA/GL/2019/02

tingimused tehingute läbiviimisel. Lisaks sellele peavad üldtingimustes olema välja toodud vaidluste lahendamise kord, tähtajad ning informatsioon kliendile kaebuste esitamiseks pädevale järelevalveasutusele.[47] See tähendab, et krediidiasutuse ja kliendi vahel on lepinguline suhe.

Krediidiasutuse isikusamasuse tuvastamise kohustus kliendi ja krediidiasutuse vahelises suhtes tekib võlaõigusseaduse 2. jaost ning panga kohustusi sätestavatest üldtingimustest. See tähendab, et isikusamasuse tuvastamise kohustuse kohased nõuded saavad kliendil tekkida tuginedes üldtingimustele ning võlaõigusseaduse 2. jaole.

2.3 Teenusepakkuja ja kliendi vahelised õiguslikud suhted

Olukorras, kus krediidiasutus on sõlminud tegevuse edasiandmise lepingu teenusepakkujaga ning lepingu kliendiga, ei nähtu, et isikusamasuse tuvastamise kohustust täitva IT teenusepakkuja ja kliendi vahel oleks sõlmitud leping ja seega tekkinud lepingulised suhted osapoolte vahel.

Käesoleval juhul on võimalik käsitleda seda, kas krediidiasutuse ja teenusepakkuja vahel sõlmitud leping saab olla võlaõigusseaduse mõistes leping kolmanda isiku kasuks ehk käesoleval juhul kliendi kasuks. Kui tegemist on lepinguga, mis on sõlmitud kolmanda isiku kasuks, on kolmandal isikul, ehk kliendil, eelduslikult õigus nõuda lepingu täitmist (kui pole seaduses või lepingus teisiti ette nähtud).[48] Kolmanda isiku kasuks sõlmitud lepingus nähakse ette või selle võlasuhte olemusest tuleneb, et lepingus kokku lepitud kohustus täidetakse kolmandale isikule ning kolmandal isikul võib tekkida õigus nõuda lepingu täitmist.[49] Käesolev olukord oleks täidetud juhul, kui teenusepakkuja on sõlminud lepingu küll krediidiasutusega, ent isikusamasuse tuvastamist täidetakse kliendile ning klient saaks nõuda selle täitmist.

[47] RT I, 29.03.2022, 5.

[48] RKTK 3-2-1-85-09 p 20

[49] RT I, 15.03.2022, 14

Varasemalt on käesolevas töös aga leitud, et isikusamasuse tuvastamise kohustus lasub krediidiasutusel ning teenusepakkuja viib läbi isikusamasuse tuvastamise lähtuvalt krediidiasutusega sõlmitud lepingu alusel krediidiasutuse huvides. Seega on võimalik väita, et tegemist ei ole kliendi kasuks sõlmitud lepinguga, kuivõrd kliendil on küll huvi isikusamasus tuvastada, ent tegemist ei ole kliendil lasuva kohustusega ning on oma iseloomult krediidiasutuse huvi.

Eeltoodust lähtuvalt on võimalik jõuda järeldusele, et kliendi ja teenusepakkuja vahel ei ole lepingulisi õiguslikke suhteid. Seda, kas kliendi ja teenusepakkuja vahel saavad tekkida muudel alustel õiguslikud suhted, mis võivad tuleneda lepinguvälistest kohustustest või vastutuse liikidest, käsitletakse käesoleva töö alapeatükis 4.2.2.

3. Isikusamasuse kohustuse edasiandmisel kasutusel oleva infotehnoloogilise lahenduse olemus, sellekohane seadusandlus ning teenusepakkuja poolse vastutuse kuuluvust mõjutavad asjaolud.

3.1 Isikutuvastamisel kasutusel olevad elektroonsed lahendused

Vastavalt eeltoodud peatükkidele käsitatakse käesolevas töös infotehnoloogiliste vahenditena lahendusi, mida pakuvad ettevõtted krediidiasutustele selleks, et võimaldada isikusamasuse tuvastamise kohustuse täitmist distantsilt, kuluefektiivsemalt ja kiiremini. Selleks, et analüüsida vastavate infotehnoloogilistest lahendustest tõusetuvaid õiguslikke probleeme ning vastutusega seotud küsimusi, on esmalt vajalik tuvastada, millega on selliste lahenduste puhul tegemist. Seda seetõttu, et erinevatest lahendustest tulenevalt võivad seadusandlus ning õigusekspertide arvamused erineda. See tähendab, kas tegemist on tarkvaralise lahendusega või peab arvestama tehisintellektile sätestatud nõuete ja valitsevate arvamustega.

Teenusepakkujaid, kes pakuvad eelnimetatud isikusamasuse tuvastamise lahendusi on Eesti turul mitmeid. Selleks, et oleks võimalik jõuda järeldusele, milliseid lahendusi turul pakkuvad teenusepakkujad isikusamasuse tuvastamiseks kasutusele on võtnud, on vajalik ülevaade turul pakutavatest lahendustest.

Üheks ettevõtteks, kes pakub isikusamasuse tuvastamise ning „tunne oma klienti“ kohustuse täitmise lahendust on Veriff. Teenusest huvitatud ettevõtted saavad ostetavat teenust enda vajaduste järgi kohandada, et tagada vastavus neile kohalduvate õigusaktide ja dokumentatsiooniga ning et vältida pettuste ilmnemist. Veriff pakub eraldi finantsasutustele suunatud ja kohandatud lahendust, kasutades tehisintellekti ja masinõppimist, pakkumaks täielikult automatiseeritud identifitseerimislahendust, mis teeb otsused sekunditega. Ettevõte pakub kontole sisse logimiseks, kontole ligipääsu taastamiseks ning suuremahuliste ülekannete sooritamiseks näotuvastuslahendust ning dokumendi identifitseerimist, kasutades pilti dokumendist. Lisaks sellele kasutab tehisintellekti baasil loodud süsteem informatsiooni ka

teistest allikatest, näiteks annab täiendavat informatsiooni identifitseerimist sooviva inimese kohta, näiteks kas inimene on sanktsioneeritute või muude piirangutega nimekirjas, kas isiku kohta on muud negatiivset informatsiooni avalikes allikates ning teostab ka jooksvat monitoorimist kõige eelnimetatu üle.[50] See tähendab, et Veriff pakub tehisintellektile põhinevat lahendust isikusamasuse tuvastamiseks.

Isikusamasuse tuvastamise ning „tunne oma klienti" automatiseeritud lahendust pakub lisaks Veriffile ka etteevõte GetID. Ka GetID lahendus pakub kiiret, rahapesuvastaste õigusaktidega kooskõlas olevat lahendust. GetID kodulehe järgi kasutab ettevõte tehisintellekti tehnoloogiat selleks, et kliendi identiteeti ning dokumendi ehtsust tuvastada. Selleks võrdleb süsteemi algoritm isiku nägu tema isikut tõendava dokumendiga ning teeb kindlaks, kas on tegemist sama isikuga. Tagamaks täiendavat turvalisust, on GetID lahenduste hulgas ka kontrollmehhanism, mille eesmärgiks on tagada, et tuvastamise aluseks olevad pildid ja videod ei oleks varasemalt omandatud ja salvestatud. Selleks on süsteemi lisatud isikusamasust tuvastavale isikule erinevate ülesannete sooritamine, näiteks naeratamine, silmade pilgutamine või pea liigutamine teatud etteantud viisil. GetID kontrollib kliendi kohta käivat informatsiooni saadaval olevatest allikatest, et tuvastada isikutega seonduvaid riske, kellega krediidiasutus lepingulistesse suhetesse astub või on astunud.[51] Sarnaselt Veriffile, on ka GetID pakutav lahendus baseeritud tehisintellektile.

Lisaks eelnimetatule, pakuvad sarnaseid isikusamasuse tuvastamise lahendusi ka ettevõtted Basis ID[52] ja Jumio[53], kes on samuti suunanud oma teenuseid krediidiasutustele selleks, et tagada krediidiasutuse tegevuse kooskõla rahapesu ja terrorismi rahastamise tõkestamise nõuetega ning klientide isikusamasus. Mõlemad ettevõtted rakendavad tehisintellekti kasutavat lahendust selleks, et tuvastada krediidiasutuste klientide isikusamasus, leida nende kohta

[50] Veriff. AML & KYC compliance solution. Veriff kodulehekülg. Arvutivõrgus: https://www.veriff.com/product/aml-kyc-compliance (03.04.2022)

[51] GetID. A complete Identity verification and KYC solution for fintech companies. GetID kodulehekülg. Arvutivõrgus: https://getid.com/industries/fintech/ (03.04.2022)

[52] Basis ID. KYC and AML solution. Basis ID koduleht. Arvutivõrgus: https://www.basisid.com (03.04.2022)

[53] Jumio. Automated identity proofing, eKYC and transaction monitoring. Jumio koduleht. Arvutivõrgus: https://www.jumio.com/products/ (03.04.2022)

informatsiooni saadaval olevatest allikatest ning tuvastada kliendi kohta esitatud andmete õigsust.

Tegemist ei ole ammendava nimekirjaga teenusepakkujatest, kes pakuvad elektroonset isikutuvastamise lahendust. Käesoleva peatüki kirjutamise käigus tutvus töö autor mitmete erinevate kodulehtedega. Lisaks töös välja toodud Veriff, GetID, Basis ID ja Jumiole, pakuvad isikusamasuse tuvastamise teenust lisaks SumSub[54] ning Passbase[55], ent kumbki koduleheküIg ei sisalda informatsiooni, milliseid lahendusi on kasutusele võetud selleks, et isikute isikusamasust tuvastada läbi erinevate andmebaaside, vaid tutvustatakse teenuseid ning võimalusi, mida ettevõte pakub. Samuti pakutakse turul rahapesu tõkestamiseks vajalikke teenuseid, mis abistavad krediidiasutusi rahapesu vastaste õigusaktide täitmisel ning klientide monitoorimisel, ent ei ole kasutatavad isikusamasuse tuvastamisel, näiteks Coinfirm ja Comply Advantage.

Vastavalt eeltoodule, on töö autori järeldus, et suur osa leitavatest isikusamasuse tuvastamise lahendustest ning teenusepakkujatest kasutab krediidiasutuse klientide tuvastamiseks tehisintellektile baseeritud lahendusi. See tähendab, et käesoleva magistritöö raames tehtud järeldused masinvastutuse osas isikusamasuse tuvastamise kontekstis, baseeruvad teenusepakkujatele, kes on laialt levinud ning kergesti leitavad ning kasutavad isikusamasuse tuvastamisel tehisintellekti lahendusi.

Tuginedes teenusepakkujate poolt pakutavate lahenduste kirjeldustele, tuvastatakse krediidiasutuse klientide isikusamasus tehisintellekti abil automatiseeritud viisil, mis on võimeline ise õppima ning teeb otsuseid väga kiiresti. Levinud on tehisintellekti abil näotuvastusfunktsioon, mille läbi võimaldatakse isikul end tuvastada sisse logides või ülekandeid tehes. Näotuvastusel võrreldakse isiku reaalajas kuvatavat nägu tema isikut tõendava dokumendiga. Läbi tehisintellekti on näotuvastusel võimalik lisada kontrollmehhanisme, mille alusel saab tehisintellekt saavutada kõrgema tõenäosusprotsendi, et tegemist on korrektse isikuga. Tehisintellekt võimaldab süsteemil isiku tuvastamisel kasutada

[54] Sumsub. Sumsub koduleht. Arvutivõrgus: https://sumsub.com (10.04.2022)

[55] Passbase. Passbase koduleht. Arvutivõrgus: https://passbase.com (10.04.2022)

informatsiooni ka teistest allikatest väga lühikese aja jooksul ning monitoorib allikates kliendi kohta sisalduvat teavet jooksvalt ajas.

3.2 Tehisintellekt ja selle kasutus finantssektoris

Tehisintellekti roll ja kasutus on 21. sajandil laialt levinud. Kuigi tehisintellekti definitsioon on endiselt ebaselge (legaaldefinitsioon on Euroopa Liidu Komisjoni ettepanekul loomisel), siis üheks võimaluseks on seda defineerida kui arvutiprotsessi loomist, mis käitub viisil, mida tavaline isik peaks intelligentseks.[56] Tehisintellekti saab defineerida veel ka kui arvuteid, mis viivad läbi toiminguid, mida varasemalt arvati, et ainult inimesed on võimelised tegema ning mis on masinõppevõimekad ehk masin kasutab reegleid, et analüüsida andmeid, avastada ja tunda ära mustreid ja selle pinnalt teha ennustusi. Kuigi arvatakse, et tehisintellekt asendab inimelementi, ei tähenda siiski tehisintellekti kasutuselevõtt seda, et inimesi vastavate protsesside juures enam ei vajata. Justnimelt inimesed on vajalikud selleks, et luua reegleid ja parameetreid seadmetele, et masinõpe oleks võimalik. Seda eriti tehisintellekti loomise algfaasis. Ka õigusvaldkonna tegevustes on tehisintellekti kasutusele võtmiseks mitmeid võimalusi, näites olukordades, kus on vajalik suure andmekogu analüüs või korduv ja blanketne tegevus.[57]

Tehisintellekti kasutus finantssektoris on kasvanud alates 2000ndatest aastatest ning olenevalt sektorist, võib selle kasutusulatus moodustada suure osa tegevusest, näiteks tehisintellekti baasil loodud kauplemisvahenditega sooritatud tehingud.[58] Erinevatest uuringutest nii

[56] Rajpurohit, D. S; Seal, R. Legal definition of artificial intelligence. Supremo Amicus 10, 2019, lk 87-95. Arvutivõrgus: https://heinonline-org.ezproxy.utlib.ut.ee/HOL/Page?public=true&handle=hein.journals/supami10&div=17&start_page=87&collection=journals&set_as_cursor=24&men_tab=srchresults (03.04.2022)

[57] Shields, A. C. Managing artificial intelligence. Law Practice, vol 45, issue 3, 2019, lk 14-15. Arvutivõrgus: https://heinonline-org.ezproxy.utlib.ut.ee/HOL/Page?collection=journals&handle=hein.journals/lwpra45&id=177&men_tab=srchresults (03.04.2022)

[58] Euroopa Keskpank, pangandusjärelevalve. Algorithmic trading: trends and existing regulation. Euroopa Keskpank, pangandusjärelevalve koduleht. Arvutivõrgus:

Ühendkuningriikides kui ka Hong Kongis, on selgunud, et enam kui pooled finantsasutused kasutavad või on kasutusele võtmas tehisintellekti baasil toimivad süsteemid selleks, et vältida rahapesu, kelmusi, küberkuritegevust ning abistada klienditoe ning muuhulgas ka isikute tuvastamisega. Sarnaselt käesoleva töö peatükis 1.1 välja toodud üldiste elektroonsete lahenduste eelistega, oodatakse tehisintellekti implementeerimisest samuti uut efektiivsust, kulude vähenemist ja uutmoodi väärtuste loomist finantssektoris. Finantssektor tervikuna soodustab tehisintellekti kasutuselevõttu seoses finantssektorile kuuluvate omadustega. Nendeks on laialdaste digiteeritud andmete olemasolu mitmekümnete aastate ulatuses ja kindlate reegli- ja parameetripõhiste otsuste tegemise vajadus, millele saab tehisintellekt tugineda ning inimestest efektiivsemalt ja kiiremini otsuseid langetada. Kõik eelnimetatu on oluline seetõttu, et tegevusega kaasnevad kohustused seadusandluse mõttes on ulatuslikud ning ajas kasvanud. Selleks, et vältida sanktsioone ja tagada nõuete, sh rahapesu vastaste nõuete täitmine, mida varasemas infotehnoloogia kauges keskkonnas olid võimelised inimesed mõistliku aja ja tööjõukuluga läbi viima, on finantsasutused keskendunud tehisintellekti potentsiaali ärakasutamisele.[59]

Tehisintellektiga kaasnevad ka riskid. Kuigi tehisintellekti ja tehnoloogia kasutus on võimaldanud luua abivahendid seaduse nõuete täitmiseks, rahapesu tõkestamiseks ning pettuste avastamiseks, siis paradoksaalsel viisil on ühed suurimad viimaste aastate trahvid määratud krediidiasutustele, kelle tegevuses on realiseerunud tehnoloogiast tulenevad riskid.[60] Tehisintellekt konkureerib inimestega kui ressurss, kes analüüsib ja teeb otsuseid. Selle tagajärg ühiskonnale ja tööturule võib olla märkimisväärne. Lisaks sellele võib tehisintellektil olla võimekust täita kohustusi, ent tehisintellekti vastutama panemine on komplitseeritud. Tehisintellekti kasutusega võib tekkida oht, et inimesed kasutavad tehisintellekti selleks, et anda üle oma kohustused ja ise vabaneda endale kuuluvast vastutusest. Kuna tehisintellekt omab võimekust mõelda, õppida ja teha otsuseid väga kiiresti ja efektiivsemalt kui inimesed, võib tekkida olukord, kus inimestel on väga keeruline mõista ja hinnata tehisintellekti otsuste

https://www.bankingsupervision.europa.eu/press/publications/newsletter/2019/html/ssm.nl190213_5.et.html (10.04.2022)

[59] Buckley, R.P.; Zetzsche, D. A.; Arner, D. W; Tang, B.W. Regulating artificial intelligence in finance: putting the human in the loop. Sydney Law Review, 42 (1), 03.2021, lk 43-82. Arvutivõrgus: https://heinonline-org.ezproxy.utlib.ut.ee/HOL/Page?public=true&handle=hein.journals/sydney43&div=5&start_page=43&collection=journals&set_as_cursor=0&men_tab=srchresults (13.04.2022)

[60] Buckley, R.P.; Zetzsche, D. A.; Arner, D. W; Tang, B.W. 03.2021, lk 53-54.

tegemise protsessi ja käitumise muutumist. Seoses tegutsemiskiirusega, võivad suuremad olla ka vigadest tekkinud tagajärjed, kuna vastavate vigaste andmete või tegude tõttu on tehisintellektil võimekus oma tegevust korrata suurtel kiirustel korduvalt. Tehisintellekti puuduseks loetakse ka tema jäikust, mille tõttu ei ole tehisintellekt võimeline lähtuma olukordade spetsiifikast, tegema kompromisse või reeglitest põhjendatud juhtudel kõrvale kalduma. Kõiki eeltoodud riske teadvustades, on tehisintellekti kasutuselevõtt juba alanud ning mingis ulatuses ka paratamatus.[61] Seetõttu on vajalik luua tehisintellektile õiguslik raamistik, mis sätestab printsiibid, mis võimaldavad valdkonda turvaliselt arendada.[62]

3.3 Tehisintellekti käsitlevad õiguslikud dokumendid

2019. aastal avaldas Euroopa Komisjoni poolt moodustatud sõltumatu kõrgetasemeline tehisintellekti eksperdirühm eetikasuunised usaldusväärse tehisintellekti arendamiseks.[63] Suuniste eesmärgiks on edendada usaldusväärset tehisintellekti tagades, et tehisintellekti tegevus oleks seaduspärane, eetiline ning robustne. Kõige eelnimetatu eesmärk on tagada, et ühiskond tunneks end turvaliselt, et tehisintellekt ei põhjustaks ettenägematuid tagajärgi ega kahju ning oleks kooskõlas erinevate tavade ja kultuuridega.[64] Suunised annavad riikidele juhised, kuidas jõuda suunises välja toodud tulemusteni, ent suuniste implementeerimine siseriiklikusse õigusesse ei ole Euroopa Liidu riikidele kohustuslik, vaid pigem julgustatakse nii ettevõtteid kui ka riike neid arvesse võtma.[65] Suunistes sisalduvad printsiibid on loodud

[61] Whittaker, A. Artificial intelligence – the new EU guidlines. Journal Of International Banking Law and Regulation, 2019, 34(9), lk 295-200.

[62] Karu, K. Tehisintellekti keerukad küsimused. Juridica 1/2021, lk 43-54.

[63] Sõltumatu kõrgetasemeline tehisintellekti eksperdirühm (AI HLEG), Eetikasuunised usaldusväärse tehisintellekti arendamiseks. 08.04.2019. Euroopa Liidu Väljaannete Talituse koduleht. Arvutivõrgus: https://op.europa.eu/et/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1 (13.04.2021)

[64] Burkadze, K. The legal aspects of artificial intelligence based on the EU experience. Law and World, 2021, 20, lk 8-12. Arvutivõrgus: https://heinonline-org.ezproxy.utlib.ut.ee/HOL/Page?public=true&handle=hein.journals/lwwrld20&div=4&start_page=[8]&collection=journals&set_as_cursor=1&men_tab=srchresults

[65] Whittaker, A. 2019, lk 299.

tuginedes Euroopa Liidu konventsioonidele ja põhiõiguste hartas sisalduvatele fundamentaalsetele väärtustele.[66]

Võttes arvesse ekspertrühma soovitusi, avaldas Euroopa Komisjon valge raamatu, mis käsitles euroopa käsitust tipptasemel ja usaldusväärsest tehnoloogiast tehisintellekti kasutusel. Dokument lõi ühtse arusaama tehisintellekti käsitusest Euroopale ning arengusuuna innovatsioonisuutlikkuse edendamiseks tehisintellekti valdkonnas, rõhutades Euroopa Komisjoni toetavat suhtumist tehisintellekti kasutuselevõtu osas.[67] Vastusena Euroopa Komisjoni valgele raamatule, koostas Euroopa Parlament aastal 2020. Euroopa Komisjonile resolutsiooni tehisintellekti, robotitehnoloogia ja seonduva tehnoloogia eetiliste aspektide[68] ning tehisintellekti tsiviilvastutuse[69] korra kohta. Euroopa parlamendi resolutsioonide põhjal tegi 2021. aastal Euroopa Komisjon Euroopa Parlamendile ja nõukogule ettepaneku kehtestada määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte. Vastav ettepanek on käesoleva magistritöö kirjutamise ajal on läbinud esimese lugemise Euroopa Nõukogus, ent menetlusega Euroopa Parlamenti esimesele lugemisele jõudnud ei ole. Määruse eesmärgiks on kehtestada ühtlustatud õigusnormid, mis käsitlevad tehisintellekti, kuna tehnilised muutused on kiired ja võimalikke probleeme võib esineda rohkelt. Seda eelkõige seetõttu, et Euroopa Komisjoni hinnangul on tehisintellektil potentsiaali luua majanduslikke ja ühiskondlikke hüvesid ning luua konkurentsieeliseid ettevõtjatele ja Euroopa majandusele.[70] Võrreldes Euroopa Komisjoni poolt koondatud dokumenti eksperdirühma suunistega, on tegemist konkreetsete ettepanekute ning liikmesriikidele õiguslikult siduvate seisukohtadega, mis jõuavad liikmesriikide

[66] Cyman, D. Regulation of Artificial intelligence in BRICS and the European Union. BRICS Law Journal, vol 8, nr 1, 2021, lk 86-115.

[67] Euroopa Komisjon, 19.02.2020. Valge raamat. Tehisintellekt: Euroopa käsitlus tipptasemel ja usaldusväärsest tehnoloogiast. Brüssel, COM(2020) 65 final. Arvutivõrgus: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_et.pdf (15.04.2022)

[68] 20.10.2020, Euroopa Parlament, tehisintellekti, robootika ja seonduva tehnoloogia eetiliste aspektide raamistik. P9_TA(2020)0275. Arvutivõrgus: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ET.pdf (13.04.2022)

[69] 20.10.2020, Euroopa Parlament, tehisintellekti tsiviilvastutuse kord. P9_TA(2020)0276. Arvutivõrgus: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_ET.pdf (13.04.2022)

[70] 21.04.2021 Euroopa Komisjon, Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte. ELT COM/2021/206 final. Arvutivõrgus: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0017.02/DOC_1&format=PDF (13.04.2022)

seadusandlusesse. Kuna määrus ei ole Euroopa Parlamendi ja Nõukogu poolt kehtestatud, siis käesoleval juhul ei ole võimalik tehisintellektist tõusetuvaid küsimusi kõne all oleva määruse abil lahendada. Võimalik on võtta arvesse Euroopa Komisjoni poolt välja kujunenud seisukohad ning suuna, kuhu Euroopa Liidu seadusandlus on liikumas.

Sarnaselt Euroopa Liidu ülesele initsiatiivile luua tehisintellektile õigusraamistik ja parim strateegia tehisintellekti implementeerimiseks igapäevaellu, kutsus Eesti 2018. aastal kokku ekspertrühma, et kaardistada meetmeid, läbi mille saaks enim kasu tehisintellektist ja kuidas oleks võimalik tehisintellekti kasutuselevõttu toetada. Vastavas protsessis nimetatakse tehisintellekti kratiks.[71] Kuna ka Eestis järjest rohkem ülesandeid automatiseeritakse kasutades tehisintellekti, siis tuvastati vajadus leida konkreetsem sisu tehisintellekti puudutavale seadusandlusele.[72] Majandus- ja Kommunikatsiooniministeeriumi eesmärgiks oli eristuda mujal maailmas valitsevast praktikast, mille kohaselt lähtutakse tehisintellekti reguleerimisel valdkonnapõhisest lähenemisest, luues ühe seaduse, mis reguleerib kogu tehisintellektiga seonduvat, olles samal ajal piisavalt üldine ilma tehnoloogilistesse eripäradesse laskumata. Seda seetõttu, et kiiresti muutuvas valdkonnas võib liigne detailsus pidurdada innovatsiooni. Selle selgituseks toob ministeerium, et probleemküsimused andmekaitse, privaatsuse, vastutuse, eetika ja moraali kohta on valdkondade üleselt sarnased. Samuti on üheks oluliseks loodava raamistiku aspektiks toodud küsimus vastutusest, mida oleks võimalik tuvastada ka valdkonna osas eriteadmisi mitte omava isiku poolt.[73] Ekspertrühma poolt kujundatud seisukohtade baasilt on koostatud algoritmiliste süsteemide mõjude reguleerimise väljatöötamise kavatsus ehk krati väljatöötamise kavatsus aastal 2020. Kavatsus kaardistab olemasolevaid probleemkohti, kirjeldab hetkeolukorda, pakub lahendusi tõusetuvatele probleemidele ning analüüsib õigusliku regulatsiooni mõjutusi ning loomist. Muuhulgas käsitletakse kavatsuses tehisintellekti poolt tehtud vigu, mille tekkimist on inimesel (sh inimesel kes on algoritmi loonud) keeruline selgitada. Samuti tõusetuvaid probleeme, mille korral võib tekkida põhiõiguste rikkumine, kahju või diskriminatsioon. Dokumendis sisalduv eelnõu kavand loob selged paragrahvid, mille kehtestamisel oleks võimalik tagada

[71] Kratid Eesti heaks. Krattide projekti koduleht. Arvutivõrgus: https://www.kratid.ee (14.04.2022)

[72] Tehisintellekti kasutus peab austama põhiõigusi. 18.08.2020. Justiitsministeeriumi koduleht. Arvutivõrgus: https://www.just.ee/uudised/tehisintellekti-kasutus-peab-austama-pohioigusi (15.04.2022)

[73] Kaevats, M. Kuidas kratt Eesti paremaks teeb? 23.07.2018. Arvutivõrgus: https://medium.com/digiriik/kuidas-kratt-eesti-paremaks-teeb-cfebc526cb47 (15.04.2022)

tehisintellekti läbipaistvus ja inimeste põhiõigused ning luua kõrgendatud nõuded suurema riskiga tehisintellekti süsteemidele, mille mõju inimeste põhiõigustele on ulatuslikum. Vastava kavandi lõppeesmärgiks oli uue tehisintellekti seaduse koostamine, mille eeldatavaks jõustumise ajaks ennustati aastat 2022.[74] Töö kirjutamise hetkel 2022. aasta esimeses pooles ei ole vastav seadus jõustunud ning ei ole võimalik välja tuua ka konkreetseid tehisintellekti puudutavaid sätteid olemasolevas seadusandlusest.

Krati eelnõu ja plaan tehisintellekti reguleerida eraldi seadusega tekitas vastukaja ning mitmete ekspertide hinnangul vastavat valdkonda selliselt reguleerida ei ole võimalik. On seisukohti, mille kohaselt ühte kõikehõlmavat seadust koostada, mis käsitleks kõiki tehisintellektiga seonduvaid küsimusi, ei ole otstarbekas, kuna valdkonna ülereguleerimine võib takistada valdkonna arengut Eestis. Erinevate hinnangute kohaselt arvatakse, et Eesti peaks võtma sarnase lähenemise Euroopa Liidule ja selle liikmesriikidele, kus enne rangete õigusraamistike loomist peaks eelkõige leppima kokku eetilistes põhimõtetes ning vahendites põhiõiguslike riivete vältimiseks.[75] Samuti on tõusetunud küsimus sellest, kas tehisintellektiga seonduv peaks olema aluseks olemasolevate seaduste muutmiseks ja uute loomiseks või piisaks olemasolevast õiguskorrast.[76]

3.4 Vastutusküsimused tehisintellekti käsitlevates õiguslikes dokumentides

Vastavalt eeltoodule on võimalik jõuda järeldusele, et tehisintellekt on dünaamiline, iseõppiv ning otsuseid iseseisvalt vastu võttev süsteem, mille osatähtsus finantssektoris on tõusuteel. Nagu eelpool mainitud, võib tekkida taolistest lahendustest oht, kus isikud, kelle otsustuskohustused kantakse üle tehisintellektile, vabanevad taolisest vastutusest, kuna otsust

[74] Algoritmiliste süsteemide mõjude reguleerimise väljatöötamise kavatsus („krati VTK“). 14.08.2020, Justiitsministeeriumi avalik dokumendiregister. Arvutivõrgus: https://adr.rik.ee/jm/dokument/7458502 (15.04.2020)

[75] Ojamets, I. Juristid jäävad krattide kasutamise reguleerimisega kimbatusse. 02.11.2020. Arvutivõrgus: https://novaator.err.ee/1154043/juristid-jaavad-krattide-kasutamise-reguleerimisega-kimbatusse (15.04.2020)

[76] Turk, K; Pild, M. Kratiga või kratita- see on küsimus. Robititest ja tehisintellektist tsiviilõiguslikult.. Juridica 1/2019, lk 43.

langetanud nad isiklikult ei ole. Isikusamasuse tuvastamisel kasutatakse valdavalt just tehisintellektile baseeruvaid lahendusi, mis on oluline nii krediidiasutusele oma kohustuste täitmiseks kui ka klientidele neile oluliste teenuste kättesaadavuseks. Seetõttu on oluline vastata küsimusele, kes vastutab juhul, kui tehisintellekt on toime pannud rikkumise või on teinud vea, mille eest tekib vastutus ning kas taolist vastutuse tekkimist on võimalik üle kanda ka käesolevas töös käsitlevale teemale ehk isikusamasuse tuvastamise kohustuse täitmisele kasutades tehisintellekti?

Eksperdirühma eetikasuunistes on toodud välja II peatükis ühe aspektina usaldusväärse tehisintellekti teostamiseks vastutuse võtmine. Suunise mõttes on tegemist nõudega, mis on seotud õigluse põhimõttega ning mille kohaselt on vajalik luua mehhanismid, mis abistaksid vastutuse kandmise ja võtmise küsimustes tehisintellekti süsteemide ja nende väljundite eest. Vastutuse võtmine tähendab suuniste mõttes tehisintellekti auditeeritavust, negatiivsete mõjude minimeerimist ja neist teatamist, kompromisside tegemist ja õiguskaitset. Sellekohaselt on kohustus tagada tehisintellekti nõuetelevastavus näiteks läbi auditeerimistegevuse, teavitada koheselt ilmnenud negatiivsetest tagajärgedest ja rikkumistest ning tagada piisav õiguskaitse juhuks, kui toimub kõrvalekalle normaalsusest ning seetõttu tekib ebaõiglaselt kahjulik süsteemi mõju. Kuigi juhend selgitab, et tehisintellekti käitumismustrid tuleks kohandada vastavalt õiguslikule raamistikule ja muudele käitumisjuhistele ning suunistab organisatsioone looma raamistikke, mis tagaksid vastutuse võtmise eetiliste aspektide eest, ei lahenda dokument vastutusküsimust selle osas, kes vastutab või kuidas vastutus jaguneb tehisintellekti poolt teostatud vigase käitumise tõttu.[77]

Euroopa Parlamendi ja nõukogu määrus, mis magistritöö kirjutamise ajal ei ole veel jõustatud, käsitleb vastutuse probleemi ulatuslikumalt, kuid vaid suure riskiga tehisintellektisüsteemide osas. Määrus sätestab lõikes 53, et suure riskiga tehisintellektisüsteemi turule laskmisega või selle kasutusele võtmise eest võtab vastutuse konkreetne füüsiline või juriidiline isik, kes on tehisintellekti puhul pakkujaks, olenemata asjaolust, kas konkreetne isik on seda süsteemi projekteerinud või arendanud. Käesoleva sätte sõnastus viitab asjaolule, et taoline vastutus on kohaldatav vaid juhul, kui kõne all olev tehisintellekt kvalifitseerub suure riskiga

[77] Sõltumatu kõrgetasemeline tehisintellekti eksperdirühm (AI HLEG), 08.04.2021, lk 15-27.

tehisintellektisüsteemina. Määruse mõistes on suure riskiga tehisintellektisüsteemid need, mis põhjustavad märkimisväärseid riske isikute ohutusele, põhiõigustele või tervisele ehk tehisintellektisüsteemid, mis on mõeldud kasutamiseks selliste toodete turvakomponendina, mille kohta teeb kolmas isik vastavuse eelhindamise, eelkõige masinad, mänguasjad, liftid, raadioseadmed jne, või III lisas loetletud süsteemid.[78] Nendeks on näiteks tehisintellektisüsteemid, mis on mõeldud füüsiliste isikute reaalajas ja tagantjärele toimuva biomeetrilise tuvastamise jaoks, maanteeliikluse korraldamise ja käitamise turvakomponentidena jne.[79] Määruse lõikes 33 alusel märgitakse, et „füüsiliste isikute biomeetrilise kaugtuvastamise jaoks mõeldud tehisintellektisüsteemide tehniline ebatäpsus võib kaasa tuua tulemuste kallutatuse ja põhjustada diskrimineerimist. Eriti oluline on see vanuse, etnilise päritolu, soo või puuete puhul. Seepärast tuleks nii reaalajas kui ka tagantjärele toimuva biomeetrilise kaugtuvastamise süsteemid liigitada suure riskiga süsteemideks.“[80] Eelnimetatud sätetest on võimalik teha järeldus, et isikusamasuse tuvastamisel kasutusel olevad tehisintellektisüsteemid on suure riskiga tehisintellektisüsteemid Euroopa Komisjoni ettepaneku mõistes. Seega isikusamasuse tuvastamise kohustuse täitmiseks rakendatavad teenusepakkuja poolsed tehisintellekti lahendused kuuluvad käesoleva määruse kohaldamislasse kui suurema riskiga tehisintellektisüsteemid ning töös tõusetuvate vastutusküsimuste lahendamisel saab tugineda määruses esitatud seisukohtadele. Määruse lõike 53 sõnastus viitab sellele, et füüsiline või juriidiline isik on kohustatud võtma küll kogu vastutuse turule laskmise ja kasutusele võtmise eest, ent jääb selgusetuks, kas sätte mõte on ka vastavale isikule panna vastutust suure riskiga tehisintellektisüsteemi kasutusele võtmisel tekkinud rikke või selle tagajärgede eest. Käesolevas töös käsitletava teema raames oleks kõige tõenäolisemalt vastavaks juriidiliseks või füüsiliseks isikuks ettevõte ise või isik, kes omab kõige rohkem kontrolli toote pakkumise, turule laskmise ja kasutusele võtmise üle.

Euroopa Komisjoni ettepanek baseerub Euroopa Parlamendi resolutsioonidele, mille esitas Euroopa Parlament komisjonile seoses tehisintellekti vastutuse ja eetiliste aspektide raamistiku

[78] 21.04.2021 Euroopa Komisjon

[79] Lisad järgmise dokumendi juurde: Euroopa Komisjon, 21.04.2021 Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte. ELT COM/2021/206 final. Arvutivõrgus: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0017.02/DOC_2&format=PDF (13.04.2022)

[80] 21.04.2021 Euroopa Komisjon

loomisega. Euroopa Parlamendi soovitustega resolutsioon tehisintellekti tsiviilvastutuse korra kohta on väga detailne vastutuse mõiste osas ning käsitleb konkreetselt kahepoolset suhet, kus üks on teise ees vastutav. Resolutsioonis on välja toodud, et tehisintellekti süsteemide puhul on aktuaalsed vastutusekohased õiguslikud probleemid, sest tegemist on läbipaistmatute süsteemidega, mille puhul võib olla väga keeruline või võimatu selgeks teha, kes omas kontrolli tehisintellektiga seotud riski üle või millised asjaolud, näiteks kood, sisend või andmed, vastutuse aluseks oleva tagajärje põhjustasid. Seetõttu on raskendatud isikute vastutusele võtmine. Selleks on parlamendi hinnangul vajalik täiendavad kohandused õigusnormides, et tehisintellekti keeruka süsteemi puhul oleks võimalik tuvastada vastutus. Lisaks sellele toob parlament välja, et tehisintellekti süsteemide rikete puhul leidub alati isik, kes on süsteemid loonud, rakendusse võtnud või nende töösse sekkunud, ent kuna selle tuvastamine valdkonna spetsiifika tõttu on keeruline, oleks vajalik vastutavaks muuta süsteemiga seotud riske tekitavaid, alalhoidvad või kontrollivaid isikuid kogu väärtusahela ulatuses. Välja on toodud, et tehisintellekti süsteemide käitaja vastutus peaks sarnanema suurema ohu allika poolse tekitatud süüta vastutusena, mis võimaldaks rikkumisest mõjutatud isikutel, kellel puudub lepinguline suhe tehisintellekti manageeriva juriidilise või füüsilise isikuga, panna vastutama tehisintellekti üle kontrolli omav või tehisintellekti anomaalia põhjustanud isik.[81] Euroopa Komisjon ei ole enda ettepanekus Euroopa Parlamendile ja nõukogule eeltoodud vastutuse tõlgendustega arvestanud ning on tsiviilvastutust enda ettepanekus käsitlenud minimaalselt. Parlamendi poolsed Euroopa Komisjoni valgele raamatule baseeruvad ettepanekud ja argumentatsioonid on põhjalikud ja annaksid selgust Euroopa Liidu ülese tehisintellekti poolsest rikkumisest tekkinud vastutuse jagunemise kohta. Kuna see analüüs aga Euroopa Komisjoni konkreetses ettepanekus ei kajastu, siis käesolevad seisukohad ei ole hetkel ega tulevikus kinnitatava Euroopa Parlamendi ja komisjoni määrusega Euroopa Liidu tasandil reguleeritud. Arvestades Euroopa Komisjoni ning Euroopa Parlamendi seisukohti ning defineeritud Euroopa käsitust tehisintellektiga seotud õigusraamistikust, on võimalik jõuda järeldusele, et vastutuse reguleerimine tulevikus Euroopa Liidu tasandil on vältimatu.

Majandus- ja Kommunikatsiooniministeeriumi krati eelnõus on vastutuse kohase seisukoha võtmisel tuginetud Euroopa Nõukogu soovitusele tagada tehisintellekti auditeeritavus,

[81] 20.10.2020, Euroopa Parlament, tehisintellekti tsiviilvastutuse kord.

negatiivse mõju minimeerimine ja teatamine, kompromissid ja õiguskaitse. Eelnõus pole aga teadlikult vastutuse jagunemise kohta seisukohta võetud seoses Euroopa Liidu ülese ühtse seisukoha puudumisega.[82]

3.4.1 Vastutus tehisintellekti tagajärjel tekkinud masintekkelisel rikkumisel

Eeltoodud peatükkidest 3.3 ja 3.4 selgub, et Euroopa Liidu üleselt ei ole kehtestatud üheseid reegleid ning lahendusi selleks, et tuvastada vastutuse jagunemine juhul, kui tehisintellekti poolt sooritatud tegevuse tagajärjeks on kokkulepitud kohustuste rikkumine. See tähendab, et eeltoodu alusel ei ole võimalik teha järeldusi vastutuse jagunemise kohta isikusamasuse tuvastamisel kasutusel olevate tehisintellektisüsteemide rikete korral. Juhul, kui toimub rikkumine isikusamasuse tuvastamisel kasutades tehisintellekti, jääb küsimus, et kes kannab tehisintellekti poolt toime pandud teo eest vastutust. Veel enam, kas on võimalik seda vastutusküsimuse lahendust üle kanda ka käesolevas töös käsitletud olukorrale, kus tehisintellekt on kasutusel isikusamasuse tuvastamise kohustuse täitmisel ning isikusamasuse tuvastamise kohustus on krediidiasutuse poolt täitmiseks edasiantud .Kuna puuduvad Eesti siseriiklikud ning Euroopa Liidu ülesed jõustatavad õigusraamistikud, siis käesolevale küsimusele, kuidas võiks jaguneda vastutus juhul, kui tehisintellekti kasutamisel toimub masintekkeline rike, on vajalik vastata tuginedes õiguskirjandusele ning Euroopa Liidu institutsioonide juhenditele ja käsitustele käesolevast teemast.

Vastutusküsimuse lahendamisel on osapooli, kes rikkumise eest vastutust kanda võiksid mitmeid. Näiteks isik, kes kasutas tehisintellekti, tehisintellekti ja selle parameetreid seadistanud spetsialist, tehisintellekti kasutusele võtmise otsuse teinud isik, tehisintellekti loonud ettevõtte juht, tehisintellekti algoritmide programmeerija või isik, kes valis andmed programmi treenimiseks. Kuna tehisintellekt ise ei oma teadvust, siis seadusandluse kohaselt ei ole võimalik tehisintellekti vastutama panna. Olukord on tehisintellekti puhul mõnevõrra erinev

[82] Algoritmiliste süsteemide mõjude reguleerimise väljatöötamise kavatsus („krati VTK“). 14.08.2020

muude arvutisüsteemidega seonduvatest vastutusküsimustest, sest tehisintellekti käsitletakse iseseisvate otsuste tegijana.[83]

Tehisintellekti vastutuse küsimust käsitles esimest korda põhjalikumalt Euroopa Komisjon 19.02.2020 avaldatud valges raamatus, milles kirjeldas Euroopa käsitust tehisintellektist ja tehnoloogiast.[84] Valge raamatu juurde kuulub komisjoni aruanne, mis käsitleb ohutus- ja vastutusraamistikku. Olemasolevate ohutus- ja vastutusraamistike eesmärgiks on tagada, et kõik tehisintellekti sisaldavad teenused ja tooted, oleksid ohutud, usaldusväärsed ning nendega tekkinud kahju saaks hüvitatud. Vastutuse osas on oluline tagada, et kasutajatele pakutav kaup oleks ohutu ning ohtu sattumise risk on väike ning juhul, kui tekib kahju, saab kahju hüvitatud. Sellise olukorra lahenduseks pakub Euroopa Komisjon tootevastutuse direktiivile tuginemist, millele on võimalik tugineda juhul, kui pakutav toode või teenus on defektne ning mis pakub mittesüülist vastutust. See võimaldab toote loonud isikule panna vastutus ilma, et oleks vajalik tuvastada süü olemasolu ning aitab vältida olukordi, kus on keeruline tuvastada kahju tekitanud inimkäitumist.[85] Samas nenditakse, et tehisintellekti iseloomust ja omadustest tulenevalt võib olla keeruline tootevastutusraamistike kohaldada. Selleks, et tootevastutust rakendada, on vajalik negatiivne tagajärg seostada isikuga, mis võib tehisintellekti puhul olla raskendatud. Seetõttu tehakse ettepanek kaaluda tootevastutuse direktiivi vastavaks muutmist, et ei tekiks olukorda, kus ei oleks võimalik tehisintellekti tegevuse eest kedagi vastutusele võtta. Euroopa Komisjoni aruandest selgub veel, et tootevastutuse direktiivi on võimalik rakendada vaid juhul, kui tekib teenuse või toote kasutajale füüsiline või materiaalne kahju. Olukorra kohta, kus tehisintellekt on toime pannud rikkumise, mille tagajärjed on teise iseloomuga, näiteks isikuandmete lekkimine, ei anna Euroopa Komisjoni aruanne vastuseid. [86]

Euroopa Parlamendi poolt koostatud tehisintellekti tsiviilvastutuse kord kordab suures osas Euroopa Komisjoni arvamust vastutuse osas, ent mõnevõrra eemaldub vastutuse sidumisest

[83] Karu, K. Lk 53

[84] Euroopa Komisjon, 19.02.2020. Valge raamat.

[85] Euroopa Komisjon, 19.02.2020. Komisjoni aruanne Euroopa Parlamendile, nõukogule ning Euroopa Majandus- ja Sotsiaalkomiteele. Aruanne selle kohta, milline on tehisintellekti, asjade interneti ja robootika mõju ohtutusele ja vastutusele. Brüssel, COM(2020) 64 final. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52020DC0064&from=ET (15.04.2022)

[86] Euroopa Komisjon, 19.02.2020. Valge raamat.

vaid varalise kahju tekkimise olemasoluga. Nimelt Euroopa Parlamendi resolutsioonis tuuakse välja, et õiglase vastutuse menetluse eesmärgiks on see, et igal inimesel, kes kannatab tehisintellektisüsteemide poolt põhjustatud kahju või kellele põhjustasid vastavad süsteemid varalist kahju, peaksid omama sarnast kaitset nagu juhtudel, kus seda ei põhjustanud tehisintellekt. Lisaks rõhutatakse, et kavandatavad reeglid peaksid hõlmama ka märkimisväärset mittemateriaalset kahju. Euroopa Parlament peab õigustatuks tehisintellekti käitaja vastu tsiviilvastutusnõuete esitamist ning võrdleb osapoolte vahelisi õigussuhteid ning tehisintellekti käitajat kui auto omanikku ehk suurema ohu allika omanikku. Eesmärgiks on välistada olukorrad, kus isikud on tehisintellekti tegevusest mõjutatud, ent ei oma lepingulisi suhteid tehisintellekti käitajaga ning seetõttu jäävad ilma õigusest esitada nõudeid tehisintellekti käitaja vastu. Samuti lisatakse, et tehisintellekti käitaja on mõjutatud isiku esimeseks nähtavaks kontaktpunktiks. Tehisintellekti käitaja all mõistetakse nii isikut, kes saab süsteemi käitamisest kasu ja omab teatavat kontrolli tehisintellekti üle kui ka isikut, kes aktiivselt omab reaalselt kontrolli ja tagab tehisintellekti tugiteenuseid. Juhul, kui taolisi isikuid on juhtumite puhul mitmeid, on Euroopa Parlament seisukohal, et sellisel juhul peaksid käitajad vastutama solidaarselt, kui ei ole võimalik teha kindlaks ulatus, mil määral isikud omasid realiseerunud riski üle kontrolli.[87]

Tehisintellekti vastutuse puhul on toodud paralleele ka vastutusega laste tekitatud kahjude eest. Põhjus, miks see sarnaneb tehisintellekti tõttu tekkinud vastutusega on see, et vastutus on tekkinud õigusvõimetu isiku poolt, mille tõttu ei ole võimalik tegu teinud osapoolt vastutusele võtta. Selleks, et tegu teinud isikut oleks võimalik vastutusele võtta, peab saama isik aru enda tegevustest ning selle keelatusest. Kuna masinatel ei ole taolist omadust mõelda ning neile ei saa omistada tahtlust, ei saa neil olla ka süüd. Vea põhjus, mille tehisintellekt sooritab, võib olla näiteks programmeerimisviga või tahtlik programmi mõjutamine, aga ei saa tuleneda tehisintellektist enesest. Vastutama peab inimene, kelleks võib olla tootja, operaator, tehisintellekti omanik või kasutaja või teatud juhtudel inimene, kes oleks pidanud nägema taolist sündmust ette ja seda takistama. Tehisintellektiga seotud rikkumistes peetakse ebaoluliseks fakti, kas rikkumine toimus programmeerimise ja süsteemi loomise käigus või tehisintellekti iseseisva masinõppimise tagajärjel, kuna tehisintellekti puhul on võimatu

[87] 20.10.2020, Euroopa Parlament, tehisintellekti tsiviilvastutuse kord

tõmmata piiri selle vahele, mille osas on tehisintellekti edasi arenenud ja millisena ta on loodud.[88] Seda lähenemist toetab ka seisukoht, mille kohaselt on tehisintellekt „agent“ või instrument, kelle tegevusest tuleneva vastutuse korral asendatakse agent inimfaktoriga. Tehisintellekti saab pidada vahendiks isiku käes, kes omab selle üle kontrolli ja vastutab täies ulatuses tehisintellekti poolt tekitatud tagajärgede eest. Lisaks analoogiale laste tekitatud kahjudega, saab pidada tehisintellekti seda loonud või omava isiku varaks, mille puhul on sätestatud vara omaniku range vastutus tema vara poolt tekitatud kahju eest. Võimalik on ka tõlgendus, et tehisintellekt on omaette isik, mille juhtumist täie kindlusega tulevikus välistada ei saa, ent tänapäevase tehnoloogilise arengu juures seda lähenemist veel ei tunnustata.[89]

Selleks, et teha kindlaks, kes tehisintellekti poolt sooritatud rikkumise eest konkreetselt vastutab, on vaja arvestada konkreetse juhtumi asjaolusid, kuna vastutav isik võib tugevalt sõltuda vastavast olukorrast. Üheks võimaluseks on aluseks võtta konkreetne ülesanne, mida täidab tehisintellekt ning sellest teha järeldus, kes on isik, kes tehisintellekti seda konkreetset ülesannet täitma määras. Teiseks võimaluseks on võtta arvesse seda, kellel on kõige suurem võimekus ja võimalus tehisintellekti tegevust mõjutada monitooringu, järelevalve ja õpetuse läbi. Tehisintellekti arendamisfaasis omavad tõenäoliselt kõige rohkem kontrolli programmeerijad, tootjad ja tehisintellekti disainerid. Kui tehisintellekt on juba kasutusel, seda tõenäolisem on, et tehisintellekti operaator või omanik peaks olema isik, kes vastutab tehisintellekti poolt toime pannud rikkumiste eest. Taoline vastutus ei tähenda, et vastutav isik on süüdi tehisintellekti tegevuse eest, vaid pigem seda, et tegevus, mis tehisintellektile täitmiseks anti, oli isiku kontrolli ja autoriteedi all. Kui kolmas osapool tungib tehisintellekti tegevusse ning kontrollib seda ja seetõttu paneb tehisintellekt toime rikkumise, peaks vastutus kanduma koheselt sellele isikule, kui teda on võimalik identifitseerida. Juhtudel, kui tehisintellekti tegevus on mitme inimese vastutusalas, siis jaguneb vastutus kõigi vahel. Samuti on võimalus enne intsidentide juhtumist määrata ära, kes on vastutavaks isikuks juhtudel, kui rikkumised peaksid toimuma.[90]

---

[88] Santos Divino, S. Critical considerations on artificial intelligence liability: e-personality proportions. Revista Electroniga Direito Sociedade, 8(2), 2020, lk 203-206. Arvutivõrgus: https://heinonline-org.ezproxy.utlib.ut.ee/HOL/Page?public=true&handle=hein.journals/redes8&div=31&start_page=193&collection=journals&set_as_cursor=1&men_tab=srchresults (15.04.2022)

[89] Lior, A. AI entities as AI agents: artificial intelligence liability and the AI respondeat superior analogy. Mitchell Hamline Law Review, 46(5), 2020, LK 1043-1102.

[90] Lior, A. 2020, lk 1043-1102

Eeltoodust tulenevalt on võimalik jõuda seisukohale, et tehisintellekti poolt toime pandud rikkumise eest isikusamasuse tuvastamise kohustuse täideviimisel tehisintellekt vastutada ei saa ning selle vastutuse peab üle kandma isikule, kes omab teadvust ning õigusvõimet. Erinevate Euroopa Liidu institutsioonide juhendid ja suunised sisaldavad võimalikke vastutusküsimuste lahendusi, ent õiguslikult siduvalt neid vormistatud ei ole. Nii eelnimetatud juhendites ja suunistes kui ka õiguskirjanduses on jõutud seisukohtadele, et tehisintellekti poolt toime pandud rikkumise eest vastutab isik, olenemata tema süüst, kes omab tehisintellekti tegevuse üle kontrolli, kelle tegevuse/tegevusetuse tõttu tehisintellekt taoliselt käitus või kes omab tehisintellekti. Jaatatakse olukorda, et kui on võimalik teha kindlaks ja tuvastada tehisintellekti rikkumine konkreetse isiku teo tagajärjena, siis on võimalik tehisintellekti tegevuse vastutus kanda üle sellele isikule. Samuti on võimalik enne taolise olukorra tekkimist sätestada, kes vastutab tehisintellekti poolt toime pandud rikkumiste eest. Juhul, kui taolist otsust tehtud ei ole, on vajalik iga üksikjuhtumi puhul analüüs lähtudes olukorra asjaoludest ning seetõttu ei ole otstarbekas seadustes vastutuse kindlat määratlemist reguleerida. Seega olukorras, kus teenusepakkuja täidab krediidiasutuse isikusamasuse tuvastamise kohustust omavahelise lepingu alusel, ei ole võimalik ettevõttel vastutusest vabanemiseks tugineda tehisintellekti poolsele rikkumisele. Seda eelkõige seetõttu, et tehisintellekt ei oma õigusvõimet ega teadvust ning tehisintellekti poolse rikkumise eest peab vastutama isik, kes tehisintellekti ajahetkel kontrollis. Kuna Euroopa Liidus ei ole jõutud ühtsele arusaamale tehisintellekti vastutuse küsimustes, tähendab see, et õiguslike vaidluste vältimiseks on oluline roll vastutuse küsimuste reguleerimisel poolte vahelises isikusamasuse tuvastamise tegevuse edasiandmise lepingus. Kui lepingus vastutuseküsimust reguleeritud ei ole, tuleb lähtuda konkreetse olukorra asjaoludest: kas on võimalik tuvastada rikkumisega kõige enam seotud isik või isik, kes tehisintellekti isikusamasuse tuvastamisel toimunud rikkumise ajahetkel kontrollis või kas näiteks teenusepakkuja ettevõtte siseselt on sätestatud vastutuse jagunemine selle tekkimisel.

4. Vastutuse jagunemine isikusamasuse tuvastamise kohustuse edasiandmise osapoolte vahel masintekkelisel rikkumisel

Käesolevas töös eeltoodud peatükkides ja vastutust käsitlevates alapeatükkides 4.1 ja 4.2, käsitletakse masintekkelise rikkumisena tehisintellekti poolt toime pandud rikkumist isikusamasuse tuvastamisel. Võimalikud olukorrad, mida saab pidada isikusamasuse tuvastamise kohustuse rikkumiseks tulenevalt seadusest, on isikusamasuse tuvastamata jätmine, esitatud teabe mitte kontrollimine usaldusväärsest ja sõltumatust allikast hangitud teabe põhjal, kliendi esindaja isikusamasuse ja esindusõiguse tuvastamata jätmine ja mitte kontrollimine, tegeliku kasusaaja tuvastamata jätmine ja tema isikusamasuse kontrollimiseks meetmete mitte võtmine.[91] Samuti tulenevalt käesoleva töö analüüsist, on kohustuse rikkumiseks ka lepinguliste või muudel alustel tekkinud kohustuste rikkumine, sh kahju tekitamine (nii varaline kui ka mitte varaline), isikusamasuse tuvastamise nurjumine ja lepingutingimuste mitte täitmine. Samuti kõik muud tagajärjed, mis eelnimetatud kohustuste mitte täitmisest tekkida võivad. Isikusamasuse kontrollimata jätmise alla on võimalik paigutada ka olukord, kus isikusamasus tuvastatakse vääralt. Seda seetõttu, et nõuetele vastav isikusamasus jääb kontrollimata ning ebakorrektsest isikusamasuse tuvastamisest võivad tekkida veel täiendavad tagajärjed. Eeltoodu põhjal on võimalik jõuda järeldusele, et käesolevas töös käsitletakse masintekkelise rikkumisena olukorda, kus tehisintellekti tegevuse tagajärjel on toimunud rikkumine, rikkumiseks saab pidada käesolevas lõigus käsitletud juhtumeid ning teatud juhtudel on selle rikkumise tagajärjel tekkinud kahju.

4.1 Krediidiasutuse vastutus

RahaPTS-st tuleneb, et vaatamata tegevuse edasiandmisele, ei vabane krediidiasutus vastutusest klientide ning järelevalveasutuse ees. Krediidiasutustele on sätestatud ulatuslikud

[91] RT I, 12.03.2022, 19

nõuded teenusepakkuja taustakontrolli teostamiseks, mis töö kirjutaja hinnangul raskendab krediidiasutuse poolt vastutusest vabanemist, st paneb krediidiasutuse hoolsuskohustuse teenusepakkuja valikul kõrgeks ning raskendab või lausa välistab tegevuse edasiandmisel tekkivate rikkumiste korral tuginemist teenusepakkuja poolsele rikkumisele või puudujääkidele.[92] Arvestades taolist kindlameelset seisukohta krediidiasutuse kui kohustatud isiku vastutuse kohta, on vajalik analüüs, millistel alustel ja kelle ees vastutab krediidiasutus isikusamasuse tuvastamise kohustuse rikkumise korral, kui isikusamasuse tuvastamine on antud edasi teenusepakkujale ja rikkumine on masintekkeline.

4.1.1 Krediidiasutuse väärteovastutus

Isikusamasuse tuvastamise kohustus krediidiasutusele tuleneb Eesti seadusandlusest rahapesu ja terrorismi rahastamise tõkestamise seadusest. Krediidiasutus on kohustatud jälgima ulatuslikke hoolsusmeetmeid, sh tuvastama tehingus osaleva isiku isikusamasuse ja esitatud teabe õigsuse usaldusväärsest ja sõltumatust allikast hangitud teabe põhjal. Seda ka juhul kui kasutatakse e-identimist ning e-tehinguid. See teeb krediidiasutusest kohustatud isiku jälgimaks, et isikusamasuse tegevus ja kohustus saaks täidetud. Eelnimetatud seaduse alusel on krediidiasutusel kui kohustatud isikul võimalus anda isikusamasuse tuvastamise funktsioon edasi, st krediidiasutusel on õigus tugineda teise osapoole poolt kogutud andmetele ning dokumentidele nõutud tingimuste täitmisel.[93]

Käesolevat teemat käsitlevad juhendid, suunised ja õigusaktid ei seo krediidiasutuse vastutust kahju tekkimisega. See tähendab, et juhul, kui toimub isikusamasuse tuvastamise kohustuse rikkumine, kas krediidiasutuse või teenusepakkuja poolt, kes pakub isikusamasuse tuvastamise teenust, vastutab krediidiasutus kohustuse täitmata jätmise fakti eest, olenemata, kas selle tagajärjel tekib osapooltele kahju.

[92] Finantsinspektsioon 05.08.2019.

[93] RT I, 12.03.2022, 19

Füüsilise isiku isikusamasuse tuvastamise kohustus tekib krediidiasutustele RahaPTS seadusest §-st 21, mille alusel on krediidiasutus kohustatud tuvastama kliendi või tema esindaja isikusamasus ning säilitama nende kohta asjaomased andmed. Samast paragrahvist tuleneb kohustus veenduda esitatud andmete õigsuses, kasutades lisaks esitatud andmetele ka muudest usaldusväärsetest ja sõltumatutest allikatest pärinevat teavet. Lisaks kohustusele tuvastada isikusamasus, tuleneb käesoleva seaduse §-st 31 kohustus isikusamasuse tuvastamisel kasutada infotehnoloogilisi lahendusi, kui esinevad seaduses sätestatud olukorrad, sh kui ärisuhte loomisel ei viibi krediidiasutus kliendiga samas kohas, klient on pärit Euroopa Majanduspiirkonna välisest riigist või tema elu- või asukoht on eelnimetatud riigis või juhul, kui kliendi poolt sooritatavate tehingute kogusumma ületab ühes kalendrikuus füüsilise isiku puhul 15 000 euro ja juriidilisest isikust kliendi puhul 25 000 eurot. Kasutades infotehnoloogilisi vahendeid isikusamasuse tuvastamisel kehtivad samasugused nõuded tuvastamise aluseks olevatele dokumentidele ning lisaks kasutatavatele allikatele. Sellele lisanduvad nõuded kasutatavale infotehnoloogilisele lahendusele.

Isikusamasuse tuvastamise kohustust on tuginedes RahaPTS § 24 alusel võimalik edasi anda teisele osapoolele. See sätestab nõuded hoolsuskohustuse täitmisele juhul, kui tuginetakse teise isiku andmetele või hoolsuskohustust täidab teine isik. § 24 lõige 7 sätestab, et seadusest tulenevate kohustuste täitmise eest vastutab ka juhul, kui tegevus on teisele poolele edasiantud, kohustatud isik ehk käesoleva töö mõistes krediidiasutus.

Juhul, kui isikusamasuse kohustuse tuvastamine ning kontrollimise kohustus jääb täitmata krediidiasutuse, tema juhatuse liikme või töötaja poolt, karistatakse RahaPTS § 84 alusel füüsilist isikut rahatrahviga kuni 300 trahviühikut või arestiga ning krediidiasutust rahatrahviga kuni 400 000 eurot. Eelnimetatud paragrahv on väärteovastutuse tekkimise aluseks. Käsitletav paragrahv ei sätesta mitte väärteolist vastutust isikusamasuse tuvastamata jätmise eest, vaid isikusamasuse tuvastamise ja kontrollimise kohustuste rikkumise eest. See tähendab, et lisaks isikusamasuse tuvastamisele peavad olema täidetud ka kohustusi sätestavates paragrahvides esitatud nõuded isikusamasuse tuvastamisele ning hoolsusmeetmete kohaldamise edasiandmisele. Juhul, kui isikusamasuse tuvastamise kohustus jääb täitmata seoses teenusepakkuja poolsele tingimustele mitte vastamisega, siis vastutab krediidiasutus oma hoolsuskohustustele sätestatud tingimuste rikkumise eest.

Kõik eeltoodu tähendab, et olukorras, kus krediidiasutus on andnud enda RahaPTS alusel tekkinud isikusamasuse tuvastamise kohustuse edasi teenusepakkujale, kes kasutab isikusamasuse tuvastamiseks tehisintellekti, siis tehisintellekti tegevuse tagajärjel tekkinud rikkumine toob kaasa krediidiasutuse isikusamasuse tuvastamise kohustuse täitmata jätmise. Eelnimetatud juhul ei ole krediidiasutusele pandud hoolsuskohustused täidetud ning seetõttu on rikkumise toimumine võimalik. Kuivõrd RahaPTS alusel on krediidiasutusel õigus anda enda hoolsusmeetme täitmine edasi teisele osapoolele, tuleneb seadusest nõue, et teenusepakkuja poolt pakutav teenus peab vastama samadele tingimustele, mis on sätestatud krediidiasutuse poolsele hoolsusmeetme täitmisele. Tehisintellektist tuleneva masintekkelise rikkumise tagajärjel tekkinud isikusamasuse tuvastamise kohustuse rikkumise eest tekib väärteovastutus krediidiasutusel ka juhul, kui isikusamasuse tuvastamise tegevust täidab osapoolte vahelise lepingu alusel kolmas osapool. Rahapesu ning terrorismi rahastamise tõkestamise seaduse sõnastuse kohaselt on tegemist absoluutse vastutusega, st tahtlus või kasutusel oleva infotehnoloogilise vahendi toimimise katkemine vastutust või vastutuse määra ei mõjuta. [94]

Käesoleva alapeatüki analüüsist lähtuvalt on töö autor seisukohal, et kuna krediidiasutuse väärteovastutus on absoluutne ning rikkumise iseloom või tekkepõhjus seda ei mõjuta, peab krediidiasutus pooltevahelisi suhteid ulatuslikult reguleerima, eriti olulise või kriitilise funktsiooni edasiandmisel teenusepakkujale. Selleks peab krediidiasutus tagama ulatusliku järelevalve mehhanismi, defineerima väga põhjalikult suhteid teenusepakkujaga nendevahelises lepingus ning samuti, juhul kui tekib teenuses tõrkeid või puudujääke, koheselt reageerima. Samuti, arvestades, et käesolevas töös on jõutud järeldusele, et isikusamasuse tuvastamise kohustus on kriitiline või oluline funktsioon, võib krediidiasutuse otsus anda isikusamasuse tuvastamise kohustus edasi vaid ühele teenusepakkujale olla ebapiisav negatiivsete tagajärgede vältimiseks.

[94] RT I, 15.03.2022, 14.

4.1.2 Krediidiasutuse tsiviilõiguslik vastutus

Lisaks sellele, et krediidiasutus on seaduse alusel kohustatud klientide isikusamasust tuvastama ning on lepingulistes suhetes teenusepakkujaga, on vastavalt käesoleva töö alapeatükile 2.2 krediidiasutuse ja kliendi vahel lepingulised suhted. Krediidiasutus ja klient on sõlminud eriliigilised võlaõiguslikud lepingud ning lisaks lepingutele, reguleerib nendevahelisi suhteid krediidiasutuse üldtingimused, mille on sätestatud krediidiasutus ning teinud need kliendile kättesaadavaks. See tähendab, et rikkumise korral tekib krediidiasutusel vastutus võlaõigusseaduse alusel. Käesolevas peatükis käsitletud rikkumisena saab pidada krediidiasutuse ja kliendi vahelist õiguslikku suhet arvesse võttes eelkõige olukorda, kus kliendile tekib kahju. Juhul, kui isikusamasuse kohustust on rikutud ning isikusamasus on vääralt tuvastatud, ent kahju ei teki, ei teki kliendile selle kohustuse rikkumisest tagajärgi ning ei ole võimalik kasutada õiguskaitsevahendeid selleks, et taastada varasemat olukorda.

Krediidiasutuse kohustus isikusamasus tuvastada ning teha seda korrektselt kliendi ees nende lepingulise suhte raames, tekivad võlaõigusseaduse § 724^6 alusel, mis sätestab, et makseteenuse pakkuja peab nõudma kliendi tugevat autentimist (käesoleva töö mõistes isikusamasuse tuvastamist) iga kord, kui maksja soovib juurdepääsu oma maksekontole interneti teel, algatada elektroonilist maksetehingut või teha muid toiminguid distantsilt, millega võib tekkida andmete väärkasutamine või pettuse oht. Samuti on VÕS § 733^4 alusel pandud tõendamiskoormis krediidiasutusele, et on rakendatud kliendi tugevat autentimist. Juhul, kui krediidiasutus ei ole rakendanud kliendi tugevat autentimist, on võimalik kliendil nõuda krediidiasutuselt kahju hüvitamist VÕS § 733^5 alusel.[95] Oluline on märkida, et vastavates sätetes ei ole tehtud erisust kahju liigi osas. See tähendab, et kui realiseerub eelnimetatud oht, kus toimub andmete väärkasutamine, sh isikuandmete ebaõige käsitlemine ja levimine, on ka sellisel juhul võimalik võlaõigusseaduse alusel nõuda krediidiasutuselt kahju hüvitamist, mitte ainult varalise kahju hüvitamise korral.

[95] RT I, 15.03.2022, 14

Olles tuvastanud selle, et kliendi ning krediidiasutuse vahelist suhet reguleerib nendevaheline võlaõiguslik leping, siis selleks, et tuvastada krediidiasutuse vastutuse olemasolu ning selle olemasolul ulatust isikusamasuse tuvastamise kohustuse rikkumisel, juhul kui isikusamasuse tuvastamise funktsioon on edasi antud teenusepakkujale ning rikkumine on tehisintellektist tulenev, on vajalik lisaks võlaõiguslikele sätetele tuvastada, kuidas on krediidiasutus vastutuse jagunemist reguleerinud üldtingimustes ning kas panga poolt koostatud vastutust puudutavad tingimused on kliendi suhtes jõustatavad.

Võlaõigusseaduse § 35 alusel on sellised lepingutingimused, mis on välja töötatud tüüplepingutes kasutamiseks või mida pooled ei ole eraldi läbi rääkinud ja mida tüüptingimust kasutav lepingupool (käesoleval juhul krediidiasutus) kasutab teise lepingupoole suhtes, kes ei saa mõjutada tingimuste sisu, tüüptingimused. Selleks, et tüüptingimused saaksid osaks lepingust, peab pool, kelle suhtes neid kasutatakse, nendest teadlik olema ning saama nende sisuga tutvuda.[96] Käesoleval juhul tehakse üldtingimused kliendile teatavaks viisil, mis on kliendile kättesaadav kas kodulehe või teeninduspunktide kaudu. Kliendil võimalust tingimuste osas läbi rääkida ei ole, kuna vastavalt krediidiasutuste seadusele, on tegemist kliendi suhtes rakendatavate standardsete tingimustega.[97] See tähendab, et saab väita, et kõne all olevad tingimused on tüüptingimused, mis on saanud osaks poolte vahel sõlmitud lepingust. Vastavalt võlaõigusseadusele, on tüüptingimus tühine juhul, kui tüüptingimus kahjustab teist lepingupoolt ebamõistlikult. Ebamõistlikuks kahjustamiseks eeldatakse muuhulgas olukorda kus kaldutakse kõrvale seaduse olulisest põhimõttest. Juhul, kui tüüptingimust jõustatakse tarbija suhtes, lisanduvad täiendavad seaduses välja toodud olukorrad, mil on tüüptingimus ebamõistlikult kahjustav.[98] Käesolevas töös, nagu märgitud varasemalt, käsitletakse jaeklienti ehk tarbijat võlaõigusseaduse mõistes ning selleks, et välja selgitada, kas krediidiasutus saab üldtingimustele tuginedes vabaneda võlaõigusseaduses sätestatud vastutusest, tuuakse näiteks AS SEB Pank ning Swedbank AS üldtingimused.

AS SEB Pank üldtingimustes on eraldi välja toodud vastutuse peatükk, milles lepitakse kokku nii panga kui ka kliendi kohustuste rikkumise korral vastutus. Üldtingimustes on sätestatud

[96] RT I, 15.03.2022, 14.

[97] RT I, 29.03.2022, 5.

[98] RT I, 15.03.2022, 14.

punktid, mille puhul on võimalik väita, et käesolevas magistritöös kirjeldatud olukorra tõusetumisel, oleks tegemist ebamõistlikult kahjustava tüüptingimusega ning panga vastutuse välistamist sisaldav üldtingimuste säte seega kliendi suhtes tühine.[99]

Esimeseks selliseks on punkt 105, mille kohaselt nii pank kui ka klient vastutavad kohustuse süülise rikkumise korral.[100] Käsitledes olukorda, kus isikusamasuse tuvastamine on toime pandud ebakorrektselt, selle tagajärjel on tekkinud kliendile kahju, siis olenemata sellest, kas kohustust on täitnud krediidiasutus ise või infotehnoloogilist lahendust pakkuv teenusepakkuja, on tegemist krediidiasutusele seaduse alusel pandud kohustusega ning vastavalt sellekohasele seadusandlusele (vt p 2.1 ning 2.2) ei oma tähtsust krediidiasutuse süü olemasolu, vaid krediidiasutus vastutab selle kohustuse mitte täitmise eest tingimusteta. See tähendab, et vastutust välistav üldtingimus, mille kohaselt pank ei vastuta sellise kahju eest, mille puhul pole tegemist süülise rikkumisega, st hooletuse või raske hooletusega toime pandud rikkumised, on kliendi suhtes tühine võlaõigusseaduse alusel, mille kohaselt on ebamõistlikult kahjustavad ning seetõttu tühised tingimused, millega välistatakse tingimuse kasutaja seadusest tulenev vastutus. [101]

Punktis 106 on AS SEB Pank toonud välja, et pank ei vastuta kohustuse rikkumise eest, kui see on põhjustatud vääramatust jõust. Muu hulgas on välja toodud vääramatuks jõuks sündmused, mida kohustatud pool ei saanud mõjutada, sh üldine arvutisüsteemide häire ning kolmanda isiku poolt toime pandud krediidiasutuse tegevuse seadusvastane häirimine küberründe näol.[102] Selle sätte puhul on oht, et krediidiasutus tugineb käesolevale sättele olukorras, kus kliendile on tekkinud kahju ning kahju on tekkinud isikusamasuse tuvastamise arvutisüsteemide ulatusliku häire tulemusel või süsteemidele teostatud ründe tagajärjel. Juhul, kui infotehnoloogiline lahendus lakkab töötamast, ka juhul, kui häired olid ulatuslikud või tulenesid seadusvastasest teost, ei vabasta see krediidiasutust endale pandud isikusamasuse tuvastamise kohustusest seaduse ees. Selliste olukordade vältimiseks on vastavalt käesoleva töö peatükis 1 ning

[99] AS SEB Pank. AS SEB Pank koduleht. AS SEB Pank üldtingimused. Arvutivõrgus: https://www.seb.ee/sites/default/files/tac/as_seb_pank_yldtingimused_01012021_est.pdf (27.02.2022)

[100] AS SEB üldtingimused. Punkt 105.

[101] RT I, 15.03.2022, 14.

[102] AS SEB üldtingimused. Punkt 106.

alapeatükkides 2.1 ning 2.2 toodud seadusandluses ning õigusaktides selged nõuded krediidiasutustele, mille kohaselt peavad krediidiasutused selliseid riske vältima ning riskide realiseerumisel need koheselt kõrvaldama viisil, mil oleks pidev toimimine tagatud. Seega juhul, kui kliendile tekib kahju seetõttu, et kasutusel olev tehisintellekti baasil toimiv lahendus, mida tagab teenusepakkuja krediidiasutusele, lakkab töötamast häire või küberründe tõttu, ei välista see krediidiasutuse vastutust kliendi ees, kuna tegemist on talle seadusest pandud kohustusega. Krediidiasutusele on pandud kohustus taolisi tagajärgi vältida, kui ta annab endale seadusega pandud funktsiooni teisele osapoolele edasi ning kõne all olev üldtingimuste säte on kliendi suhtes tühine. See tuleneb võlaõigusseadusest, mille kohaselt tuleb ebamõistlikku kahjustamist eeldada juhul, kui tüüptingimus kaldub kõrvale seaduse olulisest põhimõttest ja tarbija puhul loetakse seega tühiseks, kui tingimusega välistatakse tingimuse kasutaja seadusest tulenev vastutus.[103]

Eelnimetatud punktides 105 ja 106 toodud näited sisalduvad sarnases sõnastuses ka Swedbank AS üldtingimustes, st vastutuse olemasolu vaid süü korral ning vääramatu jõu puhul, st arvutisüsteemi häire või küberrünne. See tähendab, et töös käsitleva olukorra toimumisel oleksid ka need üldtingimuste sätted vastutuse osas kliendi suhtes tühised. Lisaks eelnimetatutele, on Swedbank AS üldtingimustes toodud veel välja punktis 12.5 panga vastutuse välistamine juhul, kui kliendile on tekkinud kahju infosüsteemide tõrgetest, kui infosüsteemide tõrgete kestus ei ületanud panga määratud tõrgete lubatavat päevast kestust. Ka punktis 12.5 panga vastutust välistav säte ei kehti juhul, kui kliendile tekib kahju infosüsteemi tõrkest, mille eesmärgiks oli isikusamasuse tuvastamine.[104] Nagu varasemalt mainitud, siis tegevuste edasiandmist krediidiasutuste poolt käsitlevad õigusaktid, suunised ja juhendid sisaldavad täielikku nulltolerantsi tegevuse katkemise kohta ning panevad selle toimimise tagamise igal ajahetkel krediidiasutuse kohustuseks, isegi juhul kui see tähendaks mitme erineva teenusepakkuja kasutamist. Seega ka Swedbank AS üldtingimused näiliselt välistavad enda vastutuse juhul, kui toimub tõrge infosüsteemide töös, milleks on ka isikusamasust tuvastavad infosüsteemid, ent kuna krediidiasutustel ei ole võimalik tugineda edasiantud

[103] RT I, 15.03.2022, 14.

[104] Swedbank AS. Swedbank AS üldtingimused. Swedbank AS koduleht. Arvutivõrgus: https://www.swedbank.ee/static/pdf/private/home/important/cond_general_est_2021_01_01.pdf (27.02.2022)

tegevuse töö katkemisel mõne teise osapoole vastutusele, siis sellise juhtumi korral on nimetatud vastutust välistav üldtingimuste säte kliendi suhtes tühine.

Eeltoodud analüüsi toetab 2021. aastal tehtud Euroopa Kohtu otsus C-609/19. Kohus selgitas lahendis, et tarbijalepingute puhul on kõik poolte vahel tüüptingimustel sõlmitud lepingu tingimused tühised ja tarbijale mittesiduvad, kui need on ebamõistlikult kahjustavad, vastuolus hea usu põhimõttega ning tekitavad lepinguosaliste lepingust tulenevate õiguste ja kohustuste olulise tasakaalustamatuse tarbija kahjuks.[105] Võlaõigusseaduse alusel tuleb ebamõistlikut kahjustamist eeldada juhul, kui tüüptingimus kaldub kõrvale seaduse olulisest põhimõttest. Veel enam, tarbijaga sõlmitud lepingus kasutatav tüüptingimust loetakse ebamõistlikult kahjustavaks, ja seega tühiseks, kui tingimusega välistatakse tingimuse kasutaja seadusest tulenev vastutus.[106] Käesoleval juhul sätestab võlaõigusseadus krediidiasutuse kohustuse tuvastada kliendi isikusamasus ning loob võimaluse kliendil nõuda krediidiasutuselt kahju hüvitamist juhul, kui isikusamasuse tuvastamise kohustust on rikutud ning selle tagajärjel on tekkinud kahju.

Eeltoodust tulenevalt selgub, et juhul, kui kliendile tekib kahju ning kahju tekib isikusamasuse tuvastamise kohustuse rikkumise tagajärjel, sh olukorras, kus isikusamasuse tuvastamise funktsioon on krediidiasutuse poolt edasiantud teenusepakkujale, ning rikkumine on toimunud masintekkeliselt tehisintellekti poolt, vastutab vastavalt krediidiasutuse ja kliendi vahel sõlmitud lepingule ning nii siseriikliku kui ka Euroopa Liidu ülese seadusandluse, suuniste ning juhendite alusel krediidiasutus. Vastutust välistavad asjaolud üldtingimustes, mis on saanud kliendi ja krediidiasutuse vahelise võlaõigusliku lepingu osaks, ei saa välistada krediidiasutuse seadusest tulenevat vastutust ning sellesisulised üldtingimustes sisalduvad tüüptingimused on tühised.

[105] EK C-609/19, *BNP Paribas Personal Finance SA versus VE,* ECLI:EU:C:2021:469.

[106] RT I, 15.03.2022, 14.

4.2 IT teenusepakkuja vastutus

Nagu varasemalt analüüsitud, ei ole IT teenusepakkuja kohustatud isik RahaPTS seaduse alusel isikusamasuse tuvastamise kohustuse täitmisel, mis tähendab, et väärteovastutust talle kohaldada ei ole võimalik olukorras, kus isikusamasuse tuvastamist teostab IT teenusepakkuja poolne tehisintellektil põhinev süsteem ning rikkumine on toime pandud süsteemist lähtuvalt. Sellele vaatamata võib tekkida IT teenusepakkujal tsiviilõiguslikud vastutuse vormid tulenevalt lepingulistest suhetest või lepinguvälistest võlasuhetest, lähtudes tehisintellekti kohasest õigusraamistikust ja tegevuse edasiandmise lepingust.

4.2.1 IT teenusepakkuja poolne lepinguliste kohustuste rikkumisest tulenev vastutus

Sarnaselt EBA suunistele, tuleb ka Eesti seadusandluse kohaselt selleks, et funktsiooni täitmist anda teisele osapoolele edasi, krediidiasutusel sõlmida kirjalik leping teise osapoolega ning lepingu sõlmimisest teavitada pädevat järelevalveasutust. Osapoolte vahel sõlmitud lepingu näol on tegemist võlaõigusliku lepinguga, mis reguleerib kahe osapoole omavahelist suhtlust. Tegevuse nõuetele vastava täitmise eest jääb vastutama seaduse mõttes kohustatud isik ehk krediidiasutus olenemata sellest, et funktsiooni täitmist krediidiasutus ise ei teosta või kuidas on vastutust reguleeritud omavahelises lepingus.[107] Muid lepingulisi suhteid töös käsitletavas tegevuse edasiandmise olukorras IT teenusepakkuja ei oma.

Teenusepakkuja poolne lahendus käesoleva töö mõistes on tehisintellektil baseeruva lahenduse pakkumine isikusamasuse tuvastamiseks. Tehisintellekti poolseteks rikkumisteks, mida saab pidada kohustuse rikkumiseks lepingulistes suhetes, on näiteks tehisintellekti otsustusprotsesside ja käitumismustrite mitte mõistmine ja seega nende korrigeerimatus, võimekus vigaseid otsuseid korrata väga lühikese ajaperioodi jooksul mõõtmatul arvul, oht põhiõigustele, diskriminatsiooniks, kahjuks (nii varaliseks kui ka mitte varaliseks) ning

[107] RT I, 12.03.2022, 19.

võimetus lähtuda olukordade spetsiifikast tegemaks kompromisse või reeglitest põhjendatud juhtudel kõrvale kalduda.[108]

Finantsinspektsiooni juhendis on esitatud nõuded tegevuse edasiandmise lepingule, mille kohaselt peavad pooled lepingus kokku leppima tegevuse olemuse, ulatuse, poolte õigused, kohustused ja vastutuse. Kuigi juhendis on toodud välja vastutuse määratlemine, õiguskaitsevahendite kokkuleppe olemasolu osapoolte vahelises lepingus ning võimaliku kahju hüvitamiseks vajalike garantiide kehtestamine viisil, mis oleks pooltele üheselt arusaadavad, ei ole avatud seda, mida Finantsinspektsioon selle all mõtleb- kas pooled saavad kokku leppida, et tegevuse katkemisel ning sellega seonduvate kahjude, sh krediidiasutusele esitatavate nõuete ning seadusest tulenevate võimalike tagajärgede eest saab vastutuse anda teenusepakkujale edasi.[109] EBA suunised lisavad muuhulgas, et teenusepakkuja ning krediidiasutuse vahelise lepingu sõlmimise hetkel tuleks kaaluda teenusepakkuja poolt kohustusliku kindlustuse sõlmimist teatud riskide vastu ning selle summa ulatust. Suunised aga ei täpsusta, milliste tagajärgede vältimiseks kindlustus sõlmida tuleks ning kas kindlustuse sõlmimise eesmärgiks võiks olla samuti krediidiasutusele tekkinud kahju hüvitamine.[110]

Seega on võimalik jõuda järeldusele, et kuigi järelevalveasutusel ning valdkonda suunistavatel institutsioonidel on õigus sekkuda krediidiasutuse ja IT teenusepakkuja privaatautonoomiasse ning lepinguvabadusse, nagu on leitud käesoleva töö punktis 1.2, siis on nende ettekirjutuste eesmärgiks peamiselt tagada teenusepakkuja tegevuse vastavus seadustele ning eeskirjadele ja tagada teenusepakkuja, kes muul juhul ei ole allutatud finantsjärelevalvele, tegevuse auditeeritavus ja vastavus nõuetele, et kindlustada sektori usaldusväärsust. Suunised, juhendid ja seadused aga ei sätesta nõudeid pooltevahelise vastutuse jagunemiseks, vaid viitavad vajadusele lepingus nendes kokku leppida. Seetõttu saab väita, et krediidiasutusel ja teenusepakkujal on võimalik tegevuse edasiandmise lepingus vastavalt poolte kokkuleppele jaotada vastutusküsimust oma äranägemise järgi. See tähendab, et pooled saavad sätestada teenusepakkuja poolt loodud ja turustatud tehisintellekti poolt toime pandud rikkumise

[108] *Supra,* lk 33, 36, 42-43

[109] Finantsinspektsioon 05.08.2019.

[110] *Ibid*

tagajärjel tekkinud vastutuse jagunemise, arvestades, et väärteovastutus saab tekkida ainult krediidiasutusel.

4.2.2 IT teenusepakkuja poolne vastutus muudel alustel

Käesolevas töös analüüsitud olukorras on isikusamasuse tuvastamise osapoolteks krediidiasutus, teenusepakkuja ning klient. Varasemalt on tuvastatud, et teenusepakkuja ning krediidiasutuse vahel on lepinguline suhe ning vastutus osapoolte vahel tekib nendevahelisest lepingust. Lähtuvalt alapeatüki 2.3 analüüsist, ei ole teenusepakkuja ning kliendi vahel lepingulisi suhteid. Selleks, et välja selgitada, kas kliendil saavad tekkida nõuded isikusamasuse tuvastamise kohustuse rikkumisest masintekkelistel põhjustel teenusepakkuja vastu, on vajalik tuvastada, kas kliendi ja teenusepakkuja vahel saab tekkida õiguslikke suhteid muudel alustel.

Nagu varasemalt käsitletud, ei ole Euroopa Liidu tasandil tehisintellekti poolse rikkumise tulemusena tekkiva vastutuse küsimusi üheselt lahendatud. See tähendab, et tuvastamaks krediidiasutuse kliendi ja teenusepakkuja vahelist õiguslikku suhet ja vastutuse jagunemist isikusamasuse tuvastamise kohustuse masintekkelisel rikkumisel, on vajalik võtta aluseks kujunenud seisukohad ja võimalused.

Kõige detailsemat käsitlust taolise olukorra lahendamiseks pakub Euroopa Parlamendi tehisintellekti tsiviilvastutuse kord, milles jõutakse seisukohale, et tehisintellekti kasutamise tagajärjel tekkinud rikkumise poolt mõjutatud isikutele peab võimaldama viisi, mil panna vastutama tehisintellekti üle kontrolli omav või tehisintellekti rikkumise põhjustanud isiku. Seda ka juhul, kui mõjutatud isikul puudub lepinguline suhe tehisintellekti omava juriidilise või füüsilise isikuga. Taolised isikud, kes on saanud kahju tehisintellektile baseeruva süsteemi tagajärjel, peaksid omama samasugust kaitset kui need isikud, kellele põhjustatud kahju ei tulene tehisintellekti poolsest rikkumisest. Selleks, et välistada olukorrad, kus lepinguliste suhete puudumise tagajärjel ei ole kahjunõuded võimalikud, peab Euroopa Parlament põhjendatuks esitada tehisintellekti käitaja vastu nõudeid kui auto omaniku ehk suurema ohu allika omaniku vastu. Juhul, kui teenusepakkuja puhul ei ole võimalik selgeks teha, keda saab

pidada käitajaks, vastutavad kõik isikud, kes saavad käitamisest kasu, omavad selle üle reaalset kontrolli ja tavad tehisintellekti tugiteenuseid, solidaarselt. Suurema ohu allika poolt põhjustatud kahju käsitluse eeliseks on see, et Euroopa Parlamendi hinnangul peaks selle läbi olema võimalik lisaks varalisele kahjule esitada ka mittevaralise kahju nõudeid.[111]

Eesti seadusandluse alusel annab see kliendile võimaluse tugineda võlaõigusseaduse 2. jaole ehk vastutusele suurema ohu allikaga tekitatud kahju eest. Tuginedes VÕS §-le 1056, vastutab kliendi ees kahju tekitamise eest ohu allikat valitsenud isik, sõltumata oma süüst. See tähendab, et klient ei pea tuvastama teenusepakkuja süüd, vaid saab lähtuda faktist, et tegemist on isikuga, kes valitseb suurema ohu allikat. Juhul, kui Euroopa Parlament on jõudnud seisukohale, et tehisintellekti käitaja on suurema ohu allika valitseja ning sellest tulenevad rikkumised on suurema ohu allikale iseloomuliku ohu realiseerumine, ei ole kliendil vajalik oma nõudes ära põhjendada, et tegemist on suurema ohu allikaga ja saabunud tagajärg on iseloomuliku ohu realiseerumine. Kliendil on kohustus aga tõendada, et kahju on tekkinud justnimelt selle ohu realiseerumise tagajärjel.[112] See tähendab, et juhul, kui tehisintellekti poolt on toime pandud masintekkeline rikkumine krediidiasutuse poolt edasiantud isikusamasuse tuvastamise kohustuse täitmisel, vastutab rikkumise eest teenusepakkuja (või vastavalt peatükis 3. analüüsitud isik, kes oma tehisintellekti üle reaalset kontrolli) ning klient saab esitada teenusepakkuja suhtes endale tekitatud varalise ja mittevaralise kahju hüvitamise nõude suurema ohu allika poolt tekitatud kahju käsitlevate sätete alusel.

Teiseks võimalikuks vastutuse aluseks peab Euroopa Komisjon tootevastutuse direktiivi. Tootevastutuse direktiivi eesmärgiks on tagada, et kaup, mida kasutajatele pakutakse, oleks ohutu ning juhul, kui toote kasutamisest tulenevalt tekib kahju, saaks kahju hüvitatud. See võimaldab rakendada mittesüülist vastutust ning lihtsustada nõude esitamist loobudes vajadusest tõendada süü.[113] Samas toob komisjon välja, et seoses tehisintellekti olemusega, võib olla keeruline eelnimetatud direktiivile tugineda, kuna tootevastutusele tuginedes on vajalik siduda negatiivne tagajärg konkreetse isikuga. See aga võib tehisintellekti puhul osutuda

[111] 20.10.2020, Euroopa Parlament, tehisintellekti tsiviilvastutuse kord.

[112] RKTK 3.2-1-161-10

[113] Euroopa Parlamendi ja Nõukogu direktiiv 1999/34/EÜ, 10. mai 1999, millega muudetakse nõukogu direktiivi 85/274/EMÜ liikmesriikide tootevastutust käsitlevate õigus- ja haldusnormide ühtlustamise kohta. ETL L 141/20.

keerukaks. Selleks, et oleks võimalik tootevastutuse direktiivi alusel võtta vastutusele tehisintellekti poolse rikkumise eest vastutavat isikut, on vajalik tootevastutuse direktiivi muutmine.[114] Lisaks sellele räägib tootevastutuse kasutamise vastu asjaolu, et selle alusel on võimalik vastutusele võtta teenuse või toote poolt tekitatud füüsilise või materiaalse kahju eest. Juhul, kus võib tekkida teiseliigiline rikkumise tagajärg, näiteks isikuandmete väärkasutamine, ei ole võimalik tootevastutust kohaldada.[115]

Lähtuvalt eeltoodust, siis vaatamata lepinguliste suhete puudumisele, vastutab IT teenusepakkuja kliendi ees juhul, kui tehisintellekti poolt on toime pandud rikkumine isikusamasuse tuvastamise tegevuse täitmisel, suurema ohu allikaga tekitatud kahju põhjustamise sätete alusel. Nii eelnimetatud juhendites ja suunistes kui ka õiguskirjanduses on jõutud seisukohtadele, et tehisintellekti poolt toime pandud rikkumise eest vastutab isik, olenemata tema süüst, kes omab tehisintellekti tegevuse üle kontrolli, kelle tegevuse/tegevusetuse tõttu tehisintellekt taoliselt käitus või kes omab tehisintellekti. Jaatatakse olukorda, et kui on võimalik teha kindlaks ja tuvastada tehisintellekti rikkumine konkreetse isiku teo tagajärjena, siis on võimalik tehisintellekti tegevuse vastutus kanda üle sellele isikule. Lähtuvalt Euroopa Liidu ülestele seisukohtadele, on võimalik kasutada tehisintellekti rikkumise korral õiguskaitsevahendeid, mis kohalduvad lisaks olukorras, kus ei ole võimalik negatiivset tagajärge siduda konkreetse isikuga. See tähendab, et kliendilt ei eeldata konkreetse tehisintellekti poolt toime pandud rikkumise sidumist rikkumise põhjustanud isikuga, vaid nõuet saab esitada teenusepakkuja kui ettevõtte vastu. On võimalik, et juhul, kui tulevikus viiakse tootevastutuse direktiivi sisse muudatused, mille alusel on võimalik tehisintellekti tegevuse eest võtta isikuid vastutusele ka juhul, kui tehisintellekti poolt põhjustatud rikkumise negatiivse tagajärje sidumine on konkreetse isikuga raskendatud, saab kohaldada ka tootevastutuse direktiivi eelnimetatud isikusamasuse tuvastamise korralduse kontekstis.

[114] Euroopa Komisjon, 19.02.2020. Valge raamat.

[115] Euroopa Komisjon, 19.02.2020. Komisjoni aruanne Euroopa Parlamendile, nõukogule ning Euroopa Majandus- ja Sotsiaalkomiteele.

Kokkuvõte

Magistritöö eesmärgiks on tuvastada isikusamasuse tuvastamise kohustuse edasiandmise osapoolte vastutus ja vastutuse jagunemine masintekkelisel rikkumisel. Selle eesmärgi saavutamiseks analüüsib töö isikusamasuse tuvastamise tegevuse edasiandmise olemust valdkonnale kehtivate suuniste, juhendite ja õigusaktide põhjal ning sellele kehtivaid nõudeid ning erisusi kontekstis, kus tagatakse isikusamasuse tuvastamine läbi tegevuse edasiandmise, kasutades infotehnoloogiliste lahendusi. Lisaks sellele on eesmärgiks tuvastada isikusamasuse tuvastamise kohustuse edasiandmise täitmise osapooled ning nendevahelised õiguslikud suhted ning infotehnoloogilised lahendused, mida on kasutusele võetud isikusamasuse tuvastamiseks teenusepakkujate poolt, kellele isikusamasuse tuvastamise tegevus edasi antakse.

Isikusamasuse tuvastamine on finants- ja krediidiasutusele hoolsusmeetmeks rahapesu ja terrorismi rahastamise tõkestamisel. Selle eesmärgiks on takistada kuritegelikult saadud vara varjamist või moondamist ja tõkestada rahapesu toimepanemist. Krediidiasutus on rahapesuvastase võitluse osas rahapesu ja terrorismi rahastamise tõkestamise seaduse mõistes kohustatud isik kohaldamaks olulisi hoolsusmeetmeid oma igapäevatöös.

Aina suuremat rolli mängib infotehnoloogia ka finantsmaailmas, seega krediidiasutused kujundavad oma ärimudeleid ümber, et selliste tehnoloogiatega kohalduda. Infotehnoloogia kasutusele võtmisel on mitmeid eeliseid – kuluefektiivsus, administratiivse koormuse vähenemine, efektiivsus, automatiseerimine, teenuste paindlikkuse suurendamine ning klientide piiriülese teenindamise lihtsustamine. Krediidiasutuse kohustus tuvastada klientide isikusamasus on üks nendest valdkondadest, milles nähakse võimalust rakendada *FinTech* lahendusi. Infotehnoloogia kasutamisel isikusamasuse tuvastamise kohustuse täitmisel tekivad aga ohud, mis varasemalt kasutusel olnud alternatiivsete lahendustega tõusetunud ei ole. Olukorras, kus on kasutusele võetud infotehnoloogilised lahendused krediidiasutuse enda kohustuse täitmiseks, on vajalik tagada, et klient ei oleks eelnimetatud lahenduste kasutusele võtmisega halvemas olukorras, kui varasemalt.

FinTech areng on kiirenenud alles viimastel aastakümnetel koos üldiste infotehnoogiliste arengutega ning sellest tulenevalt, et tagada klientide ning üldise finantssüsteemi kaitse, on käesolevat valdkonda pidanud oluliseks reguleerida nii Eesti seadusandja kui ka Euroopa Liidu institutsioonid. Sellises kiiresti arenevas sektoris on aga oht olukorra tekkeks, kus õiguslikud regulatsioonid ei ole võimelised ajaga niivõrd kiires tempos kaasas käima ning sätete kohaldumine esinevatele olukordadele võib osutuda keeruliseks. Samuti võivad tekkida põhimõttelised vastuolud ja kaalutlused valdkonna reguleerimisel, kuna seadusandlusel ning õigusorganite poolt kehtestatud põhimõtetel on, arvestades valdkonna spetsiifikat, oht takistada valdkonna edasist arengut ja innovatsiooni. Kuigi elektroonsete vahenditega isikutuvastus rahapesu ning terrorismi rahastamise vastase võitluse kontekstis omab palju eeliseid, mis on võimaldanud ettevõtetel vähendada nende nõuete täitmise kulu ning suurendada enda klientide arvu, on elektroonse isikutuvastamisega seotud mitmeid riske ning ohte. Nendeks riskideks võivad olla inimgrupi tekkimine, kes varasemalt kasutas alternatiivseid lahendusi, ent infotehnoloogilistele süsteemidele ligipääs on erinevatel põhjustel raskendatud või välistatud, ligipääsu puudumine isikutel, keda mõjutavad nendest mitteolenevad faktorid ning infotehnoloogilistele lahendustele omasete riskide realiseerumine.

Tegevuse edasiandmine on oma olemuselt äripraktika, mille kohaselt antakse teatud tegevus edasi täitmiseks kolmandale osapoolele ehk teatud tegevused või töökohad delegeeritakse osapoolele, kes on võimeline seda funktsiooni täitma kiiremini, paremini ja odavamalt. Isikusamasuse tuvastamise tegevuse edasiandmine tähendab, et ettevõte, kellega on krediidiasutus sõlminud lepingu, tagab isikute isikusamasuse tuvastamise samadel tingimustel ja kvaliteedil, mil oleks selleks kohustatud krediidiasutus.

Tegevuse edasiandmist käsitlevates juhendites ning suunistes eristatakse tegevuse edasiandmise kontekstis kõikidest funktsioonidest kriitilisi ja olulisi funktsioone. Kriitilised ja olulised funktsioonid on need, millel võib olla suur mõju krediidiasutuse riskiprofiilile ja sisemisele reeglistikule ning seetõttu on nende edasiandmisele sätestatud ka lisanõuded. Tegevuse edasiandmise juhendid ning suunised ei liigita funktsioone selgesõnaliselt kriitiliseks või oluliseks funktsiooniks ning vastav liigitus puudub ka Eesti ning Euroopa Liidu üleses õigusruumis. Selle tuvastamine isikusamasuse tuvastamise edasiandmise kontekstis on aga oluline juba enne tegevuse edasiandmise kokkuleppe sõlmimist seetõttu, et vastavalt tegevuse

liigitusele, on teatud täiendavaid aspekte, millega peab arvestama lepinguliste suhete kujundamisel ning lepingulistesse suhetesse astumise eel sellest tulenevad ohud maandama. Kriitilisi ja olulisi funktsioone täpsustavate ning kirjeldavate õigusaktide ning suuniste kohaselt on isikusamasuse tuvastamise funktsioon kriitiline või oluline funktsioon ning seda on võimalik anda teenusepakkujale edasi, arvestades kriitiliste või oluliste funktsioonide edasiandmisele sätestatud erisustega.

Isikusamasuse tuvastamise kohustuse edasiandmise osapoolteks käesoleva töö raames on krediidiasutus, teenusepakkuja ning krediidiasutuse klient. Selleks, et krediidiasutus saaks funktsiooni täitmist anda teenusepakkujale edasi, sõlmitakse kirjalik leping arvestades järelevalveasutuste poolt esitatud täiendavate nõuetega. Osapoolte vahel sõlmitud lepingu näol on tegemist võlaõigusliku lepinguga, mis reguleerib kahe osapoole omavahelist suhtlust. Asutuse suhet kliendiga reguleerib kirjalikus või kirjalikku taasesitamist võimaldavas või elektroonilises vormis sõlmitud eriliigilised lepingud. See tähendab, et krediidiasutuse ja kliendi vahel on lepinguline suhe. Kliendi ja teenusepakkuja vahel ei ole lepingulisi õiguslikke suhteid.

Teenusepakkujaid, kes pakuvad isikusamasuse tuvastamise lahendusi, on turul mitmeid. Suur osa leitavatest isikusamasuse tuvastamise lahendustest ning teenusepakkujatest kasutab krediidiasutuse klientide tuvastamiseks tehisintellektile baseeritud lahendusi. See tähendab, et masinvastutuse kohaseid järeldusi isikusamasuse tuvastamise kontekstis analüüsitakse tehisintellektile põhinevaid lahendusi pakkuvate teenusepakkujate põhjal. Tehisintellekti poolt toime pandud rikkumise eest isikusamasuse tuvastamise kohustuse täideviimisel tehisintellekt vastutada ei saa ning selle vastutuse peab üle kandma isikule, kes omab teadvust ning õigusvõimet. Erinevate Euroopa Liidu institutsioonide juhendid ja suunised sisaldavad võimalikke vastutusküsimuste lahendusi, ent õiguslikult siduvalt neid vormistatud ei ole. Vastavalt erinevatele käsitlusele, vastutab tehisintellekti poolt toime pandud rikkumise eest isik, olenemata tema süüst, kes omab tehisintellekti tegevuse üle kontrolli. Seega olukorras, kus teenusepakkuja täidab krediidiasutuse isikusamasuse tuvastamise kohustust omavahelise lepingu alusel, ei ole võimalik ettevõttel vastutusest vabanemiseks tugineda tehisintellekti poolsele rikkumisele. Kuna Euroopa Liidus ei ole jõutud ühtsele arusaamale tehisintellekti vastutuse küsimustes, tähendab see, et õiguslike vaidluste vältimiseks on oluline roll vastutuse

küsimuste reguleerimisel poolte vahelises isikusamasuse tuvastamise tegevuse edasiandmise lepingus.

Masintekkelise rikkumisena on käsitletav tehisintellekti poolt toime pandud rikkumine isikusamasuse tuvastamisel, näiteks isikusamasuse tuvastamata jätmine, esitatud teabe mitte kontrollimine usaldusväärsest ja sõltumatust allikast hangitud teabe põhjal, kliendi esindaja isikusamasuse ja esindusõiguse tuvastamata jätmine, tegeliku kasusaaja tuvastamata jätmine ja tema isikusamasuse kontrollimiseks meetmete mitte võtmine, varalise ja mittevaralise kahju tekitamine, isikusamasuse tuvastamise nurjumine, lepingutingimuste mitte täitmine ning isikusamasuse tuvastamine vääralt.

Finantsinspektsioon on oma tegevuse edasiandmise juhendis märkinud, et vaatamata tegevuse edasiandmisele, ei vabane krediidiasutus vastutusest klientide ning järelevalveasutuse ees. Krediidiasutustele on sätestatud ulatuslikud nõuded teenusepakkuja taustakontrolli teostamiseks, mis raskendab krediidiasutuse poolt vastutusest vabanemist, st paneb krediidiasutuse hoolsuskohustuse teenusepakkuja valikul kõrgeks ning raskendab või lausa välistab tegevuse edasiandmisel tekkivate rikkumiste korral tuginemist teenusepakkuja poolsele rikkumisele või puudujääkidele. Seega tekib krediidiasutusel isikusamasuse tuvastamise kohustuse täitmata jätmisel, ka juhul, kui rikkumine on masintekkeline ja krediidiasutuse isikusamasuse tuvastamise kohustus on edasi antud teenusepakkujale, väärteovastutus. Lisaks sellele, et krediidiasutus on seaduse alusel kohustatud klientide isikusamasust tuvastama ning on lepingulistes suhetes teenusepakkujaga, on krediidiasutusel lepingulised suhted ka kliendiga. Krediidiasutuse isikusamasuse tuvastamise kohustus kliendi ja krediidiasutuse vahelises suhtes tekib võlaõigusseadusest ning panga kohustusi sätestavatest üldtingimustest. Juhul, kui krediidiasutus ei ole rakendanud kliendi tugevat autentimist, sh kui isikusamasuse tuvastamise kohustuse rikkumine on toimunud masintekkeliselt, on kliendil võimalik nõuda krediidiasutuselt nii varalise kui ka mitte varalise kahju hüvitamist tuginedes võlaõigusseadusele. Krediidiasutuste kohustus tuvastada kliendi isikusamasus võib tuleneda ka nende lepingulise suhte osaks saanud üldtingimustest. Eelnimetatu üldtingimuste näol on tegemist tüüptingimustega, mis on saanud osaks poolte vahel sõlmitud lepingust. Vastavalt võlaõigusseadusele, on tüüptingimus tühine juhul, kui tüüptingimus kahjustab teist lepingupoolt ebamõistlikult. Vastutust välistavad asjaolud üldtingimustes, mis on saanud

kliendi ja krediidiasutuse vahelise võlaõigusliku lepingu osaks, ei saa välistada krediidiasutuse seadusest või lepingust tulenevat vastutust ning sellesisulised üldtingimustes sisalduvad tüüptingimused on tühised.

Teenusepakkuja ning kliendi vahel lepingulised suhted puuduvad. Euroopa Liidu ülesed tehisintellekti vastutuse kohased käsitlused annavad kliendile võimaluse tugineda võlaõigusseaduse 2. jaole ehk vastutusele suurema ohu allikaga tekitatud kahju eest ehk kahju tekitamise eest vastutab ohu allikat valitsenud isik sõltumata oma süüst. See tähendab, et juhul, kui tehisintellekti poolt on toime pandud masintekkeline rikkumine krediidiasutuse poolt edasiantud isikusamasuse tuvastamise kohustuse täitmisel, vastutab kliendi ees rikkumise eest ka teenusepakkuja ning klient saab esitada teenusepakkuja suhtes endale tekitatud varalise ja mittevaralise kahju hüvitamise nõude suurema ohu allika poolt tekitatud kahju käsitlevate sätete alusel. Teiseks võimalikuks teenusepakkuja vastutuse aluseks kliendi ees saab pidada tootevastutuse direktiivi. See võimaldaks samuti rakendada mittesüülist vastutust. Samas, seoses tehisintellekti olemusega, võib olla keeruline eelnimetatud direktiivile tugineda, kuna tootevastutusele tuginedes on vajalik siduda negatiivne tagajärg konkreetse isikuga. See aga võib tehisintellekti puhul osutuda keerukaks. Juhul, kus võib tekkida mittevaraline kahju, näiteks isikuandmete väärkasutamine, ei ole võimalik tootevastutust kohaldada.

Eeltoodu tähendab, et juhul, kui kliendile tekib isikusamasuse kohustuse rikkumisest kahju ning rikkumine oli masintekkeline, on võimalik kahju hüvitamist nõuda nii krediidiasutuselt lepinguliste ning seadusest tulenevate kohustuste rikkumise eest kui ka rikkumise põhjustanud tehisintellekti omava või kontrolliva füüsilise või juriidilise isiku käest tulenevalt Euroopa Liidu institutsioonide käsitluste alusel. Oluline on jälgida tekkinud rikkumise tagajärgi ning kahju iseloomu selleks, et valida sobiv õiguskaitsevahend, sest mittevaralise kahju hüvitamise nõude korral kõiki eelnimetatud nõude aluseid kasutada ei ole võimalik.

Selleks, et anda krediidiasutuse tegevuse täitmist teisele osapoolele edasi, peab krediidiasutus sõlmima kirjaliku lepingu teise osapoolega. Osapoolte vahel sõlmitud lepingu näol on tegemist võlaõigusliku lepinguga, mis reguleerib kahe osapoole omavahelist suhtlust. Tegevuse nõuetele vastava täitmise eest väärteovastutuse alusel jääb vastutama seaduse mõttes kohustatud isik ehk krediidiasutus olenemata sellest, et funktsiooni täitmist krediidiasutus ise ei teosta või kuidas

on vastutust reguleeritud omavahelises lepingus. Nõudeid tegevuse edasiandmise lepingule on esitatud mitmeid. Kuigi juhendis on toodud välja vastutuse määratlemine, õiguskaitsevahendite kokkuleppe olemasolu osapoolte vahelises lepingus ning võimaliku kahju hüvitamiseks vajalike garantiide kehtestamine, ei ole avatud seda, mida selle all mõeldakse. Samuti on soovitatud teenusepakkuja ning krediidiasutuse vahelise lepingu sõlmimise hetkel kaaluda teenusepakkuja poolt kohustusliku kindlustuse sõlmimist teatud riskide vastu ning selle summa ulatust, täpsustamata, milliste tagajärgede vältimiseks kindlustus sõlmida tuleks ning kas kindlustuse sõlmimise eesmärgiks võiks olla krediidiasutusele tekkinud kahju hüvitamine. Kuigi järelevalveasutusel ning valdkonda suunistavatel institutsioonidel on õigus sekkuda krediidiasutuse ja IT teenusepakkuja privaatautonoomiasse ning lepinguvabadusse, ei täpsusta suunised, juhendid ja seadused nõudeid poolte vahelise vastutuse jagunemiseks, vaid viitavad vajadusele lepingus nendes kokku leppida.

Pooled peaksid sõlmitavas lepingus pöörama tähelepanu ja kaardistama võimalikud rikkumised ja tagajärjed, mis võivad masintekkelistest rikkumistest tekkida, ning sätestama vastutuse jagunemise selliste rikkumiste esinemise korral. Ettepanekud vastutuse jagunemise olukordadeks, mida vaidluste tekkimise vältimiseks tegevuse edasiandmise lepingus käsitlema peaks on:

1. Krediidiasutuse kui isikusamasuse tuvastamiseks kohustatud isiku väärteovastutusest tulenev rahatrahv olukorras, kus isikusamasuse tuvastamise kohustust on rikutud. Olukorras, kus krediidiasutusel tekib väärteovastutus kui kohustatud isikul, ei ole väärteovastutust võimalik teenusepakkujale küll üle kanda, ent juhul, kui rikkumine on toimunud tulenevalt masintekkelisest rikkumisest, mille on põhjustanud teenusepakkuja poolt pakutud lahendus, on võimalik väita, et teenusepakkuja on oma lepingulisi kohustusi rikkunud. Sellest tulenevalt, saades teenusepakkujalt teenuse, mis ei vasta kokkulepitud tingimustele ning on põhjustanud rikkumise, mille tagajärjel on krediidiasutus kandnud kahju väärteovastutuse alusel määratud rahatrahvi ulatuses, on põhjendatud lepingus krediidiasutuse tagasinõudeõiguse reguleerimine vastava rahatrahvi ulatuses teenusepakkujalt. Sellises olukorras peab rikkumine olema põhjustatud tehisintellekti poolsest tegevusest, mitte teenusepakkuja valikul kehtivate nõuete mitte järgmisest.

2. Kliendi poolne lepinguline nõue tulenevalt tema isikusamasuse tuvastamisel tekkinud rikkumisest krediidiasutuse vastu. Kliendil on võimalik krediidiasutuselt poolte vahel sõlmitud lepingu alusel nõuda temale tekitatud kahju hüvitamist olukorras, kus tema isikusamasuse tuvastamisel on toimunud rikkumine. Seda olenemata rikkumise tekkimise põhjusest. Sellest tulenevalt, saades teenusepakkujalt teenuse, mis ei vasta kokkulepitud tingimustele ning on põhjustanud rikkumise, mille tagajärjel on krediidiasutus kandnud kahju kliendi poolt esitatud kahjunõude ulatuses, on põhjendatud lepingus krediidiasutuse tagasinõudeõiguse reguleerimine vastava nõude ulatuses teenusepakkujalt. Sellises olukorras peab rikkumine olema põhjustatud tehisintellekti poolsest tegevusest, mitte teenusepakkuja valikul kehtivate nõuete mitte järgmisest.
3. Kliendi poolne suurema ohu allikaga tekitatud kahju vastutuse/tootevastutuse alusel tekkinud nõue tulenevalt tema isikusamasuse tuvastamisel tekkinud rikkumisest teenusepakkuja vastu. Olukorras, kus kliendile tekib kahju teenusepakkuja poolt kasutusel oleva lahenduse tegevuse tagajärjel isikusamasuse tuvastamisel, on kliendil kahju hüvitamise nõudeõigus teenusepakkuja vastu tulenevalt võlaõigusseadusest ning tootevastutuse direktiivi põhimõtetest. Olukorda, kus klient esitab nõude teenusepakkuja vastu ning teenusepakkuja on kohustatud kahju hüvitama, on pooltel võimalik reguleerida omavahelises lepingus. Kuigi krediidiasutusel on seadusest tulenev kohustus isikusamasus korrektselt tuvastada, ei saa teenusepakkuja seadusest tulenevast vastutusest kliendi ees vabaneda. Seda peaksid osapooled reguleerima omavahelises lepingus, kas ja millises ulatuses on teenusepakkujal kliendi esitatud nõude osas tagasinõudeõigus krediidiasutuse vastu.
4. Erinevate leppetrahvide kehtestamine. Osapooled saavad tegevuse edasiandmise lepingus poolte kokkuleppel kehtestada erinevaid leppetrahve, mille eesmärgiks on rikkumiste vältimine, lepingule mittevastavuse eest leppetrahvi maksmine jne. See tagab kohese reageerimise lepingulistele mittevastavustele ning sellest tulenevate potentsiaalsete kahjuhüvitiste katmise.
5. Lepinguline kokkulepe kindlustuse osas. Kuigi tegevuse edasiandmist käsitlevad suunised mainivad kohustusliku kindlustuse sõlmimist, siis selle kohustuse sisu avatud ei ole. Pooled peaksid lepingus kokku leppima, kas on vajalik sõlmida kindlustus, milliseid kahjusid kindlustus katma on määratud ja kelle kohustuseks kindlustuse

sõlmimine on. Üheks võimaluseks on sõlmida ühel või mõlemal poolel kindlustus kõikide käesolevas töös nimetatud tagajärgede hüvitamiseks, st kõikide nõuete hüvitamiseks, mis isikusamasuse tuvastamise tegevuse edasiandmisel tekkinud masintekkelise rikkumise tagajärjel pooltel tekkida saavad. Juhul, kui kindlustuse sõlmib vaid teenusepakkuja, on võimalik kindlustusmakse võrra teenuse hinda tõsta. Sellisel juhul on vajalik analüüs, kas teenusepakkuja poolt sõlmitud kindlustus on piisavaks kaitseks krediidiasutusele, kellel võivad tekkida lisaks võlaõiguslikele nõuetele ka väärteovastutus.

6. Lepinguline kokkulepe selle osas, kes teenusepakkuja poolt vastutab tehisintellekti poolse rikkumise tagajärgede eest. Kuna Euroopa Liidu õigusaktides ning õiguskirjanduses ei ole üheselt jõutud selgusele selle osas, kes tehisintellektiga seotud isikutest tehisintellekti tegevuse eest vastutab, on mõistlik sätestada see juba tegevuse edasiandmise lepingus. Juhul, kui teenusepakkuja ettevõttes on võimalik väga täpselt määratleda isikud, kes on enim seotud tehisintellektiga ning kes teenusepakkuja hinnangul peaksid vastutama, peaks selle lepingus kirjalikult sätestama. Samuti on üheks võimaluseks vastutavaks isikuks määrata juriidiline isik ehk teenusepakkuja enda ettevõtte. See on oluline seetõttu, et välistada vastutuse langemine üksikisikutele, kes on küll tehisintellektiga seotud, ent ei vastuta selle rikkumiste eest või kellega ei ole mõistlik vastutust siduda.

Magistritöö annab vastused kõikidele sissejuhatuses püstitatud uurimisküsimustele. Kuna isikusamasuse tegevuse edasiandmise kohta ei leidu ulatuslikku seadusandlust, õiguskirjandust ning kohtupraktikat, on käesolevas töös antud hinnangud ning tõlgendused tehtud lähtuvalt töös käsitletud olukorrast. Lisaks sellele on tehisintellekti kohane õigusraamistik Euroopa Liidu tasandil alles arenemisjärgus. See tähendab, et tehisintellekti vastutuse lahendamisel lähtutakse eelkõige Euroopa Liidu institutsioonide ning õiguskirjanduses kajastunud seisukohtadest, mis võivad lähiaastatel muutuda juhul, kui kehtestatakse tehisintellekti õigusraamistik, mis kaldub kõrvale seni valitsevatest arvamustest.

Liability of the Parties of Outsourcing the Obligation to Identify and Verifiy a Person in the Event of a Machine-related Breach

Abstract

The aim of the master's thesis is to identify the liability of the parties outsourcing the obligation of the identification of a person and the division of liability in the event of a machine-related breach. To achieve this goal, the thesis analyses the nature of outsourcing the activity of the identification of a person based on the applicable guidelines, instructions and legislation in the field, and the requirements and specifications that apply to it in the context of ensuring the identification of a person through the outsourcing of activity using IT solutions. In addition, the aim is to identify the parties involved in the outsourcing of the duty of identification of a person and the legal relations between them and the IT-solutions that have been used for the identification of a person by the service providers to whom the identification activity is outsourced.

An identification of a person is a due diligence measure for financial and credit institutions in preventing money laundering and terrorist financing. Its purpose is to prevent the concealment or alteration of property derived from criminal activity and to prevent money laundering. A credit institution is an obliged entity within the meaning of the Money Laundering and Terrorist Financing Prevention Act to apply significant due diligence measures in its daily work.

Information technology is playing an increasingly important role in the financial world, so credit institutions are reshaping their business models to adapt to such technologies. The adoption of information technology has several advantages – cost efficiency, reduction of administrative burden, efficiency, automation, increased flexibility of services and simplification of cross-border customer service. The duty of a credit institution to identify customers is one of the areas in which it is possible to implement *FinTech* solutions. However, the use of information technology in fulfilling the duty to identify a person poses risks that have not increased with the alternative solutions previously used. In a situation where IT solutions have been introduced to fulfil the credit institution's own obligation, it is necessary to ensure

that the customer is not in a worse situation than before by implementing the aforementioned solutions.

The development of *FinTech* has accelerated only in recent decades with general IT developments, and as a result, in order to ensure the protection of customers and the general financial system, both the Estonian legislature and the European Union institutions have considered it important to regulate this area. However, in such a fast-growing sector, there is a risk of developing a situation where legal regulations are not able to follow up at such a rapid pace with time and that the application of the provisions to existing situations could present difficulties. There may also be fundamental contradictions and considerations in the regulation of the field, as the legislation and the principles established by the judicial authorities, taking into account the specifics of the field, risk hindering the further development and innovation of the field. Although electronic identification in the context of the fight against money laundering and terrorist financing has many benefits that have enabled companies to reduce the cost of complying with these requirements and increase the number of their customers, there are a number of risks and dangers associated with electronic identification. These risks may include the emergence of a group of people who have used alternative solutions in the past, but access to information technology systems is difficult or excluded for various reasons, lack of access for those affected by factors beyond their control, and the realization of risks associated with information technology solutions.

Outsourcing is by nature a business practice whereby certain activities are outsourced to a third party, i.e., certain activities or jobs are delegated to a party who is able to perform those functions faster, better and cheaper. The outsourcing of activities of identification of a person means that the undertaking with which the credit institution has entered into a contract ensures the identification of a persons under the same conditions and with the same quality as the credit institution would be required to do.

The instructions and guidelines for outsourcing distinguish between critical and significant functions from all functions in the context of outsourcing. Critical and significant functions are those that may have a significant impact on a credit institution's risk profile and internal rules and therefore additional requirements are set for their outsourcing. The instructions and guidelines for the outsourcing of an activity do not explicitly classify functions as critical or

important, and the corresponding classification does not exist in the jurisdiction across Estonia and the European Union. However, its identification in the context of the outsourcing of identification of a person is important even before the outsourcing contract is concluded, because, depending on the classification of the activity, there are certain additional aspects that need to be taken into account when forming a contractual relationship and addressing the risks arising therefrom before entering into a contractual relationship. According to legislation and guidelines that specify and describe critical and essential functions, the function of identification of a person is a critical or essential function and may be delegated to a service provider, taking into account the specificities of the outsourcing of critical or essential functions.

The parties to the outsourcing of the obligation of identification of a person within the framework of this thesis are the credit institution, the service provider and the customer of the credit institution. In order for the credit institution to be able to outsource the performance of the function to the service provider, a written contract shall be concluded taking into account the additional requirements set out by the supervisory authorities. A contract concluded between the parties is a contract under the law of obligations, which regulates the communication between the two parties. The institution's relationship with the customer is governed by special contracts concluded in writing or in a form that can be reproduced in writing or in electronic form. This means that there is a contractual relationship between the credit institution and the customer. There are no contractual legal relationships between the customer and the service provider.

There are several service providers on the market that offer people identification solutions. A large part of the found people identification solutions and service providers use solutions based on artificial intelligence to identify the credit institution's customers. This means that the findings under machine liability in the context of identification of a person are analyzed on the basis of service providers offering solutions based on artificial intelligence. An artificial intelligence cannot be held liable for the breach committed by an artificial intelligence in the performance of the obligation to identify a person, and this responsibility must be outsourced to a person who has consciousness and legal capacity. The instructions and guidelines of the various European Union institutions contain possible solutions to liability issues, but they are

not legally binding. According to different approaches, a person who has control over the activities of an artificial intelligence is liable for the breach committed by the artificial intelligence, regardless of its fault. Thus, in a situation where the service provider fulfils the duty identify a person of a credit institution on the basis of a contract between them, it is not possible for an undertaking to rely on a breach by artificial intelligence in order to be released from liability. The lack of a common understanding of the liability of artificial intelligence in the European Union means that the regulation of liability in the contract on the outsourcing of identification activities between the parties plays an important role in avoiding legal disputes.

Machine-made breach is defined as a breach of identification of a person by an artificial intelligence, such as not identifying a person, failure to verify the information provided on the basis of information obtained from a reliable and independent source, failure to identify the customer's representative and the right of representation, failure to identify the beneficial owner and failure to take steps to verify his/her identity, and causing non-pecuniary damage, failure to identify a person, non-compliance with the terms of the contract and misidentification.

The Financial Supervision Authority has stated in its instructions on the outsourcing of its activities that despite the outsourcing of activities, the credit institution is not released from liability to customers and the supervisory authority. Extensive requirements are imposed on credit institutions to perform service provider background checks, which makes it difficult for the credit institution to exempt itself from liability, i.e., places a high level of due diligence on the choice of service provider and makes it difficult or even impossible to rely on non-compliance or deficiencies. Thus, a credit institution incurs misdemeanor liability if it fails to comply with the obligation to identify a person, even if the breach is machine-related and the duty of a credit institution to identify a person has been transferred to the service provider. In addition to the fact that a credit institution is required by law to identify customers and has a contractual relationship with the service provider, the credit institution also has a contractual relationship with the customer. The obligation to establish the identity of a credit institution in the relationship between the customer and the credit institution arises from the Law of Obligations Act and the general conditions of the obligations of the bank. In case a credit institution has not implemented strong customer authentication, including if the breach of the obligation to identify a person has occurred mechanically, the customer may demand

compensation for both proprietary and non-proprietary damage based on the Law of Obligations Act. The obligation of credit institutions to identify a customer may also arise from the general terms and conditions that have become part of their contractual relationship. The above general terms and conditions are standard terms and conditions that have become part of the contract concluded between the parties. According to the Law of Obligations Act, a standard term is void if the standard term unreasonably damages the other party. Circumstances precluding liability in the general terms and conditions which have become part of the contractual agreement between the customer and the credit institution cannot exclude liability arising from the law or the contract of the credit institution, and the standard terms and conditions contained therein are void.

There is no contractual relationship between the service provider and the customer. The European Union's approach to the liability of artificial intelligence gives the customer the opportunity to rely on section 2 of the Law of Obligations Act, i.e., liability for damage caused by a major source of danger, i.e., the person who controlled the source of risk is liable for the damage regardless of culpability. This means that if an artificial intelligence has committed a machine breach in the credit institution's compliance with the duty of identification of a person, the service provider is also liable to the customer for the breach and the customer can claim compensation for material and non-material damage caused against the service provider on the basis of the provisions concerning the liability for damage caused by major source of danger. Another possible basis for the service provider's liability to the customer is the Product Liability Directive. It would also allow for non-fault liability. However, due to the nature of artificial intelligence, it may be difficult to rely on the above-mentioned Directive, as reliance on product liability requires a negative consequence to be attributed to a specific person. However, this can be difficult in case of artificial intelligence. In cases where non-pecuniary damage may occur, such as misuse of personal data, product liability cannot be applied.

The aforementioned means that if the customer suffers damage as a result of a breach of a duty of identification a person and the breach was machine-made, it is possible to claim damages from the credit institution for breach of contractual and legal obligations as well as from the natural or legal person who owns or controls the artificial intelligence that caused the breach, according to the approaches of the European Union institutions. It is important to monitor the

consequences of the breach and the nature of the damage in order to choose an appropriate remedy, as it is not possible to use all the grounds for the aforementioned claim in the case of a claim for compensation for non-pecuniary damage.

In order to outsource the performance of a credit institution's activities to another party, the credit institution must enter into a written contract with the other party. A contract concluded between the parties is a contract under the law of obligations, which regulates the communication between the two parties. The obligated person within the meaning of the law, i.e., the credit institution, remains liable for the performance of activities in accordance with the requirements on the basis of misdemeanor liability, regardless of the fact that the credit institution does not perform the function itself or how the liability is regulated in the mutual contract. There are a number of requirements for an outsourcing contract. Although the guidance sets out the definition of liability, the existence of a contract on remedies in the agreement between the parties and the establishment of the necessary safeguards to compensate for possible damages, it is not clear what is meant by this. It is also recommended that at the time of concluding a contract between a service provider and a credit institution, the service provider should consider taking out compulsory insurance against certain risks and the amount, without specifying the consequences and whether the purpose of the insurance should be to indemnify the credit institution. Although the supervisory authority and the referring institutions have the right to interfere with the private autonomy and freedom of contract of the credit institution and the IT service provider, the guidelines, instructions and laws do not specify the requirements for the division of liabilities between the parties but indicate the need to agree on a contract.

The parties to the contract should pay attention to and map out possible breaches and the consequences that may result from machine-made breaches and provide for the division of liabilities in the event of such breaches. The proposed situations for the division of liabilities that should be addressed in the outsourcing contract in order to avoid disputes are:

1. A fine arising from the misdemeanor liability of a credit institution as a person required to identify a person in a situation where the duty to identify a person has been breached. In a situation where a credit institution incurs misdemeanor liability as an obliged entity, it is not possible to outsource the misdemeanor liability to the service provider, but if

the breach has occured due to a machine-made breach caused by the solution offered by the service provider, it is possible to claim that the service provider has breached its contractual obligations. Consequently, when receiving a service from a service provider that does not comply with the agreed conditions and has caused a breach, as a result of which the credit institution has suffered a loss in the amount of the fine imposed on the basis of misdemanour liability, it is justified to regulate the right of redress of the credit institution in the amount of the corresponding fine from the service provider. In such a situation, the breach must be caused by the action of the artificial intelligence system and not by choice of the service provider to not to comply with the requirements.

2. A contractual claim by a customer due to a breach in connection of his/her identification against a credit institution. The customer can demand compensation for the damage caused from the credit institution on the basis of the contract concluded between the parties in a situation where a breach has occurred in his/ her identification. This is regardless of the reason for the breach. Consequently, by receiving a service from a service provider that does not comply with the agreed conditions and has caused a breach as a result of which the credit institution has suffered damage to the extent of the customer's claim, it is justified to regulate the right of redress of the credit institution in the contract to the extent of the corresponding claim from the service provider. In such a situation, the breach must be caused by the action of the artificial intelligence system and not by non-compliance with the requirements applicable by the choice of service provider.
3. A claim against the service provider arising on the basis of liability/product liability for damage caused by a major source of danger by the customer due to a breach of his/her identification. In a situation where the customer suffers damage as a result of the operation of the solution used by the service provider in his/her identification, the customer has the right to claim damages against the service provider pursuant to the Law of Obligations Act and the principles of the Product Liability Directive. The situation where the customer submits a claim against the service provider and the service provider is obliged to compensate the damage can be regulated by the parties in a mutual contract. Although a credit institution has a legal obligation to correctly identify a person, the service provider cannot be released from its legal liability to the customer. This should be regulated by the parties in a contract between themselves as to whether

and to what extent the service provider has a right of redress against the credit institution in respect of the customer's claim.

4. Implementation of various contractual penalties. In the contract on the outsourcing of activities, the parties may, by agreement between the parties, impose various contractual penalties aimed at preventing breaches, paying a contractual penalty for non-compliance with the contract, etc. This ensures an immediate response to contractual non-compliances and the coverage of potential damages deriving from it.
5. Contractual agreement on insurance. Although the outsourcing guidelines mention compulsory insurance, the content of this obligation is not disclosed. The parties should agree in the contract whether it is necessary to take out insurance, which losses the insurance is intended to cover and who is obliged to take out the insurance. One possibility is to take out insurance for one or both parties to compensate for all the consequences mentioned in this thesis, i.e., for all claims that may arise for the parties as a result of a machine-related breach in the outsourcing of identification activities. In case the insurance is taken out only by the service provider, it is possible to increase the price of the service by the insurance premium. In such a case, it is necessary to analyse whether the insurance taken out by the service provider is sufficient protection for the credit institution, which may incur misdemeanor liability in addition to the claims under the law of obligations.
6. Contractual agreement on the liability within the service provider. Since there is no clear consensus deriving from European law nor legal literature on the matter, which person connected to the artificial intelligence is liable for its misdemeanors, it would be reasonable to regulate the matter already in the process of drafting the outsourcing contract. Provided it is possible to identify specific people connected to the artificial intelligence the most and should be liable for its actions, it should be clearly stated in the contract. One possibility is to assign the liability to a legal person, service provider’s company. The agreement of the matter is essential to avoid situations, where the liability falls upon persons connected to the artificial intelligence, but who is not responsible for its actions, or their liability is unreasonable.

The master's thesis provides answers to all the research questions raised in the introduction. As there is no extensive legislation, legal literature nor case law on the outsourcing of an activity

of identification of a person, the assessments and interpretations given in this thesis have been made based on the situation discussed in the thesis. In addition, the legal framework for artificial intelligence at EU level is still evolving. This means that the liability of artificial intelligence will be resolved primarily on the basis of the views of the European Union institutions and the legal literature, which may change in the coming years if the legal framework for artificial intelligence deviates from the prevailing views.

Kasutatud kirjandus

Algoritmiliste süsteemide mõjude reguleerimise väljatöötamise kavatsus („krati VTK“). 14.08.2020, Justiitsministeeriumi avalik dokumendiregister.

Buckley, R.P.; Zetzsche, D. A.; Arner, D. W; Tang, B.W. Regulating artificial intelligence in finance: putting the human in the loop. Sydney Law Review, 42 (1), 03.2021.

Burkadze, K. The legal aspects of artificial intelligence based on the EU experience. Law and World, 2021, 20.

Chau, D. Dijck Nemcsik, M. Anti-money laundering transaction monitoring systems implementation. Finding anomalies. *Sine loco*: Wiley 2020.

EBA. Guidelines on outsourcing arrangements. European Banking Authority koduleht 25.02.2019. Arvutivõrgus: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1

Euroopa Keskpank, pangandusjärelevalve. Algorithmic trading: trends and existing regulation. Euroopa Keskpank, pangandusjärelevalve koduleht. Arvutivõrgus: https://www.bankingsupervision.europa.eu/press/publications/newsletter/2019/html/ssm.nl190213_5.et.html

Euroopa Komisjon, eGovertnment Benchmark 2018: the digitaal efforts of European countries are visibly paying off. Euroopa Komisjoni koduleht, 22.11.2018. Arvutivõrgus: https://digital-strategy.ec.europa.eu/et/node/2424

Euroopa Komisjon. Report on existing remote on-boarding solutions in the banking sector. Assessment of risks and associated mitigationg controls, including interoperability of the remote solutions. Euroopa Komisjoni koduleht. 12.2019. Arvutivõrgus: https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/doc

uments/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf

Euroopa Parlament. Euroopa Liidu õiguse allikad ja kohaldamisala. Euroopa Parlamendi koduleht. Arvutivõrgus: https://www.europarl.europa.eu/factsheets/et/sheet/6/euroopa-liidu-oiguse-allikad-ja-kohaldamisala

Finantsinspektsioon. Finantsinspektsiooni soovituslik juhend „Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks. Finantsinspektsiooni koduleht 26.11.2018. Arvutivõrgus: https://www.fi.ee/sites/default/files/2018-11/FI_AML_Soovituslik_juhend.pdf

Finantsinspektsioon. Finantsinspektsiooni soovituslik juhend „Rahapesu ja terrorismi rahastamise tõkestamise meetmed krediidi- ja finantseerimisasutuses“. Finantsinspektsiooni koduleht 03.07.2013. Arvutivõrgus: https://www.fi.ee/failid/Soovituslik_juhend_Rahapesu_tokestamine.pdf (27.02.2022)

Finantsinspektsioon. Finantsinspektsiooni soovituslik juhend. Nõuded finantsjärelevalve subjekti poolt tegevuse edasiandmisele (outsourcing). 05.08.2019. Arvutivõrgus: https://www.fi.ee/sites/default/files/2019-08/pp%20nr%2004%2005.08.2019%20Tegevuse%20edasiandmise%20FI%20juhend%20uues%20redaktsioonis%20ET_0.pdf

Lior, A. AI entities as AI agents: artificial intelligence liability and the AI respondeat superior analogy. Mitchell Hamline Law Review, 46(5), 2020.

Mahajan, D; Sperling, O; White, O. Digital ID: The opportunities and the risks. McKinsey&Company 2019.

OECD. Digital disruption in Bankind and its impact on competition. OECD koduleht. 2020. Arvutivõrgus: https://www.oecd.org/competition/digital-disruption-in-banking-and-its-impact-on-competition-2020.pdf

Ojamets, I. Juristid jäävad krattide kasutamise reguleerimisega kimbatusse. 02.11.2020. Arvutivõrgus: https://novaator.err.ee/1154043/juristid-jaavad-krattide-kasutamise-reguleerimisega-kimbatusse

Rajpurohit, D. S; Seal, R. Legal definition of artificial intelligence. Supremo Amicus 10, 2019.

Santos Divino, S. Critical considerations on artificial intelligence liability: e-personality proportions. Revista Electroniga Direito Sociedade, 8(2), 2020.

Shields, A. C. Managing artificial intelligence. Law Practice, vol 45, issue 3, 2019, lk 14-15.

Sõltumatu kõrgetasemeline tehisintellekti eksperdirühm (AI HLEG), Eetikasuunised usaldusväärse tehisintellekti arendamiseks. 08.04.2019. Euroopa Liidu Väljaannete Talituse koduleht. Arvutivõrgus: https://op.europa.eu/et/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1

Sõltumatu kõrgetasemeline tehisintellekti eksperdirühm (AI HLEG), 08.04.2021.

Toonela, T. Tegevuse edasiandmise käsitlus finantsvaldkonna õigusaktides. Magistritöö. Juhendaja Kadri Siibak. Tallinn: Tallinna Tehnikaülikool 2019,

Turk, K; Pild, M. Kratiga või kratita- see on küsimus. Robititest ja tehisintellektist tsiviilõiguslikult.. Juridica 1/2019.

Whittaker, A. Artificial intelligence – the new EU guidlines. Journal Of International Banking Law and Regulation, 2019, 34(9).

World Bank. ID4D practitioner's guide: Version 1.0. Washington, 11.2019. Arvutivõrgus: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

Kaevats, M. Kuidas kratt Eesti paremaks teeb? 23.07.2018. Arvutivõrgus: https://medium.com/digiriik/kuidas-kratt-eesti-paremaks-teeb-cfebc526cb47

Finantsinspektsioon. Juhatuse otsus, 05.08.2019 nr 1.1-7/92. Arvutivõrgus: https://www.fi.ee/sites/default/files/2019-08/JHO%2CEuroopa%20Pangandusjärelevalve%20Asutuse%20suuniste%20Tegevuse%20edasiandmise%20suunised%20välja%20andmine..pdf

Euroopa Komisjon, 19.02.2020. Komisjoni aruanne Euroopa Parlamendile, nõukogule ning Euroopa Majandus- ja Sotsiaalkomiteele. Aruanne selle kohta, milline on tehisintellekti, asjade

interneti ja robootika mõju ohtutusele ja vastutusele. Brüssel, COM(2020) 64 final. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52020DC0064&from=ET

Euroopa Komisjon, 19.02.2020. Valge raamat. Tehisintellekt: Euroopa käsitlus tipptasemel ja usaldusväärsest tehnoloogiast. Brüssel, COM(2020) 65 final. Arvutivõrgus: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_et.pdf

20.10.2020, Euroopa Parlament, tehisintellekti tsiviilvastutuse kord. P9_TA(2020)0276. Arvutivõrgus: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_ET.pdf

20.10.2020, Euroopa Parlament, tehisintellekti, robootika ja seonduva tehnoloogia eetiliste aspektide raamistik. P9_TA(2020)0275. Arvutivõrgus: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ET.pdf

Karu, K. Tehisintellekti keerukad küsimused. Juridica 1/2021.

Union. BRICS Law Journal, vol 8, nr 1, 2021.

21.04.2021 Euroopa Komisjon, Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte. ELT COM/2021/206 final. Arvutivõrgus: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0017.02/DOC_1&format=PDF

Lisad järgmise dokumendi juurde: Euroopa Komisjon, 21.04.2021 Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte. ELT COM/2021/206 final. Arvutivõrgus: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0017.02/DOC_2&format=PDF

Kasutatud õigusaktid

Eesti õigusaktid:

Infotehnoloogiliste vahendite abil isikusamasuse tuvastamise ja andmete kontrollimise tehnilised nõuded ja kord - RT I, 04.12.2020, 9.

Krediidiasutuste seadus - RT I, 07.12.2021, 13.

Rahapesu ja terrorismi tõkestamise seadus - RT I, 02.06.2022, 19.

Võlaõigusseadus - RT I, 15.03.2022, 14

Euroopa Liidu õigusaktid:

2. veebruar 2016. aasta Euroopa Komisjoni delegeeritud määrus (EU) 2016/778, millega täiendatakse Euroopa Parlamendi ja nõukogu direktiivi 2014/59/EL seoses asjaolude ja tingimustega, mille korral võib krediidiasutuse või investeerimisühingu tasutavad erakorralised *ex post* osamaksed täielikult või osaliselt edasi lükata, ja kriitiliste funktsioonidega seotud tegevuste, teenuste ja toimingute kindlaksmääramise ning põhiäriliinide ja nendega seotud teenuste kindlaksmääramise kriteeriumidega. – ELT L 131/41.

24. november 2010. aasta Euroopa Parlamendi ja nõukogu määrus (EL) nr 1093/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Pangandusjärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/78/EÜ. – ELT L 331/12, artikkel 16.

Euroopa Parlamendi ja Nõukogu direktiiv 2014/59/EL, millega luuakse krediidiasutuste ja investeerimisühingute finantsseisundi taastamise ja kriisilahenduse õigusraamistik ning muudetakse nõukogu direktiivi 82/891/EMÜ ning Euroopa Parlamendi ja nõukogu direktiive 2001/24/EÜ, 2002/47/EÜ, 2004/25/EÜ, 2005/56/EÜ, 2007/36/EÜ, 2011/35/EL, 2012/30/EL ja 2013/36/EL ning määruseid (EL) nr 1093/2010 ja (EL) nr 648/2012. ETL L 173/190.

Euroopa Parlamendi ja nõukogu määrus (EL) nr 1093/2010.

Kasutatud kohtupraktika

Eesti kohtupraktika:

RKTK 3-2-1-161-10

RKTK 3-2-1-85-09 p 20

TMK 4-07-4261/12

Euroopa kohtupraktika:

EK C-609/19, *BNP Paribas Personal Finance SA versus VE,* ECLI:EU:C:2021:469.

EKo C-911/19, *Fédération bancaire française (FBF) versus Autorité de contrôle prudentiel et de résolution (ACPR),* ECLI:EU:C:2021:599.

Muu kirjandus

AS SEB Pank. AS SEB Pank koduleht. AS SEB Pank üldtingimused. Arvutivõrgus: https://www.seb.ee/sites/default/files/tac/as_seb_pank_yldtingimused_01012021_est.pdf

Basis ID. KYC and AML solution. Basis ID koduleht. Arvutivõrgus: https://www.basisid.com

GetID. A complete Identity verification and KYC solution for fintech companies. GetID kodulehekülg. Arvutivõrgus: https://getid.com/industries/fintech/

Jumio. Automated identity proofing, eKYC and transaction monitoring. Jumio koduleht. Arvutivõrgus: https://www.jumio.com/products/

Kratid Eesti heaks. Krattide projekti koduleht. Arvutivõrgus: https://www.kratid.ee

Passbase. Passbase koduleht. Arvutivõrgus: https://passbase.com

Sumsub. Sumsub koduleht. Arvutivõrgus: https://sumsub.com

Swedbank AS. Swedbank AS üldtingimused. Swedbank AS koduleht. Arvutivõrgus: https://www.swedbank.ee/static/pdf/private/home/important/cond_general_est_2021_01_01.pdf

Tehisintellekti kasutus peab austama põhiõigusi. 18.08.2020. Justiitsministeeriumi koduleht. Arvutivõrgus: https://www.just.ee/uudised/tehisintellekti-kasutus-peab-austama-pohioigusi

Veriff. AML & KYC compliance solution. Veriff kodulehekülg. Arvutivõrgus: https://www.veriff.com/product/aml-kyc-compliance