TARTU ÜLIKOOL
Majandusteaduskond

Ketlin Saar

# TEHISINTELLEKTI KASUTAMISE VÄLJAVAATED RAHAPESU TÕKESTAMISEL EESTI KREDIIDIASUTUSTE NÄITEL

Magistritöö

Juhendaja: professor Maaja Vadi, PhD

Tartu 2024

TEHISINTELLEKTI KASUTAMISE VÄLJAVAATED RAHAPESU TÕKESTAMISEL EESTI KREDIIDIASUTUSTE NÄITEL

Olen koostanud töö iseseisvalt. Kõik töö koostamisel kasutatud teiste autorite tööd, põhimõttelised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

**Sisukord**

## Lühendite loetelu

AI (*Artificial Intelligence*) – tehisintellekt
AML (*Anti-Money Laundering*) – rahapesu tõkestamine
AMLA (*Anti-Money Laundering Authority*) – rahapesuvastane asutus
AMLD (*Anti-Money Laundering Directive*) – rahapesuvastane direktiiv
CDD (*Customer Due Diligence*) – hoolsusmeetmed
CTR (*Cash Transaction Report*) – sularahatehingu teade
DL (*Deep Learning*) – süvaõpe
DNN (*Deep Neural Networks*) – süvanärvivõrgud
DT (*Decision Tree*) – otsustuspuu
FATF (*Financial Action Task Force*) – rahapesu vastane töökond
FIU (*Financial Intelligence Unit*) – finantsluure üksus
ISR (*International Sanctions Report*) – rahvusvahelise finantssanktsiooni teade
KYC (*Know Your Customer*) – tunne-oma-klienti põhimõte
ML (*Machine Learning*) – masinõpe
NLP (*Natural Language Processing*) – loomuliku keele töötlus
NN (*Neural Network*) – närvivõrk
PEP (*Politically Exposed Person*) – riikliku taustaga isik
RAB – Rahapesu Andmebüroo, FIU eestikeelne termin
RF (*Random Forest*) – juhuslik mets
STR (*Suspicious Transaction Report*) – rahapeskahtlusega teade
SVM (*Support Vector Machine*) – toetusvektormasin
TFR (*Terrorist Financing Report*) – terrorismi rahastamise kahtluse teade
UAR (*Unusual Activity Report*) – ebahariliku tegevuse teade
UTR (*Unusual Transaction Report*) – ebahariliku tehingu teade
XAI (*Explainable Artificial Intelligence*) – selgitatav tehisintellekt

TEHISINTELLEKTI KASUTAMISE VÄLJAVAATED RAHAPESU TÕKESTAMISEL EESTI KREDIIDIASUTUSTE NÄITEL

## Sissejuhatus

Rahapesu on olulise majandusliku mõjuga finantskuritegevus, mille vastu võitlemine on vältimatu, et kaitsta eelkõige finantssüsteemi usaldusväärsust, tagada turvalisus ning säilitada vastupanuvõime kuritegevusele. Rahapesu vastu võitlemiseks peavad asutused mõistma enda tegevusega kaasnevaid rahapesuga seotud riske ning neid vastumeetmetega maandama ehk arendama rahapesu tõkestamise süsteeme. Rahapesu tõkestamise süsteemidesse investeerimine on lisaks riskide maandamisele ka oluline regulatsioonidele vastamise ja maine säilitamise eesmärgil, kuid Eesti krediidiasutustele viimastel aastatel tehtud suuremahulised trahvid viitavad rahapesu tõkestamise süsteemides olulistele puudujääkidele.

Üldistatult põhineb asutuste rahapesu tõkestamise süsteem kliendiga seotud informatsiooni kogumisel ja mõistmisel ning kliendi finantstehingute monitoorimisel (Gerlings & Constantiou, 2022). Traditsioonilised tehingute jälgimise süsteemid on reeglitepõhised süsteemid ehk ekspertsüsteemid (Chen et al., 2018; Zhang & Trubey, 2019; Labanca et al., 2022), mis on inimesest sõltuvad (Labib et al., 2020), piiratud ekspertteadmisele (Chen et al., 2018) ja võimaldavad tuvastada vaid üksikuid tehinguid või varasemast teadaolevaid ebatavalisi käitumismustreid (Labanca et al., 2022). Ekspertsüsteeme ei saa kasutada uute rahapesu tehnikate ära tundmiseks (Zhang & Trubey, 2019; Labib et al., 2020; Kute, Pradhan, Shukla, & Alamri, 2021) ning need genereerivad palju valepositiivseid hoiatusi, mida tuleb edasi analüüsida inimesel (Kute et al., 2021; Labanca et al., 2022; Alhajeri & Alhashem, 2023; Bakry, Alsharkawy, Farag, & Raslan, 2023). Lisaks valepositiivsete hoiatuste manuaalsele analüüsimisel kogutakse finantstehingutest nähtuva kahtluse sisustamiseks kliendi kohta erinevatest allikatest täiendavat informatsiooni. Sageli on need käsitsi tehtavad lihtsad, kuid aeganõudvad toimingud (Han et al., 2020). Seega tuginevad traditsioonilised rahapesu tõkestamise süsteemid suuresti eksperdihinnangule ning manuaalselt tehtavatele ja aeganõudvatele toimingutele, mistõttu on kahtlase tegevuse tuvastamise määr madal. Lisaks sellele on rahapesu vastu võitlemine muutunud tehnoloogia kiire arengu (Alhajeri & Alhashem, 2023), finantstehingute ja üldise andmemahu suurenemise, rahapesu keerulise iseloomu ja rahapesuks kasutavate meetodite rohkuse tõttu järjest keerulisemaks (Kute et al., 2021). Need asjaolud muudavad traditsioonilised lähenemisviisid ebaefektiivseks, nõudes innovatsiooni ja pidevat vajadust kohanemiseks.

Rahapesu vastase võitluse standardeid ja meetodeid välja töötava FATF-i avaldatud raportis rõhutatakse uute tehnoloogiate, sealhulgas tehisintellekti, potentsiaali muuta rahapesu tõkestamine traditsiooniliste meetmetega võrreldes kiiremaks, odavamaks ja efektiivsemaks (FATF, 2021). Rahapesu tõkestamisel seostatakse tehisintellektiga kõige enam masin- ja süvaõppemeetodeid (Du-Harpur, Watt, Luscombe, & Lynch, 2020), mille võime käsitleda suuri andmeid, analüüsida struktureerimata teavet, tuvastada keerulisi mustreid ja uuendada ennast ise uue teabega muudavad need potentsiaalselt headeks vahenditeks finantstehingute monitoorimisel (Zhang & Trubey, 2019; Pavlidis, 2023). Lisaks rahapesukahtlaste tehingute potentsiaalselt kiiremale ja täpsemale tuvastamisele võimaldab tehisintellekt töödelda erinevatest allikatest pärinevaid andmeid vähendades seeläbi inimese töökoormust, parandades oluliselt analüüsiprotsessi kiirust ning pakkudes inimesele otsuste tegemisel vajalikku tuge (Han, Huang, Liu, & Towey, 2020). 2018. aastal kaitses Mariel Aim Tartu Ülikoolis magistritöö „Tehisintellekti kasutamispraktikad ja arenguperspektiivid Eesti finantssektori näitel“, mille raames intervjueeritud turuosaliste hinnangul on tehisintellektil kõige suurem perspektiiv rahapesu tõkestamisel ja pettuste tuvastamisel (Aim, 2018).

Käesoleva magistritöö eesmärk on välja selgitada, millised on Eesti krediidiasutuste ja valitsusasutuse esindajate väljavaated tehisintellekti kasutamisel rahapesu tõkestamisel. Teaduskirjanduses käsitletakse valdavalt rahapesu tõkestamises potentsiaalselt sobilikke tehisintellekti lahendusi, mis on olemuselt väga tehnilised. Rahapesu tõkestamine on rangelt reguleeritud ja asutused ei jaga rahapesu tõkestamiseks kasutatavaid meetodeid, mistõttu ei keskendu autor üksikasjalikult erinevatele tehisintellekti lahendustele ja nende toimimisele rahapesu tõkestamisel, vaid selles valdkonnas tegutsevate ekspertide kogemustele ja seisukohtadele selliste lahenduste rakendamisel asutuste süsteemides. Seejuures ei ole autorile teada varasemaid uuringuid, mis käsitleksid tehisintellekti kasutamisega seotud võimalusi ja väljakutseid asutuste rahapesu tõkestamise süsteemides. Sellest lähtuvalt annab käesolev magistritöö aluse selles valdkonnas esinevate võimaluste ja probleemkohtade teadvustamiseks ja edasise uurimise võimaluseks.

Magistritöö eesmärgi saavutamiseks püstitas autor kolm uurimisülesannet. Esiteks anda ülevaade rahapesu olemusest, selle tõkestamise süsteemist ning käsitleda teaduskirjanduse põhjal rahapesu tõkestamiseks potentsiaalselt sobilikke tehisintellekti lahendusi ja nende rakendamisega seotud probleemkohti. Teiseks viia läbi empiiriline uurimus ja koguda informatsiooni Eesti krediidiasutuste ning valitusasutuse ekspertidelt, et

selgitada välja, millistes rahapesu tõkestamise protsessides oleks vajalik tehisintellekti kasutada ja millised on tehisintellekti kasutamisega seotud väljakutsed. Kolmandaks analüüsida kogutud andmeid ning teha järeldusi tehisintellekti kasutamise võimalustest ja väljakutsetest rahapesu tõkestamisel.

Magistritöö koosneb kahest suuremast peatükist. Esimene peatükk ehk magistritöö teoreetiline osa on jagatud kolmeks alapeatükiks. Esimeses alapeatükis käsitleb autor üldistatult rahapesu olemust ning selle tõkestamise kujunemist nii rahvusvaheliselt kui ka Eestis. Teises alapeatükis käsitleb autor rahapesu tõkestamise süsteemi ülesehitust nii Eestis kui ka täpsemalt krediidiasutustes. Kolmandas alapeatükis käsitleb autor üldistatult tehisintellekti olemust, selle lahenduste kasutamise võimalusi rahapesu tõkestamisel ning rakendamisega esinevaid probleemkohti. Teises peatükis ehk magistritöö empiirilises osas viib autor läbi kvalitatiivse uuringu Eesti krediidiasutuste ja rahapesu tõkestamise valdkonnaga kokkupuudet omava valitsusasutuse esindajatega. Eesti rahapesu tõkestamise süsteemis on oluline roll krediidiasutustel, mis peamiselt nende osutavate teenuste tõttu on ka keskmisest kõrgema rahapesu ohuga ja üheks kõige haavatavamaks sektoriks (Rahapesu Andmebüroo, 2024). Krediidiasutuste esindajate kaasamine valimisse annab võimaluse intervjueerida inimesi, kes omavad magistritöö eesmärgi saavutamiseks vajalikke kogemusi ja teadmisi.

Teine peatükk on samuti jagatud kolmeks alapeatükiks, kus esimeses tutvustab autor uurimuse läbiviimise metoodikat ning põhjendab valimi valikut. Magistritöö eesmärgi saavutamiseks viis autor läbi poolstruktureeritud intervjuud, millega kaasas üheksa eksperdi seisukohad. Autor transkribeeris, kodeeris ja analüüsis saadud informatsiooni ning esitab tulemused teises alapeatükis. Kolmandas alapeatükis teeb autor analüüsist saadud tulemuste ja teoreetilises osas käsitletud informatsiooni põhjal järeldused ning toob välja tehisintellekti kasutamise võimalused ja kasutamisega seotud väljakutsed rahapesu tõkestamisel.

Lisaks autori enda poolt intervjuude käigus kogutud andmetele analüüsis autor magistritöö eesmärgi saavutamiseks ja uurimisülesannete täitmiseks erialast teaduskirjandust ning rahapesu tõkestamise regulatiivse ja spetsiifilise iseloomu tõttu tutvus autor ka regulatsioonide, juhendite, raportite, konventsioonide ja seadustega. Magistritöö neljandal leheküljel on välja toodud töös esinevate rahapesu ja tehisintellekti valdkondades laialdaselt kasutatavate lühendite loetelu. Seejuures toob autor töös selguse mõttes eestikeelse termini esmakordsel nimetamisel sulgudes välja ka inglisekeelse vaste.

TEHISINTELLEKTI KASUTAMISE VÄLJAVAATED RAHAPESU TÕKESTAMISEL EESTI KREDIIDIASUTUSTE NÄITEL

Töö autor tänab juhendajat Maaja Vadi igakülgse abi ja toe eest ning retsensenti Kulno Tülk eelkaitsmisel saadud väga põhjaliku ja vajaliku tagasiside eest. Samuti tänab autor kõiki intervjuueritavaid, kes andsid töö valmimisse väga olulise panuse.

Märksõnad: rahapesu, tehisintellekt, ekspertsüsteemid, masinõpe, süvaõpe, loomuliku keele töötlus
Teaduseriala kood CERCS: P176 (tehisintellekt)

## 1. Rahapesu tõkestamine tehisintellektiga: käsitlemise teoreetilised alused

### 1.1. Rahapesu määratlemine ja tõkestamise kujunemine

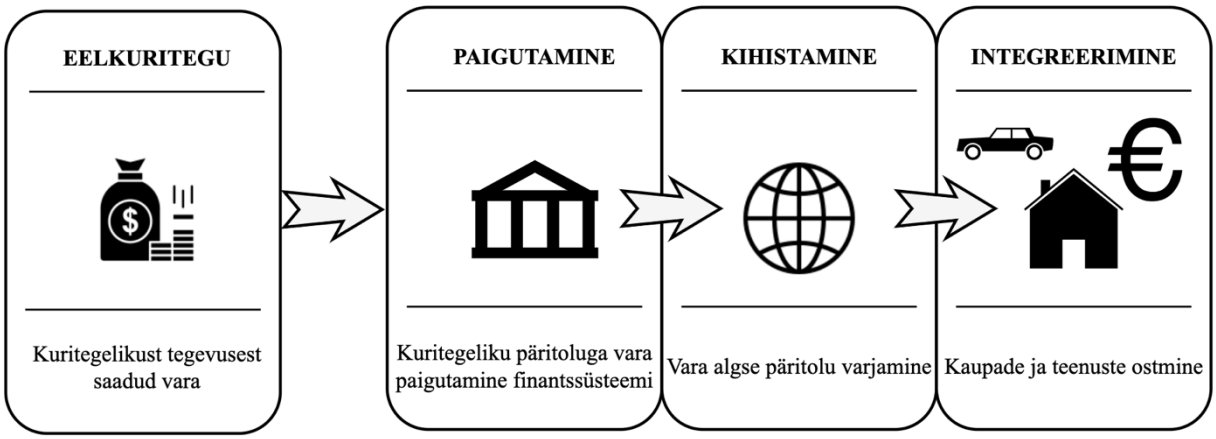
Rahapesu on protsess, mille käigus varjatakse ebaseaduslikust tegevusest saadud vara päritolu eesmärgiga jätta mulje, et tegemist on legaalset saadud varaga (Mekpor, Aboagye & Welbeck, 2018; Reznik, Utkina, & Bondarenko, 2021; Lokanan, 2024). Rahapesu ei ole õiguslikult üheselt defineeritud (Korejo, Rajamanickam, & Md. Said, 2021), kuid üldistatult rõhutatakse kahte põhimomenti: vara on saadud ebaseaduslikust tegevusest ehk toime on pandud kuritegu ning esinevad varjamistunnused ehk tehakse toiminguid, et varjata vara algset päritolu ning näidata seda legaalset saadud varana (Villányi, 2021). Rahapesule kui kuriteole eelnevad rahalist tulu teenivad kuriteod ning selliseid kuritegusid nimetatakse rahapesu eelkuritegudeks. Rahapesu eelkuritegudeks võivad muuhulgas olla narko- ja maksukuriteod, kelmus, omastamine ja korruptsioon (Levi & Reuter, 2006; Villányi, 2021).

Rahapesu jagatakse raha liigutamise järgi klassikaliselt kolme põhistaadiumi: paigutamine (*placement*), kihistamine (*layering*) ja integreerimine (*integration*) (Clark, 1995; Levi & Reuter, 2006; Cassella, 2018; Villányi, 2021). Esimeses staadiumis paigutatakse ebaseaduslikult saadud tulu finantssüsteemi. Traditsioonilised kuritegevused on sularahamahukad tegevused ning nõuavad üldjuhul sularaha paigutamist pangakontole. Kurjategijate eesmärk on oma tegevuses jääda märkamatuks, mistõttu kasutatakse vara ebaseadusliku päritolu varjamiseks erinevaid meetodeid (Villányi, 2021). Suures koguses sularaha võidakse jagada väiksemateks osadeks ning paigutada seejärel erinevatele kontodele (Thommandru, 2023) või segada kuritegeliku päritoluga sularaha seadusliku sularahaintensiivse äriühingu tuluga (Cassella, 2018).

Kihistamise etapis tehakse vara päritolu varjamiseks mitmeid keerulisi ja üldjuhul näiliseid tehinguid (Clark, 1995; Cassella, 2018; Villányi, 2021), et varjata vara algset päritolu ja

muuta see raskesti jälitatavaks. Selles etapis võidakse liigutada raha erinevate jurisdiktsioonide kaudu, segada kuritegeliku päritoluga vahendeid legaalsete vahenditega (Teichmann, 2020), kasutada fiktiivseid äriühinguid ja arveid või osta rahvusvahelistel finantsturgudel investeerimistooteid (Georgieva, 2020). Kolmandas ehk integreerimise etapis kasutatakse nüüdseks näiliselt seaduslikke vahendeid kaupade ja teenuste ostmiseks (Cassella, 2018). Vahendeid kasutatakse kinnisvara ostmiseks (Teichmann, 2020), investeerimiseks, luksuskaupade ostmiseks (Villányi, 2021; Alhajeri & Alhashem, 2023) või ka uute kuritegude toimepanemiseks (Alhajeri & Alhashem, 2023).

Kirjeldatud kolme etapiline lähenemisviis ei ole ammendav, kuna rahapesu on oma olemuselt väga keeruline ja mitmekesine protsess, hõlmates erinevaid kuriteoliike ja võimalusi vara liigutamiseks (Cassella, 2018). Rahapesule võivad iseloomulikud olla ka kirjeldatust rohkem või vähem etappe (Levi & Soudijn, 2020), kuid selline lähenemisviis on kasutusel rahapesu keerulise olemus mõistmiseks (Levi & Reuter, 2006; Cassella, 2018).




*Joonis 1*. Rahapesu protsess
Allikas: autori koostatud Clark, 1995; Levi & Reuter, 2006; Cassella, 2018; Villányi, 2021 põhjal

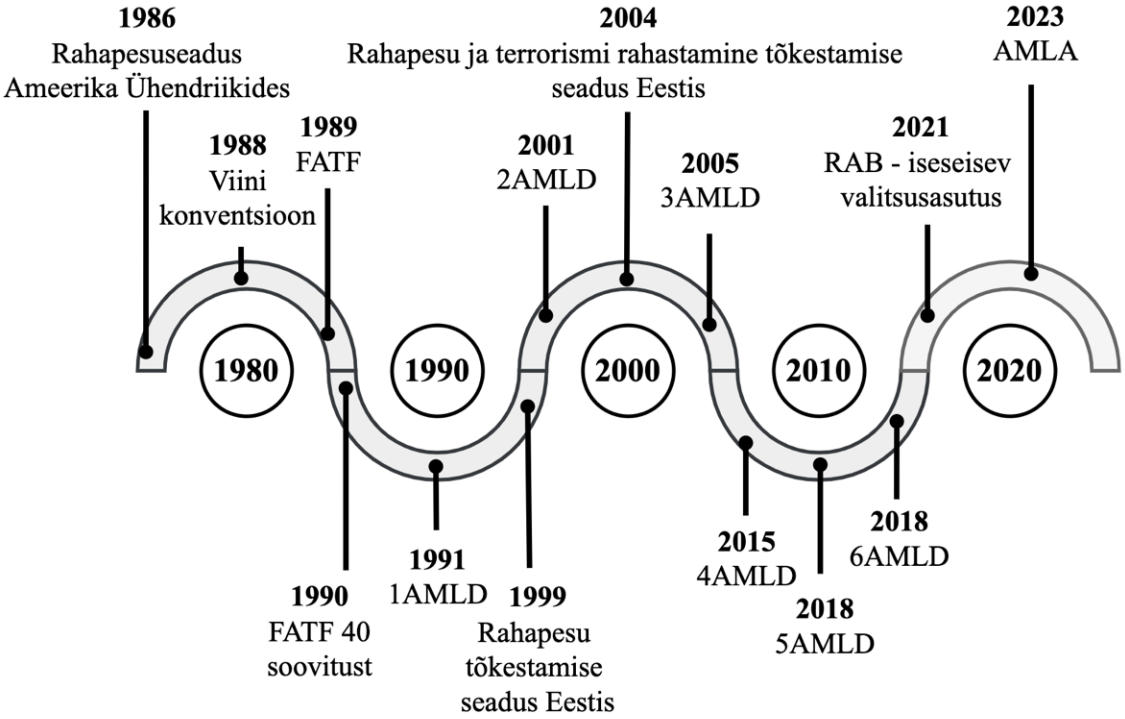
Rahapesu vastu võitlemise alguseks loetakse tegevusi Ameerika Ühendriikides (Unger, 2013), kus 1986. aastal kehtestatud rahapesuseadusega (*Money Laundering Control Act*) kriminaliseeriti narkootikumidega seotud kuritegudest saadud tulu (Tiwari, Gepp, & Kumar, 2020). Selle eesmärk oli võidelda narkokuritegevuse vastu, mis tähendab, et algusaastatel seostati rahapesu vaid narkootikumidega seotud kuritegudega (Unger, 2013). Rahvusvaheliselt anti rahapesu juriidilisele mõistele alus 1988. aastal Viinis toimunud ÜRO konverentsil, kus võeti vastu narkootiliste ja psühhotroopsete ainete ebaseadusliku ringluse

vastane konventsioon ehk Viini konventsioon (United Nations, 1988; Unger, 2013). Viini konventsioon sätestas samuti vaid narkokaubanduse vastu võitlemise rahapesu kriminaliseerimise kontekstis ning andis aluse kuritegelikust tegevusest saadud vara arestimiseks (Borghezio, 2013). Kasvava kuritegevuse vastu võitlemise asutati 1989. aastal rahapesu vastane töökond (*Financial Action Task Force*) ehk FATF, millega sai alguse rahvusvaheline koordineeritud võitlemine rahapesu vastu. 1990. aastal kehtestas FATF 40 soovitust, mis sätestavad põhjaliku meetmete raamistiku, mida riigid peaksid rakendama rahapesu vastu võitlemiseks. FATF-i soovitusi on pärast esialgset avalikustamist mitmeid kordi kohandatud ning neid tunnustatakse üle maailma rahapesu vastu võitlemise rahvusvahelise standardina (FATF, 2012-2023; (Bodescu) Cotoc, Nițu, Șcheau, & Cozma, 2021).

Euroopa Liidu tasemel võeti rahapesu vastu võitlemiseks 1991. aastal vastu esimene rahapesuvastane direktiiv (*Anti-Money Laundering Directive*, AMLD), mille eesmärk oli tõkestada narkokuritegevusest saadud tulu kasutamist kehtestades kohustused ainult finantssektorile (EUR-Lex, 1991; Silva, 2019). Tänase seisuga viimase ehk kuuenda rahapesuvastase direktiivi muudatusi tutvustati 2018. aastal ning selles mainitakse 22 rahapesu eelkuriteona kvalifitseeruvat kuritegu, sealhulgas ka keskkonna-, maksu-, küberkuriteod, pettused ja terrorism (EUR-Lex, 2018; Koster, 2020). Euroopa direktiivid rõhutavad ka vajadust luua igas liikmesriigis iseseisev ja autonoomne finantsluure üksus (*Financial Intelligence Unit*, FIU), mille ülesanne on koguda, analüüsida ja vajadusel edastada rahapesule viitavat teavet pädevale uurimisasutusele ((Bodescu) Cotoc et al., 2021). 2023. aastal jõuti kokkuleppele uue rahapesuvastase asutuse (*Anti-Money Laundering Authority*) ehk AMLA loomises. Asutuse eesmärk on parandada rahapesu ja terrorismi rahastamise tõkestamise järelevalvet ning suurendada FIU-de omavahelist koostööd (Euroopa Komisjon, 2024).

Eestis sai rahapesu vastu võitlemine alguse 1999. aastal, mil jõustus esimene rahapesu tõkestamise seadus. Rahapesu laiema määratlemise tõttu muudeti seaduse nimi 2004. aastal rahapesu ja terrorismi rahastamise tõkestamise seaduseks. Esimese rahapesu tõkestamise seaduse jõustumisega samal ajal loodi Eestis FIU ehk rahapesu andmebüroo talitusena Politseiameti kriminaalosakonnas (Rahapesu Andmebüroo, 2006). 2021. aastast alates on

Rahapesu Andmebüroo (edaspidi ka RAB) Rahandusministeeriumi haldusalasse kuuluv iseseisev valitsusasutus (Rahapesu Andmebüroo, 2022).




*Joonis 2*. Olulised tähised rahapesu tõkestamise kujunemisel
Allikas: autori koostatud Rahapesu Andmebüroo, 2006; Unger, 2013; Silva, 2019; Koster, 2020; Tiwari, Gepp, & Kumar, 2020; (Bodescu) Cotoc et al., 2021; FATF, 2012-2023; Rahapesu Andmebüroo, 2022; Euroopa Komisjon, 2024 põhjal

Kokkuvõtvalt nähtub, et rahapesu on keeruline protsess, mille vastu võitlemise meetmeid on aastate jooksul märkimisväärselt täiustatud. Rahapesu tõkestamise kujunemise algusaastatel seostati rahapesu üksnes narkokaubandusega seotud tegevustega, kuid tänaseks on rahapesu eelkuritegude loetelu oluliselt laienenud. Rahapesu tõkestamise rahvusvaheline, pidev ja tänaseni kestev areng viitab vajadusele pidevalt kohanduda kiiresti muutuva kuritegevusega ning tagada, et kasutusel olevad süsteemid, järelevalvemeetmed ja õiguslikud raamistikud oleksid piisavalt tõhusad ja kohaldatavad.

### 1.2. Rahapesu tõkestamine Eestis ja krediidiasutustes

Rahapesu tõkestamine (*Anti-Money Laundering*, AML) on termin kõikidele protseduuridele, seadustele, regulatsioonidele, mis sunnivad asutusi jälgima oma kliente ja tegema kõik endast oleneva rahapesu vastu võitlemiseks (Labib, Rizka, & Shokry, 2020). Efektiivse rahapesu tõkestamise süsteemi loomise eelduseks on riskihindamine, mis hõlmab

aru saamist erinevatest rahapesuks kasutatavate meetoditest ning mil viisil on asutuse pakutavaid teenuseid võimalik rahapesuks ära kasutada (Lowe, 2017). Asutuse tegevusega kaasnevate rahapesuga seotud riske tuleb vastumeetmetega maandada ehk arendada rahapesu tõkestamise süsteeme. Eestis reguleeritakse rahapesuga seotud riskide hindamise ja maandamise põhimõtteid rahapesu ja terrorismi rahastamise tõkestamise seadusega, mis kohaldub §-is 2 välja toodud isikutele, keda nimetatakse ka kohustatud isikuteks (Riigi Teataja, 2024). Kohustatud isikute rahapesu tõkestamise süsteemi põhielemendid on kliendi tundmise protsessid, finantstehingute monitoorimine ja kahtlase teate esitamine pädevale asutusele (Weber et al., 2018; Milon, 2024). Üldistatult saab seega öelda, et rahapesu tõkestamise süsteem on kahetasandiline, mis ühelt poolt on seotud kliendi tundmisega ning teiselt poolt kliendi finantstehingute monitoorimisega (Gerlings & Constantiou, 2022).

Rahapesuga seotud riskide maandamine tugineb oma kliendi tundmisele ehk tunne-oma-klienti põhimõtte (*Know Your Customer*, KYC) ja hoolsusmeetmete (*Customer Due Diligence*, CDD) rakendamisele (Mugarura, 2014; Shust & Dostov, 2020; He & Chen, 2022). Ärisuhte loomise aluseks on KYC põhimõte, mis hõlmab kliendi isikutuvastust ja kliendile riski määramist (Alkhalili, Qutqut, & Almasalha, 2021). KYC põhimõtte täitmiseks kohaldatakse hoolsusmeetmeid, mille eesmärgiks on aru saada kliendi kavatsustest ning mõista, kas kliendi käitumine ja tehingud vastavad kliendile määratud riskile. Hoolsusmeetmete kohaldamisel tuleb põhjalikult mõista tegelikku kasusaajat, rahaliste vahendite päritolu, tehingupartnereid ning tehingute majanduslikku sisu (Sobh, 2020). Hoolsusmeetmete kohaldamise käigus küsitakse kliendilt täiendavaid andmeid ja selgitusi, kontrollitakse kogutud andmeid ja analüüsitakse registrites ja avalikes allikates leiduvat informatsiooni. See hõlmab muuhulgas kohtuotsusteid ja meediakajastusi, millest leiduv teave võib olla oluline kliendiriski määramisel ja kliendiprofiili kujundamisel. Lisaks sellele kõrvutatakse kliendi tegevust asutusele varasemalt teadaolevale informatsioonile, järelevalveasutuste juhenditele ning rahapesu tüpoloogiatele (Lowe, 2017) ehk rahapesule iseloomulikele mustritele ja tehnikatele. Kliente ja nende tehingupartnereid tuleb kontrollida sanktsioneeritud isikute (Mugarura, 2014; Lowe, 2017; Sobh, 2020) ja ka muude jälgimisnimekirjade (Han, Huang, Liu, & Towey, 2020) suhtes eesmärgiga veenduda, et asutus ei võimaldaks äritegevust mittesobivatele isikutele (Alkhalili, Qutqut, & Almasalha, 2021). Hoolsusmeetmete kohaldamine peab vastama kliendiga seotud riskile (Mugarura, 2014) ehk mida suurem on kliendiga kaasnev risk, seda rohkem on vaja kasutusele võtta

meetmeid, et kliendist ja tema tegevusest aru saada. Asutus peab oma klientide hulgas tuvastama riikliku taustaga isikud (*Politically Exposed Person*, PEP), et nende tegevuse osas kohaldada rahapesu ja korruptsiooni ennetamiseks kõrgema tasemega hoolsusmeetmeid (Mugarura, 2014; Lowe, 2017; Sobh, 2020). Rahapesu tõkestamise süsteemi efektiivsus sõltub KYC põhimõtte ja hoolsusmeetme kohaldamise käigus kogutud andmete kvaliteedist (Alhajeri & Alhashem, 2023).

Makseteenuseid osutavates krediidiasutustes on rahapesu tõkestamise üheks oluliseks osaks tehingute monitoorimine (He & Chen, 2022), mille käigus jälgitakse ja analüüsitakse klientide finantstehinguid eesmärgiga tuvastada rahapesule iseloomulikke ebatavalist või kahtlast käitumist. Tehingute monitooring on kombinatsioon automatiseeritud süsteemidest ja analüütikust (Labanca et al., 2022), mis tähendab, et automatiseeritud süsteem genereerib tehingute monitoorimisel hoiatusi, mida inimene kontrollib ja vajadusel edasi analüüsib (Han et al., 2020). Traditsioonilised tehingute jälgimise süsteemid on reeglitepõhised (Chen et al., 2018; Zhang & Trubey, 2019; Labanca et al., 2022), mis põhinevad ekspertteadmistele ja varasemast teadaolevatele ebatavalistele käitumismustritele (Zhang & Trubey, 2019). Reeglite programmeerimine on lihtne, need on arendatud valdkonna ekspertide poolt ja suudavad hästi lahendada selgelt määratletud loogilisi probleeme, näiteks tuvastada läveväärtust ületanud tehinguid ja rahvusvahelisi makseid (Labib et al., 2020; Choi, Coyner, Kalpathy-Cramer, Chiang, & Campbell, 2020; Kute et al., 2021). Reeglitepõhise süsteemi ehk ekspertsüsteemi väljundid on analüütikute jaoks lihtsasti tõlgendatavad ja kasutatavad (Labanca et al., 2022), kuid need keskenduvad üksikutele tehingutele või lihtsatele tehingumustritele, mistõttu ei saa neid meetodeid kasutada uute rahapesu tehnikate ja skeemide ära tundmiseks ning need ei pruugi ka keeruliste tehingumustrite tuvastamiseks olla piisavad (Zhang & Trubey, 2019; Labib et al., 2020; Kute et al., 2021). Lisaks on see tehnika inimesest sõltuv (Labib et al., 2020), piiratud ekspertteadmisele (Chen et al., 2018), suudab tuvastada vaid varasemast teadaolevaid ebatavalisi käitumismustreid (Labanca et al., 2022) ning reegleid tuleb pidevalt uuendada ning asjakohasena hoida, sest rahapesu on ajas pidevalt muutuv (Chen et al., 2018; Jullum, Løland, Huseby, Ånonsen, & Lorentzen, 2020; Labanca et al., 2022). Reeglitepõhised süsteemid genereerivad palju valepositiivseid hoiatusi (Kute et al., 2021; Alhajeri & Alhashem, 2023; Bakry et al., 2023) ehk hoiatusi, mis on ekslikult märgitud kahtlaseks (Labanca et al., 2022). Automatiseeritud süsteemide poolt genereeritud hoiatusi analüüsivad inimesed, mistõttu kulutab valepositiivsete hoiatuste suur arv analüütiku

väärtuslikku aega ning suurendab riski, et kõrge riskiga hoiatused jäävad märkamata või kiiresti lahendamata (Bakry et al., 2023).

Kahtlusega haaratud tehingute mõistmiseks küsitakse vajadusel kliendilt juurde täiendavaid dokumente ehk kohaldatakse hoolsusmeetmeid. Kahtluse säilimisel avatakse toimik ning toimub täiendav analüüs, kus lisaks tehinguhoiatusele võetakse arvesse hoolsusmeetmete kohaldamise käigus kogutud informatsiooni. Rahapesu kahtlusele viitava informatsiooni korral tehakse teade pädevale asutusele (Kute et al., 2021), milleks Eestis on Rahapesu Andmebüroo. Igas riigis ei pruugi teadete esitamiseks olla samad kriteeriumid, kuid vastavalt esinevatele indikaatoritele esitatakse üldjuhul teateid rahapesu kahtlasest tehingust (*Suspicious Transaction Report*, STR) ((Bodescu) Cotoc et al., 2021). Rahapesu Andmebüroole teavitatakse lisaks rahapesu kahtlasest tegevusest ka ebaharilikust tehingust (*Unusual Transaction Report*, UTR), ebatavalisest tegevusest (*Unusual Activity Report*, UAR), piirsummat ületatavatest sularahatehingutest (*Cash Transaction Report*, CTR), terrorismi rahastamise kahtlusest (*Terrorist Financing Report*, TFR) ja rahvusvahelise finantssanktsiooni kohaldamisest (*International Sanctions Report*, ISR) (Juhend kahtlaste tehingute tunnuste kohta, 2024). Kahtlase tehingu või tegevuse tuvastamisel ei ole selgeid kriteeriume ning avastamis- ja otsustusprotsessi läbiviimisel kasutatakse riskipõhist lähenemist, tuginetakse erialasele kogemusele (Yasaka, 2017) ja Eestis ka Rahapesu Andmebüroo väljastatud juhendile (Juhend kahtlaste tehingute tunnuste kohta, 2024) ja tüpoloogiateadetele (Rahapesu Andmebüroo koduleheküg, kuupäev puudub). Rahapesu Andmebüroos toimub esitatud teadetest sisalduva informatsiooni osas täiendav analüüs ning kahtluse esinemisel edastatakse informatsioon pädevale uurimisasutusele, kus on võimalus kriminaalmenetlus algatamiseks, kohtuotsuseni jõudmiseks ja varade äravõtmiseks (Kute et al., 2021; Pavlidis, 2023).

Lisas A on kokkuvõtlikult välja toodud eelnevalt kirjeldatud tehingute monitoorimisest alguse saav rahapesu tõkestamise süsteem. Nähtub, et rahapesu tõkestamise süsteem on mitmetasandiline (Kute et al., 2021) hõlmates erinevaid protsesse ja analüüsimeetodeid asutuste siseselt ning ka asutuste vahelist teabe jagamist. Erasektoril on oluline roll rahapesu avastamisel ja ennetamisel (Verhage, 2009). Nende juures toimub klientide otsene tegevus, mistõttu on neil ligipääs kliendi poolt esitatud teabele ja tehtud finantstehingutele. Avaliku sektori roll on nendele laekuva rahapesu kahtlase informatsiooni

töötlemine (Verhage, 2009), täiendava informatsiooni kogumine ja laiema pildi analüüsimine, et vajadusel võtta kahtlase tegevuse piiramiseks vastu vajalikke meetmeid (Lowe, 2017).

Ebaefektiivne rahapesu ja terrorismi rahastamise tõkestamine võib asutusele mõjuda negatiivselt mitmelt moel: tegevuse piiramine, mainekahju, rahatrahv ning raskematel juhtudel isegi tegevusloa kaotamine. Eestis on viimastel aastatel olnud mitmeid selliseid näiteid. 2018. aastal tunnistati Eesti krediidiasutuse Versobank AS-i tegevusluba kehtetuks (Finantsinspektsiooni koduleheküIg, 2018). 2019. aastal keelati Taani krediidiasutuse Danske Bank A/S-i filiaali tegevus Eestis, seejuures kahjustas Danske Banki ebaseaduslik tegevus oluliselt finantssektori usaldusväärsust ning Eesti riigi mainet. (Finantsinspektsiooni koduleheküIg, 2019) 2020. aastal kohustati Swedbank AS-i parandama rahapesu vastu võitlemise kontrollsüsteeme (Finantsinspektsiooni koduleheküIg, 2020a) ning samal aastal sai AS SEB Pank miljon eurot trahvi (Finantsinspektsiooni koduleheküIg, 2020b). 2023. aastal trahviti ka AS-i LHV Pank samas summas (Finantsinspektsiooni koduleheküIg, 2023) ja 2024. aastal piirati AS-i TBB pank tegevust makseteenuste osutamisel (Finantsinspektsiooni koduleheküIg, 2024).

Asutusel tuleb rahapesuga seotud riskide maandamiseks kohaldada riskihinnangust lähtuvalt hoolsusmeetmeid, et mõista kliendi tegevust ning rahaliste vahendite päritolu. Finantstehingute analüüsimiseks on traditsiooniliselt kasutusel ekspertsüsteemid, mis suudavad hästi lahendada selgelt määratletud loogilisi probleem ning süsteemi väljundid on analüütikute jaoks lihtsasti tõlgendatavad. Sellised süsteemid on piiratud ekspertteadmisele, vajavad pidevat uuendamist, suudavad tuvastada vaid varasemalt teadaolevaid rahapesule viitavaid ebatavalisi tehingumustreid ega ole piisavad uute rahapesu tehnikate tundmiseks. Asutuse rahapesu tõkestamise süsteemidesse investeerimine on oluline riskide maandamise, regulatsioonidele vastamise ja maine säilitamise eesmärgil, kuid Eesti krediidiasutustele viimastel aastatel tehtud suuremahulised trahvid viitavad rahapesu tõkestamise süsteemis olulistele puudujääkidele.

### 1.3. Tehisintellekti määratlemine ja kasutamine rahapesu tõkestamisel

Üldistatult defineeritakse tehisintellekti (*Artificial Intelligence*, AI) kui tehnoloogiat, mis võimaldab masinatel jäljendada keerulisi inimoskusi (Sheikh, Prins, & Schrijvers, 2023) ning lahendada intelligentsete inimestega samasuguseid ülesandeid (Scherer, 2015). Seejuures ei ole üheselt määratletud, millised on „keerulised inimoskused“ või „intelligentsed inimesed“ (Sheikh, Prins, & Schrijvers, 2023). Sellest tulenevalt ei ole tehisintellekti mõiste

üheselt defineeritud (Scherer, 2015; Schmidt, 2020), mis on põhjustanud segaduse tehisintellekti ja selle alla kuuluvate meetodite osas. Tehisintellektile on iseloomulik võimekus analüüsida suurel hulgal andmeid, teha järeldusi, iseseisvalt õppida (Zhang & Lu, 2021) ja teha seda kõike kiiresti (Adeyeri, 2024) muutes erinevad tehisintellekti meetodid (Choi et al., 2020) potentsiaalselt vajalikeks rahapesu tõkestamise vahenditeks. Seejuures on tehisintelleki kasutamist käsitletud kõige enam tunne-oma-klienti ehk KYC põhimõtte täitmisel ja finantstehingute monitoorimisel (Pavlidis, 2023).

KYC põhimõtte täitmisel on toeks loomuliku keele töötluse (*Natural Language Processing,* NLP) lahendus, mis võimaldab erinevatest allikatest pärinevaid andmeid (registrid, dokumendid, nimekirjad, meedia) töödelda ning inimesele kättesaadavaks muuta. Asutusele teadaolevate andmetega kombineerides suudavad sellised lahendused põhistada kahtlust (Milon, 2024), teha inimesele info analüüsimise lihtsamaks, olla oluline kliendiriski määramisel, kliendi mõistmisel, võimaliku pettuse tuvastamisel (Han et al., 2018; Weber et al., 2018; Pavlidis, 2023) ja kliendiandmete uuendamisel (Chen, Huang, & Chen, 2020). NLP lahendused aitavad vähendada inimese töökoormust visualiseerides erinevatest allikatest pärineva informatsiooni ühe kogumina (Han et al., 2020). NLP suudab sekunditega läbi vaadata tuhandeid dokumente/artikleid parandades oluliselt uurimisprotsessi kiirust ning pakkudes inimesele vajalikku teavet lõpliku otsuse tegemisel (Han et al., 2020). NLP hõlmab sisu tuvastamist, masintõlkimist, informatsiooni eraldamist, klassifitseerimist (Han et al., 2020).

Mitmed autorid käsitlevad tehisintellekti ühe meetodina ka reeglitel põhinevaid ekspertsüsteeme (Choi et al., 2020; Angelov, Soares, Jiang, Arnold, & Atkinson, 2021), mida kasutatakse traditsiooniliselt tehingute monitoorimisel. Selliste süsteemide puhul täidavad arvutiprogrammid inimeste poolt lihtsasti sõnastatud loogilisi probleeme (reegleid) ning õppimise ja intelligentsuse vaheline otsene seos puudub (Choi et al., 2020). Tehisintellekti seostatakse kõige enam masinõppe ja selle alla liigituva süvaõppe meetoditega (Du-Harpur et al., 2020) millel on potentsiaali tuvastada tehingute monitoorimisel ebaharilikke ja rahapesu kahtlusele viitavaid tehinguid ning keerukaid tehingumustreid (Choi et al., 2020; Bakry et al., 2023). Masinõppe rakendamisest rahapesu tõkestamisel kirjutatud teadusartiklid on üldjuhul kirjeldavad ning vähese informatsiooniga andmetest, mudelist ja sooritusest. See on suuresti tingitud avalikult kättesaadavate andmete puudumisest, mida saaks rahapesu tõkestamiseks kasulike mudelite arendamiseks kasutada (Zhang & Trubey, 2019; Bakry et al., 2023).

Efektiivsete mudelite arendamiseks on vaja reaalseid andmeid, mis on olemas pankadel, kuid need andmed on kaitstud ning neid klientide privaatsuse tagamise eesmärgil üldjuhul ei väljastata (Han et al., 2020).

Tehisintellekti alaliik masinõpe (*Machine Learning*, ML) võimaldab uute andmetega kokku puutudes iseseisvalt õppida, muutuda ja areneda ilma igasuguse sekkumise või abita (Zhang & Trubey, 2019; Labib et al., 2020; Alhajeri & Alhashem, 2023). Masinõppe võime käsitleda suuri andmeid, analüüsida struktureerimata teavet, tuvastada keerulisi mustreid ja uuendada ennast ise uue teabega muudab selle potentsiaalselt heaks mudeliks finantstehingute monitoorimisel (Zhang & Trubey, 2019; Pavlidis, 2023). Masinõppe lahendused võivad aidata täpsemini tuvastada rahapesukahtlusega tehinguid ning vähendada seeläbi valepositiivsete hoiatuste arvu, mis omakorda muudab rahapesu tõkestamiseks efektiivsemaks ning vähendab valepositiivsete hoiatuse analüüsimisele kuluvat kulu (Kute et al., 2021). Rahapesu tõkestamiseks kasutatavad masinõppe meetodid on võimalik väga üldistatult jagada kaheks: juhendatud (*supervised*) õpe ja juhendamata (*unsupervised*) õpe (Choi et al., 2020; Alhajeri & Alhashem, 2023).

Juhendatud õppe puhul on olemas sisend- ja väljundväärtused. Algoritm õpib ajalooliste andmete alusel sisendi ja väljundi vahelist seost ning õpib paranduste tegemiseks uutest andmetest (Alkhalili, Qutqut, & Almasalha, 2021). Juhendatud õppe meetodid püüavad õppida mustreid, mis eristavad rahapesule iseloomulikke tehinguid seaduslikest tehingutest kasutades sealjuures andmeid, kus rahapesule omased sisendid ja väljundid on teada (Jullum et al., 2020). Selline mudel suudab leida kahtlustäratavaid kontosid, tegevusi ja mustreid, mis sarnanevad varasemalt tuvastatud mustrite või treeningandmetega. Rahapesu tõkestamise tööriistada loomiseks on juhendatud õppes kõige sagedamini kasutusel otsustuspuu (*Decision Tree*, DT), juhuslik mets (*Random Forest*, RF) ja toetusvektormasin (*Support Vector Machine*, SVM) (Labib et al., 2020; Alsuwailem & Saudagar, 2020). Seejuures on juhuslik mets kombinatsioon mitmest otsustuspuust ja efektiivne anomaaliate ja kahtlaste tehingute tuvastamiseks (Jullum et al., 2020, Alotibi, Almutanni, Alsubait, Alhakami, & Baz, 2022) ning teotusvektormasin on efektiivne asendus traditsioonilistele reeglipõhistele mudelitele vähendades valepositiivsete hoiatuste arvu (Alkhalili, Qutqut, & Almasalha, 2021).

Juhendatud õppe kasutamine eeldab väljundväärtustuste olemasolu, mis tähendab, et andmestikus tuleb märgendada rahapesukahtlased tehingud (Bakry et al., 2023). Efektiivse rahapesu tõkestamise süsteemi ülesehitamise probleemiks on asjaolu, kus rahapesu kahtlasest

tehingust teavitavad asutused ei saa esitatud teadetele tagasisidet ehk teavet, kas tekkinud kahtlus oli asjakohane või mitte (Zhang & Trubey, 2019). Tagasiside puudumine muudab efektiivse rahapesu tõkestamise süsteemi mudeli arendamise keeruliseks, kuna asutused ei saa vajalikku teavet, mis aitaksid parandada nende soorituse kvaliteeti ja muuta süsteeme efektiivsemaks (Han et al., 2020); Alexandre & Balsa, 2023). Kuna asutused ei saa tagasisidet, milline tehing osutus kahtlaseks, siis ei saa asutused enda andmestikku ka juhendatud õppe meetodi kasutamiseks vajalikult märgendada (Bakry et al., 2023).

Juhendatud õppele vastandub juhendamata õpe, mille korral on olemas ainult sisendid ning väljundid puuduvad. (Alkhalili, Qutqut, & Almasalha, 2021) Juhendamata õppe eesmärk on sisendandmetest tuvastada sarnasusmustreid ning kategoriseerida andmed gruppidesse. Need algoritmid on juhendamata, sest mustrid (mis võivad, aga ei pruugi esineda) ei ole juhitud eesmärgist ja jäetakse algoritmi otsustada (Choi et al., 2020). Lihtsustatult öeldes püüavad juhendamata õppe meetodid tuvastada andmetest mustreid teadmata, millised andmed vastavad rahapesule ja millised mitte (Jullum et al., 2020). See on suur erinevus võrreldes reeglipõhise ja juhendatud õppe meetodiga, mis nõuavad uute mustrite tuvastamiseks ka teavet eelnevalt tuvastatud mustrite kohta. Reeglipõhised meetodid põhinevad ekspertide poolt määratud reeglitel ning neid tuleb pidevalt ajakohastada, kuid ka siis suudavad nad tuvastada ainult kõige lihtsamad rahapesule viitavad tehingud. Juhendatud õppe meetodid on paljulubavad, kuid puuduliku märgendamise tõttu on see piiratud võimalustega. Nendest põhjustest tulenevalt on suure potentsiaaliga juhendamata masinõppe meetodid, mis suudavad tuvastada ka uusi rahapesu mustreid (Labib et al., 2020). Juhendamata õppe puuduseks on jällegi asjaolu, et igasugune hälbiv tehing või tuvastatud muster ei ole iseloomulik rahapesule (Bakry et al., 2023). Levinumad juhendamata õppemeetodid on klasterdamine (*clustering*), assotsiatsioon (*association*) ja anomaaliatuvastus (*anomaly detection*) (Choi et al., 2020). Juhendamata õppes kasutatakse kõige sagedamini närvivõrke (*Neural Network*, NN), millel põhinevad masinõppe alaliigi süvaõppe (*Deep Learning*, DL) lahendused (Zhang & Trubey, 2019; Labib et al., 2020; Choi et al., 2020).

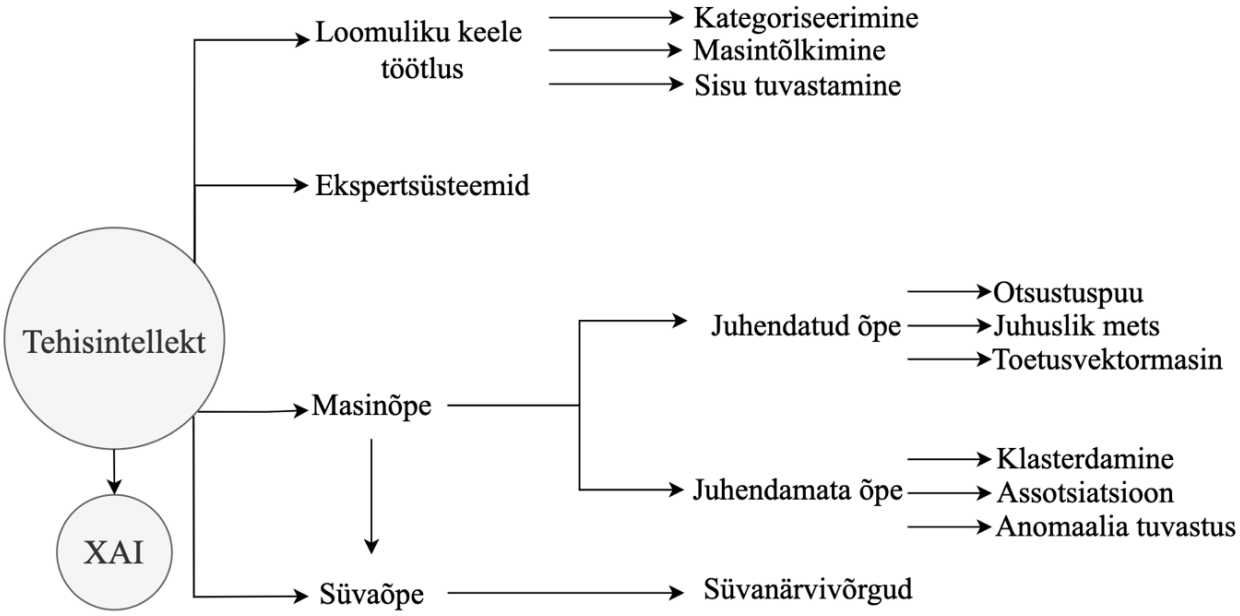
Süvaõpe põhineb süvanärvivõrkudel (*Deep Neural Networks*, DNN) (Alotibi et al., 2022) ning sellised meetodid peaksid tehisintellekti meetoditest andma kõige täpsemad tulemused (Guidotti et al., 2019; Angelov et al., 2021). Sellised mudelid põhinevad inimese jaoks arusaamatutel ja keerulistel algoritmidel, mistõttu on mitmed ja tavaliselt kõige

paremaid tulemusi pakkuvad masinõppe lahendused (DL, DNN) läbipaistmatud ja selgitatavuse probleemiga (Angelov et al., 2021; Hassija et al., 2024). See tähendab, et masina tehtud otsuseid ei suudeta põhjendada ning mudeli käitumise mõistmine ja vigade tuvastamise on väga keeruline. Sellist olukorda nimetatakse ka musta kasti probleemiks (Labib et al., 2020; Hassija et al., 2024). Musta kasti probleemiga seotud mudelid ei ole inimese poolt arusaadavad, kuid oluliste otsuste tegemisel on vajadus, et tehisintellekti algoritmid oleksid oma otsustusprotsessis ka selgitatavad. Tõlgendatavus ja selgitatavus on hädavajalikud eeltingimused tehisintellekti mudelite kasutamiseks tugevalt reguleeritud (Hassija et al., 2024; Adeyeri, 2024) ja tundlikes sektorites, nagu inimese õiguste, raha ja privaatsusega seotud valdkondades (Angelov et al., 2021). Must kasti vastandiks on valge kasti termin, kus mudeli tulemuste taga olevad toimimisviisid ja põhjendused on läbipaistvad ja kergesti mõistetavad (Hassija et al., 2024). Valge kasti meetoditeks on näiteks reeglitepõhised süsteemid, mis on inimestele lihtsasti arusaadavad ja tõlgendatavad (Guidotti et al., 2019) muutes sellised süsteemid usaldusväärseteks (Hassija et al., 2024). Kui valge kasti meetodid on sageli vähem täpsemad, kuid hästi tõlgendatavad, siis musta kasti meetodid on vastupidiselt võimekamad, kuid vähese selgitatavusega.

Kuigi masinõppe meetodid pidevalt täiustuvad ja on pakkumas paremaid tulemusi (Adeyeri, 2024), siis musta kasti probleemist tingituna arendatakse selgitatava tehisintellekti *Explainable Artificial Intelligence*, XAI) valdkonda (Chamola et al., 2023; Hassija et al., 2024). XAI eesmärgiks on arendada tehisintellekti süsteeme, mis ei anna ainult väga head tulemust, vaid võimaldab otsuste ja tegevuste kohta pakkuda ka selgitusi muutes masinaotsuse inimese jaoks usaldusväärsemaks (Angelov et al., 2021; Hassija et al., 2024). Läbipaistvus ja selgitatavus on olulised elemendid usalduse loomisel (Siau & Wang, 2018). XAI on vajalik mudelite tulemuste mõistmiseks ja vigade tuvastamiseks, et seeläbi arendada efektiivsem süsteem. Lisaks sellele on regulaatorite poolne nõue, et kasutusel olevad süsteemid oleksid selgitatavad läbipaistvuse ja mõistmise tagamiseks. XAI valdkond areneb kiiresti, kuid endiselt on väljakutseid läbipaistvuse ja privaatsuse tasakaalustamise ning keerukate mudelite jaoks tõhusate selgituste loomisel. Sellest hoolimata on sellel valdkonnal potentsiaali muuta tehisintellekt inimesele vastuvõetavaks ja usaldusväärseks (Hassija et al., 2024).

Tehisintellektiga seotud probleemidest tulenevalt nähakse vajadust selge õigusraamistiku kehtestamiseks, mis käsitleks tehisintellekti kasutamisega kaasnevaid riske

ning võimaldaks järelevalveasutustel hinnata vastavust (Pavlidis, 2024). 2021. aastal tegi Euroopa Parlament ettepaneku Euroopa Liidus tehisintellekti (*Artificial Intelligence Act*) käsitleva õigusakti loomiseks (Euroopa Parlamendi koduleheküg, kuupäev puudub), mille Euroopa Nõukogu 21.05.2024 heaks kiitis (Euroopa Nõukogu koduleheküg, 2024). See on esimene tehisintellekti kasutamist reguleeriv õiguslik alus, milles kategoriseeritakse erinevad tehisintellekti lahendused vastavalt riskitasemele. See tähendab, et mida suurem on tehisintellekti kasutamisega kaasnev risk, siis seda rangemad on kasutamisega seotud piirangud (Euroopa Nõukogu koduleheküg, 2024). Õigusakt võiks eeldatavasti suurendada asutuste usaldust tehisintellekti kasutamise vastu ja tuua kaasa tehisintellekti laialdasema kaasamise asutuste erinevatesse lahendustesse (Pavlidis, 2024).




*Joonis 3*. Rahapesu tõkestamiseks potentsiaalselt sobilikud tehisintellekti meetodid
Allikas: autori koostatud Han et al., 2020; Choi et al., 2020; Labib et al., 2020; Alotibi et al., 2022; Alhajeri & Alhashem, 2023 põhjal

Tehisintellekti arendamise ja kasutamise protsessis on oluline roll inimesel, kelle tagasiside on oluline süsteemi täiustamisel (Han et al., 2020). Olenemata vastuvõetud automatiseerimise tasemest vajab osa rahapesu tõkestamise protsessist endiselt inimese osalust (Alexandre & Balsa, 2023), sest eksperdi hinnang, intuitsioon ja sotsiaalne kontekst on vajalikud lõpliku otsuse tegemisel (Canhoto, 2021). Tehisintellekt puudub inimesele omane sotsiaalne komponent, kuid Zhang & Lu (2021) leiavad, et tehisintellekti valdkonnas

aset leidev järgmine läbimurre võib loogiliste otsuste tegemisele võimele lisada ka emotsionaalsed võimed ning masina intelligentsus võib varsti ületada inimese oma. Tehisintellekt võib ületada inimese võimekust paljudes töövaldkondades, mistõttu on sellel hetkel potentsiaali asendada inimest rutiinsetel ja madalat teadmist nõudvatel töökohtadel (Siau & Wang, 2018). Rutiinsete toimingute, nagu andmete kogumise, puhastamise ja analüüsimise automatiseerimisega võimaldab tehisintellekt analüütikul keskenduda lisaväärtust loovatele tegevustele muutes seeläbi kogu rahapesu tõkestamise süsteemi efektiivsemaks (Adeyeri, 2024).

Tehisintellekti lahendused on potentsiaalselt võimelised kiiresti analüüsima suuri andmemahtusid ning tuvastama rahapesule viitavaid mustreid (Baader & Krcmar, 2018), kuid andmete kvaliteet, maht ja kättesaadavus on põhilised väljakutsed tehisintellekti reaalsel rakendamisel (Adeyeri, 2024). Pankadel on piiratud võimalus töödelda ainult asutusele teadaolevaid andmeid. Seejuures võivad ühe panga kliendil olla pangakontod ka mitmes teises pangas, mistõttu on reaalne, et ühel asutusel ei ole kliendi kogu tegevusest täielikku ülevaadet. Iga asutus saab analüüsida ainult osa andmetest ehk enda kliendiga seotud finantstehinguid, mistõttu võivad olulised tehingud jääda tähelepanuta või rohkem tähelepanu saada ebaolulised tehingud (Canhoto, 2021). Ebapiisavad või madala kvaliteediga andmed mõjutavad lahenduste toimimise efektiivsust, kuna puudulikest andmetest võivad tuleneda ebatäpsed tulemused (Adeyeri, 2024).

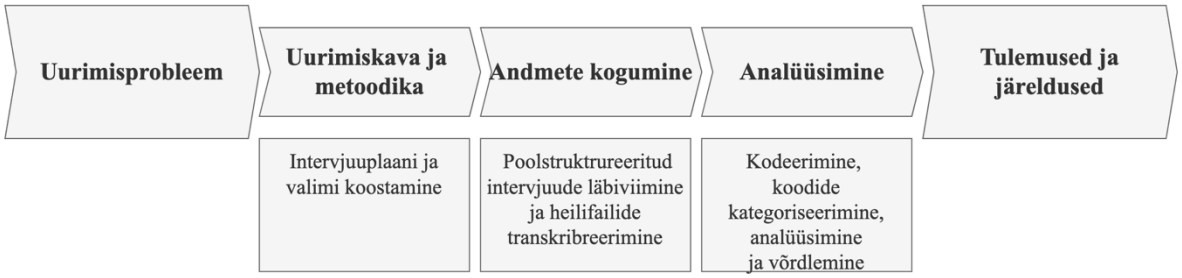
Kokkuvõtvalt on tehisintellektil rahapesu tõkestamise protsessides kõige enam potentsiaali kliendi tundmise põhimõtte täitmisel ja tehingute monitoorimisel. Loomuliku keele töötluse lahendus võimaldab kiirendada analüüsiprotsessi lihtsustades inimese tööd ja pakkudes vajalikku teavet lõpliku otsuse tegemisel. Rahapesu tõkestamise protsess vajab kindlasti inimese osalust, sest tehisintellektil puudub sotsiaalne komponent, mis on lõpliku otsuse tegemisel kriitilise tähtsusega. Tehingute monitoorimisel seostatakse tehisintellekti kõige enam masinõppe meetoditega, millel on potentsiaali tuvastada ebaharilikke ja rahapesu kahtlusele viitavaid tehinguid. Seejuures on häid tulemusi pakkuvatel lahendustel probleeme tõlgendatavuse ja selgitatavusega, mis on hädavajalikud eeltingimused tehisintellekti mudelite kasutamiseks tugevalt reguleeritud valdkondades, sealjuures ka rahapesu tõkestamises. Ilmneb, et kõige parema tulemuse võib saavutada erinevate meetodite kombineerimisel (Canhoto, 2021; Bakry et al., 2023), kus juhendamata masinõppega on võimalik üldisest tehingute andmestikust tuvastada erandlikke juhtumeid ning juhendatud

masinõppega tuvastada väljundväärtuste olemasolul ka rahapesu kahtlusega tehingud (Zhang & Trubey, 2019). Samuti on võimalus kombineerida masinõppe mudeleid ekspertsüsteemidega, et saada hea ja samal ajal ka mõistetav tulemus (Bakry et al., 2023). Tehisintellekti rakendamise suurimad piirangud on andme maht ja kvaliteet. Sageli ei ole ühel asutusel vajalikus koguses andmeid ega vajalikku tagasisidet rahapesu kahtlase tegevuse kohta, et arendada efektiivne rahapesu tõkestamise süsteem.

## 2. Empiiriline uurimus tehisintellekti kasutamisest rahapesu tõkestamisel

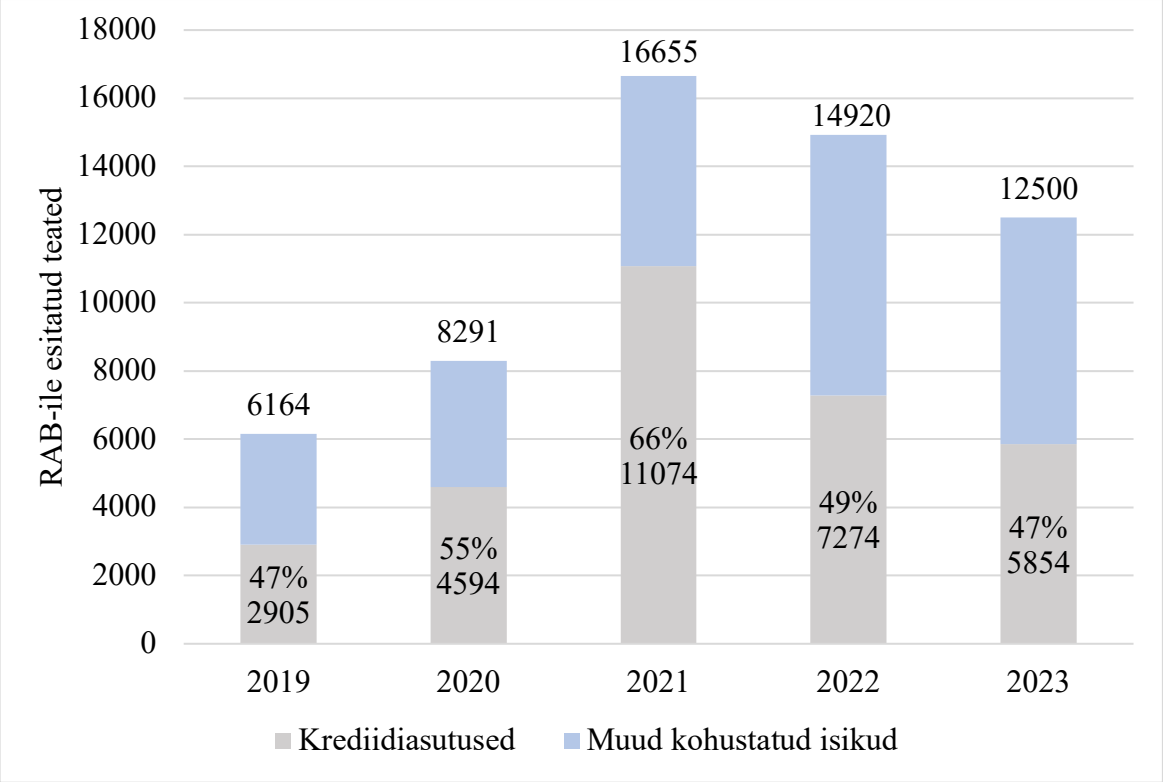
### 2.1. Metoodika ja valimi tutvustus

Magistritöö eesmärgi saavutamiseks ehk mõistmaks tehisintellekti kasutamise väljavaateid rahapesu tõkestamisel viis autor läbi empiirilise uurimuse (vt Joonis 4). Autor annab käesolevas alapeatükis ülevaate uurimisprotsessi etappidest.




*Joonis 4*. Empiirilise uurimisprotsessi etapid
Allikas: autori koostatud

Magistritöö eesmärgi saavutamiseks viis autor läbi kvalitatiivse uurimuse, mis võimaldab avastada tundmatuid või vähe uuritud valdkondi andes ülevaate intervjueeritavate kogemustest ja teadmistest uuritava valdkonna suhtes (Adeyeri, 2024). Töö autorile ei ole teada, et tehisintellekti kasutamist rahapesu tõkestamisel oleks varasemalt põhjalikult Eesti ekspertide näitel uuritud. Töö autor otsustas uurimusse kaasata asutused, mis omavad rahapesu tõkestamise valdkonnaga tugevat kokkupuudet. Rahapesu Andmebüroo avaldatud aastaraamatutele põhinedes on büroole viimase viie aastaga esitatud ligi 60 000 teadet, millest pooled on esitanud krediidiasutused (vt Joonis 5) (Rahapesu Andmebüroo, 2020-2024).




*Joonis 5*. RAB-ile aastatel 2019-2023 krediidiasutuste ja muude kohustatud isikute poolt esitatud teated
Allikas: autori koostatud Rahapesu Andmebüroo 2020-2024 põhjal

Makseteenuseid osutavates krediidiasutustes esineb tavapärasest kõrgem rahapesu risk peamiselt nende osutavate teenuste tõttu. Traditsioonilised pangad on igapäevase makseteenuse osutajad, mistõttu liigub nende vahendusel igapäevaselt väga suure mahus raha. Eesti on seotud piiriülese rahapesuga kihistamise faasis, mistõttu on keskmisest kõrgema ohuga ja üheks kõige haavatavamaks sektoriks krediidiasutused (Rahapesu Andmebüroo, 2024). Samas on pankadel ranged kohustused jälgida hoolikalt oma klientide tegevusi ning juurdepääs ulatuslikele finantstehingutele võimaldavad neil avastada potentsiaalseid rahapesu skeeme ja ebatavalisi tehingumustreid, millest ka RAB-i teavitada. RAB avalikustas krediidiasutustele 2023. aasta kohta tagasiside, milles tuuakse pankadelt laekunud teadete osas probleemkohtadena välja hilinenud teatamist (*late reporting*). Teatamisega hilinemine on oluline probleem, sest nendes juhtumites on uurimisasutuste võimalused operatiivseks sekkumiseks tavaliselt ammendunud (Rahapesu Andmebüroo tagasiside krediidiasutustele, 2024). Hilinenud teatamise asemel oodatakse, et turuosalised teeksid teavitusi reaalajas toimuvatest tehingutest (Rahapesu Andmebüroo, 2024).

Eelnevast tulenevalt on krediidiasutustel oluline roll Eesti rahapesu tõkestamise süsteemis, mistõttu on ka krediidiasutuste esindajate kaasamine käesolevasse magistritöösse põhjendatud. Magistritöö kirjutamise hetkel on Eestis üheksa aktiivset krediidiasutust (Finantsinspektsiooni koduleheküIg, kuupäev puudub), millest kuus on ka makseteenuseid osutavad krediidiasutused. Krediidiasutused on seaduse mõistes kohustatud isikud, kes peavad oma tegevuse osutamise käigus kohaldama oma klientide osas hoolsusmeetmeid ja rahapesu kahtlase tegevuse tuvastamisel teavitama Rahapesu Andmebürood (Riigi Teataja, 2024). Tehisintellekti kasutamine kui ka rahapesu tõkestamine on spetsiifilised valdkonnad, mille osas ei ole igal inimesel kogemusi ega vastavaid teadmisi. Krediidiasutuste esindajate kaasamine valimisse annab võimaluse intervjueerida inimesi, kes omavad magistritöö eesmärgi saavutamiseks vajalikke kogemusi ja teadmisi. Valimi meetodi valikul on seega arvestatud töö eesmärgi ja spetsiifikaga.

Andmete kogumiseks viis autor läbi poolstruktureeritud intervjuud, mis võimaldavad olla paindlik ja küsida intervjuu jooksul esile tekkinud oluliste teemade osas vajadusel täpsustavaid küsimusi (McGrath et al., 2019; Adeoye-Olatunde & Olenik, 2021). Lisaks on selline lähenemisviis sobilik, et mõista hetkel kasutavate süsteemide toimimist ja kuidas saaks neid intervjueeritavate hinnangul täiustada (Adeoye-Olatunde & Olenik, 2021). Intervjuuplaani koostamisel tugines autor teoreetilisest osast selgunud olulistele teemadele ning jagas küsimused kuute suuremasse teemaplokki (vt Tabel 1). Esimesed kaks teemaplokki on sissejuhatavad ning käsitlevad tehisintellekti termini mõistmist ning rahapesu tõkestamises hetkel esinevaid probleemkohti. Kolmas teemaplokk hõlmab tehisintellektiga seotud tugevusi ning selle lahenduste potentsiaalseid rakendamiskohti rahapesu tõkestamise protsessides. Lisaks kuuluvad sellesse plokki asutuse spetsiifilised küsimused, kuid tundlikust valdkonnast tingituna jätis töö autor nendele küsimustele vastamise vabatahtlikuks. Neljandas teemaplokis käsitleb autor tehisintellekti rakendamisega seotud probleemkohti ja väljakutseid. Viiendas plokis käsitletakse tehisintellekti ja inimese vahelist seost ning viimasena uurib autor intervjuueritava seisukohti tehisintellekti tulevikuväljavaadetele.

Tabel 1
*Intervjuuplaani teemaplokid ning teoreetilises osas käsitletud tulemused*

| **Teemaplokid** | **Teoreetilised tulemused** | **Autor(id)** |
|---|---|---|
| AI termin ja rakendamise eeldused | Andmekvaliteet ja maht | *Adeyeri, 2024* |
| | Regulatiivsete nõuete täitmine | *Adeyeri, 2024; Hassija et al., 2024* |
| Rahapesu tõkestamise probleemkohad | Piiratud ja sõltuvad süsteemid | *Labib et al., 2020; Chen et al., 2018* |
| | Manuaalsete toimingute rohkus | *Adeyeri, 2024; Kute et al., 2021; Labanca et al., 2022* |
| AI tugevused ja rakendamine | Keeruliste tehingumustrite tuvastamine | *Zhang & Trubey, 2019; Choi et al., 2020; Bakry et al., 2023* |
| | Kahtlaste tehingute ja tegevuste tuvastamine | *Choi et al., 2020; Bakry et al., 2023; Pavlidis, 2023* |
| | Kliendiriski määramine | *Han et al., 2018; Weber et al., 2018* |
| | Kliendiandmete uuendamine | *Chen, Huang & Chen, 2020* |
| | Pettuste tuvastamine | *Han et al., 2018; Weber et al., 2018; Pavlidis, 2023; Adeyeri, 2024* |
| | Erinevatest allikatest pärinevate andmete töötlemine | *Milon, 2024* |
| AI rakendamise probleemkohad | Selgitatavuse probleem | *Angelov et al., 2021; Hassija et al., 2024* |
| | Informatsiooni ja andmete puudumine | *Han et al., 2020; Canhoto, 2021; Alexandre & Balsa, 2023* |
| AI ja inimene | AI on otsustustoeks | *Han et al., 2020* |
| | AI asendab inimest rutiinsete toimingute tegemisel | *Siau & Wang, 2018; Adeyeri, 2024* |
| | Inimesele jääb lõpliku otsuse tegemise roll | *Alexandre & Balsa, 2023* |
| AI tuleviku-väljavaated | Emotsionaalsete võimete lisandumine | *Zhang & Lu, 2021* |
| | Selgitatav AI (XAI) | *Chamola et al., 2023; Hassija et al., 2024* |

Allikas: autori koostatud tabelis toodud autorite põhjal

Töö autor saatis Eesti krediidiasutuste esindajatele ülevaate magistritöö eesmärgist ning kutse intervjuus osalemiseks. Intervjuus osalemisega nõustusid nelja krediidiasutuse esindajad. Neljast krediidiasutusest kaks on makseteenust pakkuvad krediidiasutused. Ühte krediidiasutust esindasid kaks eksperti, mis tähendab, et intervjuudega kaasati viie eksperdi seisukohad. Lisaks viis autor läbi kolm intervjuud rahapesu tõkestamise valdkonnaga kokkupuudet omava valitsusasutuse esindajatega, kes kaasati valimisse krediidiasutuste

väliste, kuid samal alal tegutsevate ekspertidena. Valitsusasutuse esindajatega viis autor läbi kolm intervjuud, millega kaasati nelja eksperdi seisukohad. Seega viis töö autor 15. aprillist kuni 19. aprillini läbi seitse intervjuud, millega kaasati üheksa eksperdi seisukohad. Intervjuus osalesid vastavuskontrolli juhid, AML strateegia grupijuht, andmeteadlane, andmejuht, infotehnoloogia juht ning juhtivanalüütikud. Seega kaasati intervjuudega nii rahapesu tõkestamise kui ka andmeteaduse valdkonna eksperte võimaldades analüüsida ekspertide väljavaateid mõlemast valdkonnast vaadatuna. Intervjuud kestsid 20 minutist kuni 56 minutini ning töö autor kogus kokku 4 tundi ja 24 minutit audiosalvestusi (vt Lisa C). Kõik uurimisse kaasatud asutused ning nende esindajad ehk intervjueeritavad on käesolevas töös esitletud anonüümsetena.

Autor lähtus intervjuude läbi viimisel intervjuuplaanist (vt Lisa B), kuid intervjuu käigus muudeti vajadusel küsimuste järjekorda või kohandati küsimusi, et tagada intervjuude loogiline ja loomulik ülesehitus (Adeoye-Olatunde & Olenik, 2021). Autor kasutas intervjuudes avatud küsimusi ning ei laskunud asutustes kasutusel olevatesse protsessidesse, kuna asutuste turvameetmeid puudutavad protsessid on konfidentsiaalsed. Asutused ei avalikusta rahapesu tõkestamiseks kasutusel olevaid meetodeid, sest oma süsteemi üksikasjalikul avaldamisel võivad konkurendid sarnaseid meetodeid kasutusele võtta või tuvastada nendes puudusi. Lisaks suurendab sellekohaste andmete väljastamine haavatavust rünnakutele ning kurjategijad võivad sellekohast teadmist süsteemidest mööda hiilimiseks ära kasutada.

Läbiviidud intervjuude edasiseks analüüsimiseks transkribeeriti audiosalvestused koheselt pärast intervjuud TalTechi helitöötluse tehnoloogiaga tekstifailideks (Olev & Alumäe, 2022). Töö autor kontrollis kõikide intervjuude transkriptsioonide kvaliteeti kuulates audiosalvestused ise üle ning tehes tekstifailides parandused. Intervjuude uuesti ja korduv kuulamine võimaldab kogutud andmeid paremini mõista, mis on edasise andmeanalüüsi üheks oluliseks eelduseks. Lisaks võimaldab intervjuudele koheselt järgnev transkriptsioonide analüüs jätta aega leitud tulemuste ja kategooriate mõistmiseks, et hiljem teha teadlikum analüüs (McGrath et al., 2019). Kokku sai autor 69 lk transkriptsioone (stiil *Times New Roman*, suurus 12 pt ja reavahe 1,5). Töösse terviklikke transkriptsioone ei lisata, et mitte avaldada asutuste tundlikku informatsiooni.

Autor kodeeris transkriptsioonides oleva informatsiooni kasutades kvalitatiivse andmeanalüüsi tarkvara NVivo. Autor kodeeris saadud andmeid kolmel erineval korral, et

saada võimalikult täpne tulemus. Esimesel korral kodeeris autor transkriptsioonidest olulisemad tulemused. Teisel korral kodeeris autor andmed uuesti ning lisas tekkinud koodid kategooriatesse. Kolmandal korral viis autor kodeerimise uuesti läbi, koondas kattuvad koodid ja täpsustas kategooriaid. Edasisel analüüsimisel kasutatud kategooriad ja koodid on toodud Lisas D.

### 2.2. Tehisintellekti kasutamise väljavaadete analüüs

Intervjuudest saadud andmete kodeerimisel moodustas autor viis suuremat teemaplokki, mida käesolevas alapeatükis analüüsib ning võrdleb teoreetilise osa kirjeldatud seisukohtadega. Autor analüüsib tehisintellekti kasutamiseks vajalikke eelduseid, tehisintellekti tugevusi, kasutamise võimalusi, kasutamisega seotud väljakutseid ning tehisintellekti ja inimese vahelist seost rahapesu tõkestamisel.

Intervjuude tulemusena selgus, et efektiivse rahapesu tõkestamise süsteemi loomise aluseks on asutuse ärimudelist tulenevate rahapesu riskidega arvestamine. Ka teoreetilisest osast tuleneb, et riskihindamine on efektiivse rahapesu tõkestamise süsteemi loomise aluseks ehk asutus peab mõistma, millisel viisil on asutuse pakutavaid teenuseid võimalik rahapesuks kasutada (Lowe, 2017). Makseteenuseid mittepakkuvate krediidiasutuste esindajate hinnangul on nende pakutavate teenuste puhul rahapesuga seotud riskid madalad, mistõttu ei näe nad praegusel hetkel enda asutustes vajadust tehisintellekti kasutamiseks rahapesu tõkestamisel ega ressursse sellesse valdkonda suunata. Intervjueeritav 1 sõnul on rahapesu risk kõrgem finantstehinguid, sealhulgas piiriüleseid makseteenuseid, osutavates krediidiasutustes ja krüptovaldkonnas. Ka Rahapesu Andmebüroo toob enda 2023. aasta kohta avaldatud aastaraamatus välja, et keskmisest kõrgema ohuga ja kõige haavatavamad sektorid on Eestis krediidiasutused ja virtuaalvääringu teenuse pakkujad olles seotud Eestis asuvate kontode või rahakottidega (Rahapesu Andmebüroo, 2024).

„*Meie juures ei saa näiteks arvelduskontosid avada, tavapäraseid tehinguid ei saa teha ... ja selle tõttu on meie rahapesu tõkestamise nii-öelda raamistik ka fokusseeritud nendele riskidele, mis meil olemas on. Need riskid on oluliselt madalamad, selle tõttu ei ole meil täna olnud vaja ka nii ... palju ressurssi panna sellele poolele, et masinõpet seal tutvustada*.“ (Intervjueeritav 1)

Intervjueeritavad tõid välja, et tehisintellekti kasutamisel tuleb arvestada ka tehisintellektist endast tulenevate riskidega. Oluline on mõista tehisintellekti toimimist ehk aru saada, millisel viisil masin andmeid töötleb ja otsuseni jõuab. Ka Euroopa Liidu tehisintellekti käsitlev õigusakt klassifitseerib tehisintellekti lahendused riskitaseme järgi, mis tähendab, et kõrgema riskiga tehisintellekti lahenduste kasutamisel on ka rangemad piirangud (Euroopa Nõukogu koduleheküg, 2024).

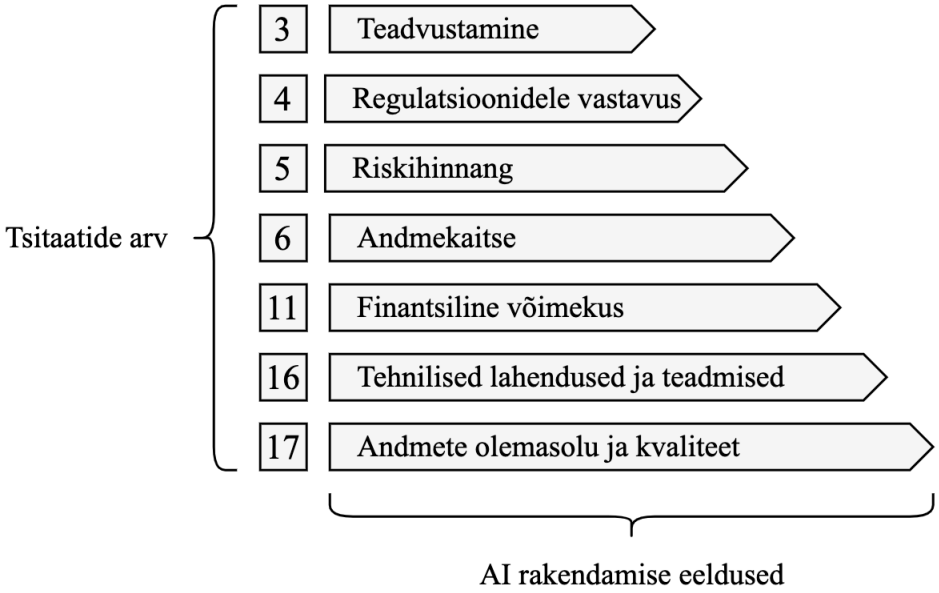
Lisaks kaasnevate riskide hindamisele tuleb tehisintellekti rakendamisel arvestada organisatsioonis olemasolevate süsteemidega. Intervjueeritav 9 tõi välja, et inimesed on küll tehisintellekti lahendustest järjest teadlikumad ning mõistavad ka nende kasutamise vajadust, kuid turul ei ole asutuse põhisüsteemidega sobituvaid lahendusi. Ka Intervjueeritav 2, kes on tehisintellekti mitte rakendava krediidiasutuse esindaja, rõhutas, et tehisintellekti lahendusi pakkuva välise partneri kaasamine oleks asutusele lisakulu- ja koormus. Lisaks kallitele lahendustele tuleks asutuses teha arendusi, et uus süsteem olemasolevate süsteemidega ühildada ning kontrolle, et omada väga head ülevaadet välise pakkuja tegevusest. Krediidiasutused käsitlevad pangasaladusega kaetud isikuandmeid ning ka pankade metoodikad on salajased, mistõttu on välise osapoole kaasamise väga keeruline.

Eelnevatest piirangutest lähtuvalt on võetud suund, et iseseisvalt ja vastavalt võimetele uusi lahendusi arendada. See tähendab, et kaasatakse spetsialiste, et asutusesiseselt uusi lahendusi pangasüsteemist lähtuvalt arendada. Uute süsteemide arendamiseks on oluline erinevate võimaluste teadvustamine, mis aitab mõista, kuidas erinevad tehisintellekti lahendused saaksid aidata rahapesuga seonduvaid riske maandada ja asutuse süsteeme efektiivsemaks muuta. Rahapesu tõkestamine ja tehisintellekti rakendamine on olemuselt väga spetsiifilised ja erinevad valdkonnad, mistõttu on hea mudeli loomiseks vaja nii teoreetilisi kui ka praktilisi teadmisi mõlemast valdkonnast. Intervjueeritav 9 tõi välja, et selle saavutamiseks tuleks süsteemi arendamisse kaasata inimesi, kes tunneksid mõlemat valdkonda ehk nii rahapesu tõkestamise valdkonna eksperte kui ka andmeteadlasi, et tekiks diskusiooni võimalus ning oleks täidetud eeldus efektiivse lahenduse loomiseks.

Tehisintellekti alla kuuluva masinõppe meetodite kasutamiseks on asutusel vaja väga palju ja hea kvaliteediga andmeid, mille põhjal oleks masinal võimalik õppida. Ka teoreetilisest osast nähtub, et tehisintellekti rakendamise kõige olulisemad eeldused on andmete kvaliteet ja maht, sest ebapiisavatest andmetest võivad tekkida ebatäpsed tulemused mõjutades seeläbi lahenduste toimise efektiivsust (Adeyeri, 2024). Eeldusel, et asutusel on

olemas piisavalt kvaliteetseid andmeid, siis on intervjueeritavate sõnul andmete haldamiseks ja töötlemiseks vaja ka tehnilisi lahendusi ja võimekust.

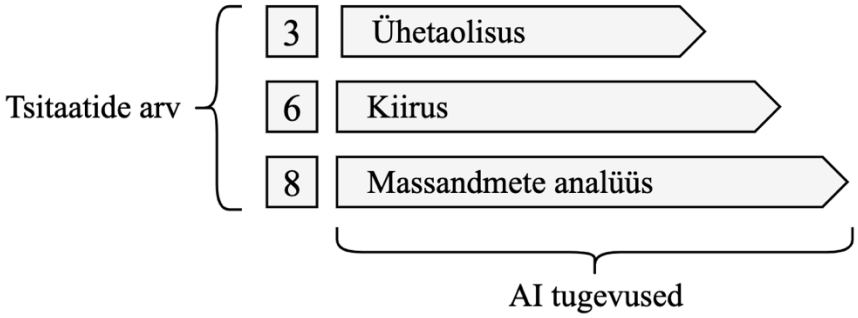
Intervjueeritavad tõid tehisintellekti rakendamise üheks oluliseks eeltingimuseks välja finantsilise valmisoleku ja võimekuse. Krediidiasutuste rahapesu tõkestamise üksused ei too pangale otsest tulu, vaid aitavad tagada turvalisema finantskeskkonna. Sellest lähtuvalt arendab iga asutus oma rahapesu tõkestamise süsteeme vastavalt oma ressurssidele, võimekusele ja valmisolekule, järgides seejuures, et kasutusele võetavad lahendused oleksid ning äriliselt mõistlikud ja regulatsioonidele vastavad.




*Joonis 6*. Intervjuudest eraldatud koodid ja tsitaatide arvud tehisintellekti rakendamiseks vajalike eelduste kohta
Allikas: autori koostatud

Sarnaselt teoreetilisele osale tõid intervjueeritavad välja, et tehisintellekti üks kõige suuremaid eeliseid inimese ees on massandmete, sealhulgas erinevatest allikatest pärineva informatsiooni töötlemise võimekus (Pavlidis, 2023; Adeyeri, 2024; Milon, 2024). Tehisintellekti lahendused suudavad inimesest palju tõhusamalt analüüsida suuri andmemasse ja hallata laialt erinevaid andmepunkte. Nendest tugevustest lähtudes on tehisintellektil oluline roll tervikpildi haldamisel ning mustrite tuvastamisel. Lisaks massandmete töötlemise võimele on tehisintellekti eeliseks inimese ees ka andmete töötlemise kiirus. Tehnilised lahendused suudavad suuri andmemahte ja erinevaid andmepunke töödelda palju kiiremini kui inimesed, mis võimaldab kiiremate ja täpsemate otsuste tegemist. Intervjueeritavad tõid

tehisintellekti tugevuseks välja ka hindamise ühetaolisust. Inimene võib jätta mõned detailid tähelepanuta, sõltuvalt kogemusest, väsimusest ja muudest teguritest. Hästi õpetatud masin ei tohiks teha tähelepanematuse vigu, sest masinad põhinevad andmetel ja algoritmidel ning ei väsi ega sõltu emotsionaalsetest või füüsilistest teguritest.




*Joonis 7*. Intervjuudest eraldatud koodid ja tsitaatide arvud tehisintellekti tugevuste kohta
Allikas: autori koostatud

Tehisintellekti võime töödelda suures mahus andmeid ning teha seda kiiresti ja ühetaoliselt, annab sellele märkimisväärse eelise inimese ees, eriti olukordades, kus kiirus ja täpsus on olulise tähtsusega. Tehisintellekti tugevusi arvestades näevad intervjueeritavad, et tehisintellektil on suur potentsiaal tööprotsesside automatiseerimisel ning selgelt määratletud ajamahukate ja mehaaniliste tööde tegemisel. Näiteks võimaldavad tehisintellekti lahenduste alla kuuluvad keelemudelid leida dokumentidest kiiresti vajaliku informatsiooni, lihtsustades oluliselt varasemalt inimese poolt tehtud manuaalset tööd, kiirendades analüüsiprotsessi ja vähendades vigade tekkimise riski. Lisaks võimaldab korduvatest ja aeganõudvatest ülesannetest vabanemine inimesel keskenduda loovamatele tööülesannetele, mille lahendamiseks ei ole tehisintellekti lahendused võimelised.

„*Miks veel nagu häirib mind see kui inimene peab tegelema sellise mehhaanilise tööga, et see tähendab seda, et sa võtad ära inimeselt selle aja kui ta tegelikult saaks tegeleda selle loova poolega, sellise nagu uue teadmise tekitamisega, just sellesama fantaasia poolega.*“ (Intervjueeritav 9)

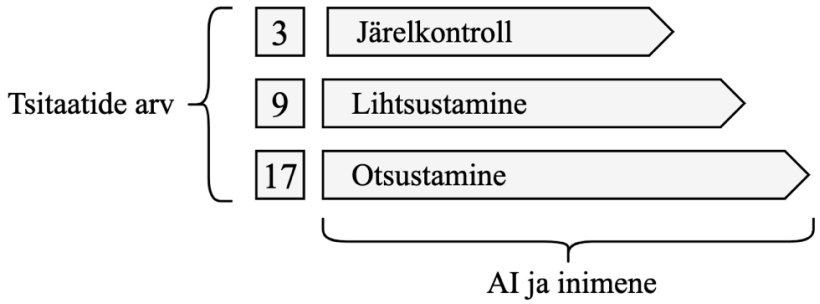
Ka teoreetilisest osast tuleneb, et tänu tehisintellekti võimele analüüsida kiiresti ja suures mahus andmeid on sellel potentsiaali teha inimesele info analüüsimine lihtsamaks, olla oluline kliendiriski määramisel, kliendi mõistmisel, võimaliku pettuse tuvastamisel (Han et

al., 2018; Weber et al., 2018; Pavlidis, 2023) ja kliendiandmete uuendamisel (Chen et al., 2020). Tehisintelletki lahendused aitavad vähendada inimese töökoormust (Han et al., 2020), lihtsustada ja kiirendada uurimisprotsessi ning pakkuda inimesele vajalikku teavet lõpliku otsuse tegemise (Han et al., 2020).

Intervjueeritavad rõhutasid, et tehisintellekti kasutamisel peab inimesele jääma otsuse tegemise roll. Tehisintellekt võib anda soovitusi ja indikatsioone ehk olla otsustustoeks, aga masin ei tohi inimese eest otsustada, sest rahapesu tõkestamises on ka inimõigusi riivavaid protsesse. Traditsioonilised pangad on elutähtsa teenuse osutajad ning tänapäeval kuuluvad pangateenused sisuliselt põhivajaduste hulka, sest ilma pangakontota on inimesel raske, kui mitte võimatu, teha paljusid eluks vajalikke toiminguid (Riigikohtu kodulehekülg, 2023). Pangad võivad rahapesu kahtluse korral makse tegemisega viivitada, makse tegemisest keelduda, konto sulgeda või kliendisuhte lõpetada ning selliste otsuste tegemise võimekus peab olema inimesel. Ka teoreetilisest osast tuleneb, et rahapesu tõkestamise protsess vajab kindlasti inimese osalust (Alexandre & Balsa, 2023), kellele peab jääma lõpliku otsuste tegemise roll (Canhoto, 2021).

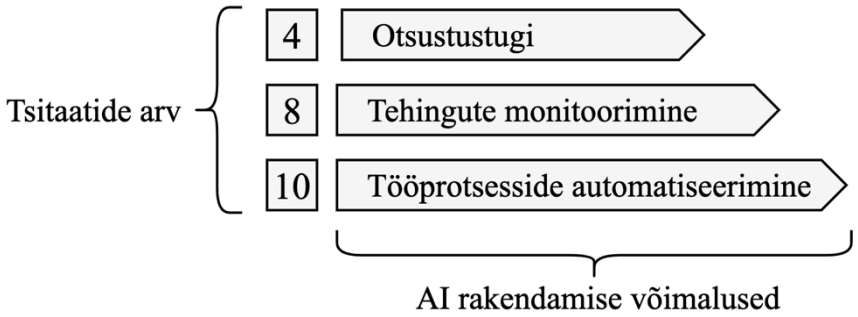
„ *...otsuste tegemise võimekus peaks selle inimese poolel olema. Küll aga võiks selle juures tehisintellekti võime olla anda sellele inimesele võimalikult häid soovitusi ja võimalikult häid selgitusi*.“ (Intervjueeritav 1)

Lisaks eelnevale tõid intervjueeritavad välja, et inimesele jääb oluline roll järelkontrollides. Intervjuueritav 7 tõi välja, et järelkontrollid on muuhulgas olulised valepositiivsete hoiatuste arvu tuvastamiseks. Inimese tagasiside on seega vajalik, et olemasolevad puudused tuvastada ning süsteem vastavalt sellele arendada.




*Joonis 8.* Intervjuudest eraldatud koodid tehisintellekti ja inimese vahelise seoses kohta
Allikas: autori koostatud

Lisaks tehisintellekti potentsiaalile tööprotsesside automatiseerimisele ning otsustustoe pakkumisele tõid intervjueeritavad esile, et tehisintellektil on massandmete töötlemise võimekusest tulenevalt potentsiaal tuvastada finantstehingute monitoorimisel rahapesu kahtlusele viitavaid tehinguid. Ka teoreetilisest osast tuleneb, et tehisintellekti seostatakse kõige enam masinõppe ja selle alla liigituva süvaõppe meetoditega (Du-Harpur et al., 2020) millel on potentsiaali tuvastada tehingute monitoorimisel ebaharilikke ja rahapesu kahtlusele viitavaid tehinguid ning keerukaid tehingumustreid (Choi et al., 2020; Bakry et al., 2023). Tehisintellekti rakendamisel tehingute monitoorimisel tõid intervjueeritavad välja mitmeid puudujääke.




*Joonis 9*. Intervjuudest eraldatud koodid tehisintellekti rakendamise võimalustest
Allikas: autori koostatud

Tehisintellekti kasutamisel tehingute monitoorimisel tõid mitmed intervjueeritavad välja musta kasti probleemi viidates olukordadele, kus tehisintellekti lahendused toimivad keerukate algoritmide või mudelite alusel ning masina otsustusprotsess ei ole inimesele arusaadav. Intervjueeritav 9 tõi välja, et musta kasti, näiteks närvivõrkudel põhinevad mudelid suudavad ennustada väga täpseid tulemusi, kuid sageli on probleem tõlgendamisega, mistõttu ei pruugi inimesele olla täpselt arusaadav kuidas masin tulemuseni jõudis ning millised olid otsustamise alused. Ka teadusallikatele põhinedes peaksid süvanärvivõrkudele põhinevad süvaõppemeetodid andma tehisintellekti meetoditest kõige täpsemad tulemused (Guidotti et al., 2019; Angelov et al., 2021), kuid sellised mudelid põhinevad inimese jaoks arusaamatutel ja keerulistel algoritmidel olles seetõttu selgitatavuse probleemiga (Angelov et al., 2021; Hassija et al., 2024). Ka teadusartiklites nimetatakse sellist probleemi musta kasti probleemi ning seda on korduvalt välja toodud (Labib et al., 2020; Hassija et al., 2024). Musta kasti mudelitele kõrvutatakse valge kaste mudeleid, näiteks ekspertsüsteeme, mis on hästi tõlgendatavad ning nende poolt tehtud otsuseid on lihtsam selgitada, kuid need mudelid

ei paku nii täpseid tulemusi kui musta kasti mudelid (Hassija et al., 2024). Ka Intervjueeritav 4 tõi esile, et on võimalik kasutada lihtsamaid mudeleid, mille kirjeldatavuse tase on parem, kuid need ei suuda pakkuda musta kasti mudelitega sama täpsusega tulemusel ega pruugi sellisel juhul täita oma eesmärki. Seejuures on mudelite selgitatavus rahapesu tõkestamise kui väga tugevalt reguleeritud valdkonna üheks kõige olulisemaks eeltingimuseks tehisintellekti kasutamiseks (Angelov et al., 2021; Adeyeri, 2024). Läbipaistmatute ja arusaamatute mudelite suhtes tekib usaldamatus, eriti kuna rahapesu tõkestamise mõistes on tegemist oluliste ja kriitiliste otsuste tegemisega. Seetõttu on oluline, et rahapesu tõkestamiseks kasutatavad mudelid oleksid mitte ainult täpsed, vaid ka inimese jaoks arusaadavad ja tõlgendatavad.

Krediidiasutuse C esindajad tõid välja, et musta kasti probleemist tingituna kasutatakse rahapesu tõkestamisel traditsiooniliselt reeglitel põhinevaid süsteeme, mis ka teoreetilisele osale põhinedes on rahapesu tõkestamises laialdaselt kasutusel (Choi et al., 2020; Angelov, Soares, Jiang, Arnold, & Atkinson, 2021). Krediidiasutuse C esindajad tunnistavad, et standardse ülesehitusega reeglitele põhinevad süsteemid on inimeressurusile koormavad. Kute et al. (2021), Alhajeri & Alhashem (2023), Bakry et al. (2023) leiavad, et reeglitele põhinevad süsteemid genereerivad palju valepositiivseid hoiatusi, mis kulutavad inimese väärtuslikku aega, mis kulub hoiatuste manuaalsele analüüsimisele. Reeglitele põhinevad süsteemid on laialdaselt kasutusel, sest asutused peavad olema suutelised põhjendama järelevalvele rahapesu tõkestamisel kasutusel olevaid reegleid ning pankade nõuetele vastavust hinnatakse ka selle põhjal, kui hästi on reeglid üles ehitatud. Intervjueeritav 3 tõi esile, et järelevalvejuhendites ja pankadele tehtavates kontrollides määratakse kindlaks valdkonnad, mida asutuste reeglid peavad katma ning järelevalve menetluste käigus hinnatakse kasutusel olevaid reegleid. Järelevalvenõuete täitmiseks peavad asutuse kliendibaasi puudutavad riskid olema kaetud reeglitega ning asutus peab olema võimeline selgitama, milline reegel ja kuidas toimib ning milline on selle lävend. Sellest lähtuvalt saab järelevalve hinnata, kas lävend on piisav. Kuna musta kasti mudelite otsustusprotsess ei ole inimesele läbipaistev, siis ei ole seda võimalik järelevalvele põhjendada ega rahapesu tõkestamise süsteemis kasutada. Musta kasti probleemi lahendamiseks arendatav selgitatava tehisintellekti ehk XAI (Chamola et al., 2023; Hassija et al., 2024) on seega potentsiaalselt sobilik tehisintellekti lahendus, kuna otsustusprotsessi läbipaistvus on vajalik ka regulaatori nõuetele vastamiseks.

„*Me peame ikkagi suutma alati selgitada, kuidas me seadust täidame, ka rahapesu tõkestamise reegleid, kuidas me seda täidame, selle jaoks, kui meil oleks nüüd tehisintellektil põhinev mingi otsustusmootor, siis me peame ka suutma ära selgitada nagu ammendavalt regulaatorile, kuidas see otsustusmootor töötab.“* (Intervjueeritav 1)

Intervjueeritavad tõid esile, et lisaks läbipaistmatuse probleemidele on tehisintellekti kasutamisel tehingute monitoorimisel ka andmete kättesaadavusest tingitud probleeme. Eesti rahapesu tõkestamise süsteem tugineb suuresti rahapesu ja terrorismi rahastamise tõkestamise seaduses välja toodud kohustatud isikutele, kes peavad rahapesukahtlase tegevuse tuvastama ning sellest Rahapesu Andmebüroole teada andma (Riigi Teataja, 2024). Selline lähenemisviis tähendab, et kohustatud isikutel on algandmed, mida tehisintellekti treenimiseks oleks võimalik kasutada. Makseteenuseid osutavatel krediidiasutustel on suures mahus kliente ning nendega seotud finantstehinguid. Seejuures tõid krediidiasutuste esindajad välja, et tehisintellekti rakendamise probleemkohaks on treeningandmestiku vähesus viidates olukorrale, et ka ühe makseteenuseid osutava krediidiasutuse andmestik ei ole tehisintellekti efektiivseks rakendamiseks piisav. Teoreetilisest osast tuleneb, et igal pangal on piiratud võimalus töödelda ainult asutusele teadaolevaid andmeid ja ka need võivad olla puudulikud (Canhoto, 2021; Adeyeri, 2024) Seejuures võivad puudulikest andmetest tekkida ebatäpsed tulemused mõjutades seeläbi lahenduste toimise efektiivsust (Adeyeri, 2024).

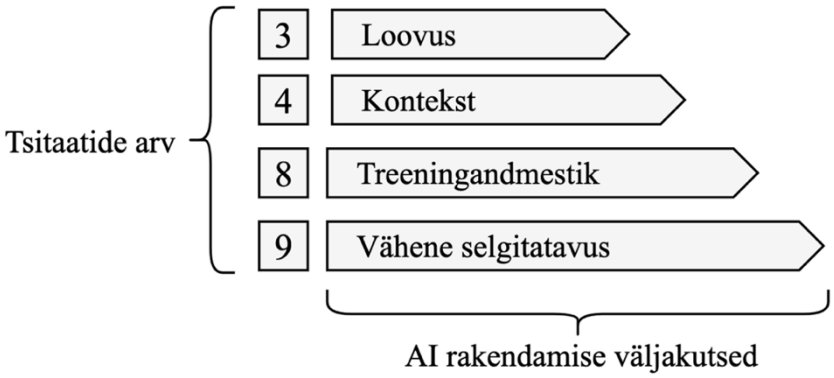
Intervjueeritav 9 tõi esile, et klassikalise juhendatud masinõppe puhul peavad olemas olema nii treeningandmed kui ka soovitud sihtmärgid (*target*), mille järgi andmeid treenida. Siinkohal tõid mitmed intervjueeritavad välja probleemkoha, kus treeningandmed on kohustatud isikutel, valdavalt makseteenuseid osutavate pankadel, kuid sihtmärgid on teada õiguskaitseasutustele ning neid andmeid omavahel ei jagata. Lisaks toodi esile, et teate esitanud asutustele ei anta tagasisidet, kas esitatud teade või tehing ka päriselt rahapesuga seotuks osutuks, et vastavalt sellele informatsioonile asutusesiseid andmeid masinõppeks vajalikult märgendada. Ka teoreetilisest osast tuleneb, et juhendatud masinõppe rakendamiseks on vaja treeningandmestik märgendada, kuid tagasiside ja asutuste omavahelise infovahetuse puudumise tõttu ei ole seda võimalik teha muutes tehisintellekti rakendamise rahapesu tõkestamise süsteemidesse keeruliseks (Zhang & Trubey, 2019; Alexandre & Balsa, 2023; Bakry et al., 2023). Teoreetilisel tasandil oleks vaja andmed omavahel kokku viies luua universiaalne mudel, kuid see eeldab väga tugevat anonüümsuse

taset ning asutuste koostöövalmidust, mida praktikas ka juriidilistest piirangutest tingituna, on keerulina saavutada.

*„ ... ehk sisuliselt anonümiseeriti, krüpteeriti seda siis piisava astmega, et seda usaldatakse. Ja kui keegi suudaks teha sellise süsteemi, miks mitte ka riigi initsiatiivil, kuhu me paneme kõik Eesti krediidiasutuste kahtlased tehingud kokku ..., et mida keegi raporteerinud on ja me suudame sinna juurde panna selle mõõtme, mis RAB on nendega teinud, kas ta on avanud siis mingisuguse toimiku või on edastanud mõnele teisele uurimisasutusele. Ja see ongi see treeningmaterjal, mille pealt siis ehitada selline universaalne mudel ...“* (Intervjueeritav 3)

Käsitletud probleemkohtades tulenevalt tõid intervjueeritavad esile, et tehingute monitoorimisel tuleks võimalikult hea tulemuse saamiseks rakendada erinevaid tehisintellekti meetodite kombinatsioone. Potentsiaalselt sobiv lahendus on kombineerida praeguseid ekspertteadmistele põhinevaid reegleid masinõppe meetoditega, nagu on järeldanud ka Bakry et al. (2023). Reeglitele põhinevt lähenemist on võimalik kasutada lihtsamate riskide tuvastamiseks, samas kui masinõppe meetodid võimaldavad tuvastada keerukamaid ja ka inimesele varasemalt teadmata rahapesule iseloomulikke mustreid. Masinõppega leitud mustreid saavad inimesed üle vaadata ning otsustada, kas selline reegel tuleks lisada ka ekspertsüsteemi. Intervjueeritavad tõid välja, et kuna masinõppe lahendustele iseloomulikud musta kasti mudelid ei ole hästi selgitatavad ning valge kasti mudelite ehk ekspertsüsteemide ennustusjõud on kehvem, siis peaks toimuma mitme mudeli kombineerimine.

Rahapesu tõkestamine ei saa toetuda alati kindlatele reeglitele. Intervjueeritavad tõid esile, et potentsiaalsete rahapesukahtlaste tehingute või seotud isikute tuvastamiseks on olulised ka analüütiku kogemus ja tunnetus ehk inimesele iseloomulikud omadused, mida masinale ei ole käesoleval hetkel võimalik õpetada. Tehisintellektil puudub empaatilisus ja sotsiaalne komponent, mistõttu on rahapesu tõkestamises vajalik ka inimese osalus, et tuvastada seoseid ja teha otsuseid, mis ei ole ainult reeglite järgimise tulemus, vaid hõlmavad ka intuitiivset arusaamist ja kogemustel põhinevat hindamist. Tehisintellekt võib tuvastada mustreid ja seoseid, mida inimsilm ei suuda, kuid inimene suudab masina leitud tulemustele anda parema konteksti.




*Joonis 10*. Intervjuudest eraldatud koodid tehisintellekti rakendamise väljakutsetest
Allikas: autori koostatud

Intervjuueritavate hinnangul on tehisintellekti kasutamine rahapesu tõkestamisel alles algusjärgus, kuid selle roll on kasvamas. Intervjueeritava 3 sõnul võiksid suured rahvusvahelised pangandusvaldkonnas tegutsevad organisatsioonid, kellel on suured andmemahud ja palju töötajaid, olla suunanäitajad, kellelt ka teised asutused õppida saaksid. Kuni ei ole praktikas leitud sobilikku lahendust, mis rahapesu tõkestamisega seotud probleeme võiksid aidata lahendada ning vastaksid samal ajal ka regulaatori nõuetele, ei kiirustata selliste lahenduste rakendamisega. Pangandussektor on konservatiivne ja rahapesu tõkestamine on tugevalt reguleeritud valdkond, mistõttu ei soodusta selle valdkonna raamistik väga kiiret arengut, sest asutustel tuleb vastata järelevalve ootustele ja nõuetele. Intervjuueritava 1 sõnul võiks enamus rahapesu tõkestamise traditsioonilisest raamistikust juhtida tegelikult tehisintellekt ning leiab, et AML protsessides on tehisintellektil lähimate aastate jooksul märkimisväärne roll. Seejuures juhtis Intervjueeritav 9 tähelepanu asjaolule, kus tehisintellekt võimaldab mitmeid protsesse tegelikult lahendada praegusest käsitlusest erinevalt, kuid võib olla on seda keeruline hetkel mõista.

„ *... mõelda, kas asju peab üldse tegema nii, nagu me praegu teeme, et see AI, seda ta võimaldab, et meei pea tegema asju üldse nii, nagu me praegu teeme. Ja aga sellest on juba raske inimesel lahti võtta. Aga ma olen harjunud oma tööd tegema kogu aeg nii ja las see masin teeb lihtsalt minu praegust tööd lihtsamaks. Aga, aga väga ei taheta mõelda selle peale, et äkki teeks üldse kuidagi teistmoodi, masin võimaldab teha hoopis teistmoodi*“ (Intervjueeritav 9)

### 2.3. Järeldused tehisintellekti kasutamise võimalustest ekspertide vaatest

Selgub, et tehisintellekti kasutamise oluliseks eeltingimuseks rahapesu tõkestamisel on asutuse ärimudelist tulenevate rahapesu riskidega hindamine. Juhul kui asutuse pakutavate lahendustega kaasnevad rahapesu riskid on madalad ja neid on võimalik hallata asutuses olemasoleva inimressursiga, siis ei pruugi olla otsest vajadust tehisintellekti lahenduste rakendamiseks. Tehisintellekti lahenduste rakendamine on asutusele märkimisväärne lisakulu- ja koormus ning nõuab nii tehnilist võimekust kui ka teoreetilisi teadmisi, mis võivad ületada väiksemate asutuste finants- ja inimressursside võimekuse ega ole äriliselt otstarbekas sellesse investeerida. Lisaks on oluline arvestada, et rahapesu tõkestamine ei ole otseselt tulu teeniv osa asutuse tegevusest, vaid aitavad maandada riske, täita regulatsioonidele vastavust ja tagada turvalisemat finantskeskkonda. Sellest lähtuvalt arendavad asutused oma rahapesu tõkestamise süsteeme vastavalt olemasolevatele ressurssidele, võimekusele ja keskendudes eelkõige sellele, et kasutusel olevad lahendused oleksid vastavad kehtivatele regulatsioonidele. Seega ei pruugi tehisintellekti lahenduste kasutamine olla vajalik asutustele, millele on iseloomulikud madalad rahapesu riskid, mis on inimteadmistega lihtsasti maandatavad. Asutustel, millel on ärimudelist tulenevalt kõrged rahapesu riskid ning suures mahus andmeid ehk palju kliente ning nendega seotud finantstehinguid, peavad tagama, et olemasolevad lahendused oleksid rahapesu tõkestamiseks piisavad. Võimalusel tuleks kaaluda ka tehisintellekti kasutamist, et tagada efektiivne ja ajakohane rahapesu tõkestamise süsteem. Eestis on keskmisest kõrgema rahapesu ohuga ja kõige haavatavamad sektorid krediidiasutused ja virtuaalvääringu teenuse pakkujad, kellel on suur hulk kliente ning vajadus nendega seotud finantstehinguid monitoorida.

Tehisintellektil on massandmete töötlemise võimekusest tulenevalt potentsiaal tuvastada finantstehingute monitoorimisel rahapesu kahtlusele viitavaid tehinguid. Tehisintellekti seostatakse kõige enam masin- ja süvaõppemeetodietega, millel on potentsiaali tuvastada ebaharilikke ja rahapesule viitavaid tehinguid ning keerulisi tehingumustreid. Hoolimata sellest võimekusest on tehisintellekti rakendamisel tehingute monitoorimisel mitmeid puudujääke. Esiteks on tehingute monitoorimiseks sobilikele tehisintellekti lahendustele iseloomulik musta kasti probleem, mis tähendab, et tehisintellekti lahendused toimivad keerukate algoritmide või mudelite alusel ning masina otsustusprotsess ei ole inimestele arusaadav. Läbipaistmatute ja arusaamatute mudelite suhtes tekib usaldamatus, eriti kuna rahapesu tõkestamise mõistes on tegemist oluliste otsuste tegemisega,

milles on ka inimõigusi riivavaid protsesse. Lisaks ei vasta sellised lahendused järelevalve nõuetele. Seega on mudelite selgitatavus rahapesu tõkestamise kui väga tugevalt reguleeritud valdkonna üheks kõige olulisemaks eeltingimuseks tehisintellekti kasutamiseks.

Eelnevast tulenevalt on traditsioonilised rahapesu tõkestamise süsteemid reeglitele põhinevad lahendused, mille väljundid on inimese jaoks lihtsasti tõlgendatavad ja arusaadavad ning suudavad vastata ka järelevalve nõuetele. Sellised süsteemid suudavad tuvastada vaid üksikuid kahtlaseid tehingud ega ole piisavad keeruliste tehingutemustrite ja uute rahapesu tehnikate tuvastamiseks. Vaatamata tehisintellekti lahenduste potentsiaalile anda praegu kasutatavatest ekspertsüsteemidest paremaid tulemusi, ei ole asutustel selgitatavuse probleemi tõttu võimalik ainult sellistele lahendustele põhineda. Kuna rahapesu mustrid muutuvad ajas pidevalt ning ekspertsüsteemid ei ole suutelised neid tuvastama ning ainult masinõppe lahendusi ei ole võimalik nende läbipaistmatuse tõttu kasutada, siis tuleks tehingute monitoorimisel kasutada kombinatsioone erinevatest tehisintellekti lahendustest.

Efektiivsete rahapesu tõkestamise süsteemide loomiseks on võimalik kombineerida erinevaid masinõppe meetodeid, kuid kõige potentsiaalselt sobilikum lahendus oleks kasutada kombinatsiooni reeglitele ja masinõppele põhinevatest meetoditest. Reeglitepõhise lähenemisega on võimalik tuvastada lihtsamaid rahapesule iseloomulike tehinguid olles samal ajal lihtsasti tõlgendatav ja regulatsioonidele vastav. Juhendamata masinõppe meetodid võimaldavad andmestikust tuvastada keerukamaid ja ka inimesele varasemalt teadmata rahapesule iseloomulikke mustreid. Selliselt saadud informatsiooni on võimalik kasutada uute reeglite välja mõtlemiseks parandades seeläbi reeglitele põhineva rahapesu tõkestamise süsteemi efektiivsust ning jäädes samal ajal ka regulatsioonidele vastavaks. Kuna ekspertsüsteemide tulemused on sageli vähem täpsemad, kuid need on hästi tõlgendatavad ja masinõppe meetodid on vastupidiselt võimekamad, kuid vähese selgitatavusega, siis peaks toimuma mitme mudeli kombineerimine.

Lisaks juhendamata masinõppele on tehingute monitoorimisel potentsiaalselt sobilik ka juhendatud masinõpe, mis vajab lisaks treeningandmestikule ka väljundväärtuseid õppides nende andmete omavahelist seost, et tuvastada rahapesu kahtlusega tehingud. Väljundväärtuste olemasolu tähendab, et andmestikus on vaja märgendada rahapesukahtlased tehingud. Andmestiku märgendamiseks vajavad asutused tagasisidet, kas nende poolt raporteeritud tehing osutus või ei osutunud kahtlaseks, kuid sellist teavet asutuste vaheliselt ei jagata. Tagasiside puudumise tõttu ei saa asutused enda andmestikku ka juhendatud õppe

meetodi kasutamiseks vajalikult märgendada ning muudab üleüldiselt efektiivse rahapesu tõkestamise süsteemi mudeli arendamise keeruliseks, kuna asutused ei saa vajalikku teavet, mis aitaksid parandada nende soorituse kvaliteeti ja muuta süsteeme efektiivsemaks. Lisaks tagasiside puudumisel on tehisintellekti rakendamise üheks piiranguks treeningandmestiku vähesus. Sageli on ühel asutusel ainult piiratud koguses teave enda klientide tegevuse kohta ning puudulikest andmetest võivad tekkida ebatäpsed tulemused, mis mõjutab ka süsteemi toimimise efektiivsust.

Seega on tehisintellekti alla kuuluvate masinõppe meetodite efektiivseks kasutamiseks tehingute monitoorimisel vaja suures koguses kvaliteetseid andmeid ning rahapesu kahtlase tehingu tuvastamiseks ka treeningandmestik vastavalt märgendada. Kuna igas makseteenuseid osutavas krediidiasutuses on üldjuhul filtreeritud teave oma kliendi tegevusest ning tehingute märgendamiseks vajalik teave on ainult õiguskaitseasutusel, siis on efektiivse rahapesu tõkestamise süsteemi arendamine märkimisväärselt keeruline. Teoreetilisel tasandil oleks vaja kõik need andmed omavahel kokku viia ning töötada välja universiaalne mudel, kus oleksid nii kõik erasektorile teadaolevad tehingud kui ka avalikus sektorile teadaolevad sihtmärgid ehk andmestiku märgistamiseks vajalik teave. Selline mudel eeldab väga tugevat anonüümsuse taset ning asutuste omavahelise koostöö valmisolekut, mida praktikas andmekaitsest tulenevatest piirangutest tingituna ei ole lihtne saavutada. Seni kuni selliselt toimimine ei ole võimalik, siis arendab iga asutus võimaluste piires ise oma rahapesu tõkestamise süsteeme, järgides seejuures, et kasutusele võetavad lahendused oleksid ning äriliselt mõistlikud ja regulatsioonidele vastavad.

Lisaks tehingute monitoorimisele on tehisintellektil suur potentsiaal automatiseerida rahapesu tõkestamise protsesse, näiteks kliendiriski määramist ja kliendiandmete uuendamist. Tehisintellekti lahendused suudavad ühetaoliselt ja inimesest kiiremini analüüsida massandmeid, hallata väga laialt erinevaid andmepunkte ning tuvastada mustreid seal, kus inimene ei pruugi olla võimeline. Tehisintellektil on seega kogu tervikpildi haldamisel oluline roll, sest suudab inimesest paremini kogu andmemassiga toime tulla ning luua kliendist terviklik ülevaade. Lisaks mitmete erinevate andmepunktide töötlemise võimele on tehisintellekti eelis inimese ees ka see, et masin suudab andmemahte töödelda palju kiiremini. Tehisintellekti alla kuuluvate keelemudelitel on võimekus analüüsida erinevatest andmestikest kiiresti vajalikku informatsiooni kiirendades selliselt analüüsiprotsessi, lihtsustades oluliselt varasemalt inimese poolt tehtud manuaalset tööd ning vähendades

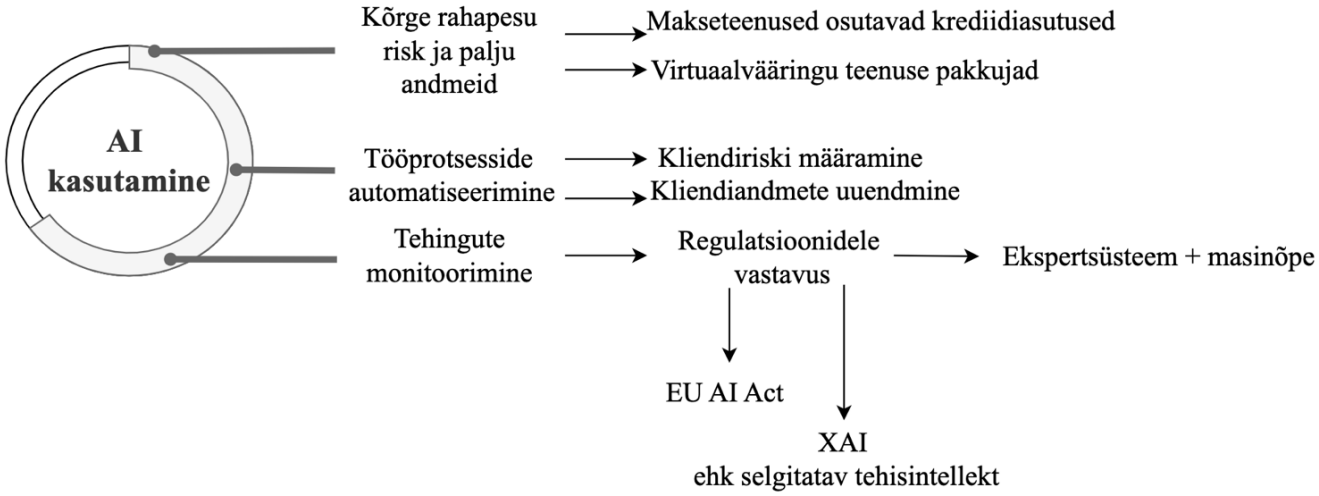
vigade tekkimise riski. Lisaks jätab korduvatest ja aeganõudvatest ülesannetest vabanemine inimesel rohkem aega, et keskenduda loovatele ülesannetele, mille lahendamiseks ei ole tehisintellekt veel võimeline. Tehisintellektil on seega potentsiaali parandada ka Rahapesu Andmebüroole esitatavate teadete kvaliteeti ning vähendada hilinenud teatamist, mis Rahapesu Andmebüroo krediidiasutustele tehtud tagasisidearuannetes on probleemkohana välja toodud. Tehisintellekti võimekus hallata suures koguses ja kiiresti erinevaid andmeid võimaldaksid asutustel edastada informatsiooni kiiremini Rahapesu Andmebüroole muutes kogu rahapesu tõkestamise süsteemi efektiivsemaks. See tähendab, et RAB-ile peaks jõudma kiiremini laiema haardega teave, millel oleks ka selletõttu suurem menetlusperspektiiv.

Olenemata vastuvõetud automatiseerimise tasemest vajab rahapesu tõkestamise protsess kindlasti ka inimese osalust. Inimese eelis tehisintellekti lahenduste ees on kindlasti empaatilisus ja sotsiaalne komponent. Rahapesu tõkestamises on inimõigusi riivavaid protsesse, mistõttu võib tehisintellekt anda inimesele soovitusi ja indikatsioone, aga inimese osalus peab kindlasti alles jääma, sest eksperdi hinnang, intuitsioon ja sotsiaalne kontekst on ainult inimesele iseloomulikud omadused, mis on vajalikud lõpliku otsuse tegemisel.

Tehisintellekti kasutamine on rahapesu tõkestamises alles algusjärgus, kuna valdkond on tugevalt reguleeritud ja uued lahendused peavad vastama rangetele nõuetele. Sellest hoolimata on tehisintellektil suur potentsiaal muuta rahapesu tõkestamise süsteeme efektiivsemaks. Käesoleval hetkel on lahenduste kasutamisel, eelkõige finantstehingute monitoorimisel, kõige suurem takistus vähene selgitatavus, mistõttu on tehisintellekt osas tekkinud usaldamatus. Kiiresti on arenemas XAI ehk selgitatava tehisintellekti valdkond, mille eesmärgiks on arendada tehisintellekti süsteeme, mis võimaldab lisaks heale tulemusele pakkuda ka otsuste ja tegevuste kohta selgitusi. Selliste lahenduste otustusprotsess on läbipaistev, inimesele mõistetav ning regulaatori ootustele vastav ning suudaks viia tehisintellekti inimesele vastuvõetavamaks ja usaldusväärsemaks. Lisaks sellele kiideti alles hiljuti heaks Euroopa Liidus esimene tehisintellekti kasutamist reguleeriv õiguslik alus, mis võiks eeldatavasti samuti suurendada usaldust tehisintellekti kasutamise vastu ning tuua kaasa tehisintellekti laialdasema kasutuse ka rahapesu tõkestamises.

Kokkuvõtvalt nõuab tehisintellekti kasutamine rahapesu tõkestamisel ärimudelist tulenevate riskide hoolikat hindamist, sest kõrgema rahapesu riskiga ja suure andmemahuga asutustele võib tehisintellekti kasutamine kõige sobilikumaks osutuda. Tehisintellektil on suur potentsiaal automatiseerida rahapesu tõkestamise süsteemis olevaid protsesse, näiteks

määrata automaatselt kliendiriski või uuendada kliendiga seotud andmeid. Lisaks sellele on tehisintellektil suur märkimisväärne võimekus tehingute monitoorimisel ning rahapesukahtlasrte tehingute tuvastamisel. Siiski tuleb hinnata nende lahenduste vastavust regulatsioonidele, sest kõige paremaid tulemusi annavad masinõppe lahendustel, millel on sageli selgitatavuse probleem. Tehingute monitoorimisel on soovitatav kasutada masinõppe lahendusi kombinatsioonis reeglite põhise süsteemiga, et tagada regulatsioonidele vastavus ning mõista masina otsustusprotsessi. XAI ehk selgitatava tehisintellekti arengul ja Euroopa Liidu tasandil vastu võetavatel regulatsioonidel on oluline roll tehisintellekti laiemal kasutuselevõtul rahapesu tõkestamisel, suurendades tehisintellekti lahenduste läbipaistvust ja usaldusväärsust (vt Joonis 11).




*Joonis 11*. Järeldused tehisintellekti kasutamise võimalustest rahapesu tõkestamisel
Allikas: autori koostatud

## Kokkuvõte

Rahapesu on olulise mõjuga kuritegevus, mille tõkestamine on muutunud järjest keerulisemaks. Seejuures on tehnoloogia kiire arenguga muutunud oluliseks tehisintellekti roll rahapesu vastases võitluses. Teadusallikates käsitletakse erinevate tehisintellekti lahenduste ja nende kombinatsioonide rakendamise võimalusi rahapesu tõkestamisel, kuid vähem on uuritud selliste lahenduste kasutamist asutuste rahapesu tõkestamise süsteemides. Sellest lähtuvalt võttis töö autor eesmärgiks selgitada välja rahapesu tõkestamise valdkonnas tegutsevate ekspertide väljavaated tehisintellekti kasutamisega seotud võimalustest ja väljakutsetest asutuste rahapesu tõkestamise süsteemides.

Teoreetiliselt käsitlusest selgus, et rahapesu on keeruline protsess, mille vastu võitlemise meetmeid on aastatega oluliselt täiustatud. Rahapesu tõkestamiseks tuleb asutustel kohaldada hoolsusmeetmeid, et maandada tegevusega kaasnevaid rahapesuga seonduvaid riske. Üldistatult põhinevad rahapesu tõkestamise süsteemid kliendi tundmise põhimõttele ning finantstehingute monitoorimisele. Finantstehingute analüüsimiseks on traditsiooniliselt kasutusel reeglitel põhinevad süsteemid, mis on inimese jaoks lihtsasti mõistetavad, kuid ei suuda tuvastada uusi rahapesule iseloomulikke meetodeid ega keerulisi tehingumustreid. Eesti krediidiasutustele viimastel aastatel tehtud suuremahulised trahvid viitavad rahapesu tõkestamise süsteemis ka olulistele puudujääkidele. Tehisintellekti lahendustel on võime kiiresti analüüsida suuri andmemasse, mis teoreetilises käsitluses tähendab, et lahenduste kasutamisel suudaksid asutused kiiremini ning põhjalikumalt tuvastada potentsiaalseid rahapesu riske. Lisaks sellele on masin- ja süvaõppemeetoditel võimekus tuvastada rahapesule iseloomulikke mustreid, milleks reeglitele põhinevad süsteemid ei ole võimelised.

Magistritöö empiirilises osas viis autor läbi intervjuud Eesti krediidiasutuste ning valitsusasutuse esindajatega, et selgitada välja ekspertide väljavaateid tehisintellekti kasutamisel rahapesu tõkestamisel. Ilmneb, et reeglitele põhinevad süsteemid on praegune standard, kuivõrd on need järelevalvele lihtsasti põhjendatavad. Tehisintellekti alla kuuluvate masin- ja süvaõppemeetodite probleemkohaks on vähene selgitatavus, mistõttu on nende kasutamine rangelt reguleeritud rahapesu tõkestamise süsteemides komplitseeritud. Lisaks mõistmise keerukusele on masinõppe lahenduste kasutamine andmete puudulikkusest tingituna piiratud. Esiteks on probleemkohaks treeningandmestiku vähesus, sest iga asutus saab arendada süsteeme oma asutusest lähtuvalt, kuid üldjuhul on need puudulikud ega ole sobilikud efektiivsete lahenduste arendamiseks. Lisaks oleks treeningandmestikku vajalik

märgendada ehk teada reaalselt rahapesule iseloomulikku tehinguid, kuid sellekohast tagasisidet asutustele ei jagata, mistõttu ei ole võimalik rahapesu tõkestamise süsteeme sellele vastavalt arendada.

Kuigi tehingute monitoorimisel on tehisintellekti lahenduste kasutamine piiratud, siis reeglitele põhinevas süsteemi efektiivsema lahenduse loomiseks on võimalik kasutada kombinatsiooni reeglitele ja masinõppele põhinevatest meetoditest. Selliselt on lisaks lihtsamatele rahapesule iseloomulikele tehingutele võimalus tehisintellektiga tuvastada tehingumustreid, mida inimene varem tuvastanud ei ole ning kasutada saadud informatsiooni uute reeglite loomiseks. Tehisintellekti on potentsiaalselt sobilik ka rahapesu tõkestamises olevate lihtsamate tööprotsesside automatiseerimiseks. Tehisintellekti alla kuuluvad lahendused võimaldavad erinevatest andmestikest analüüsida inimesest rohkem ja kiiremini informatsiooni ning kiirendada seeläbi analüüsiprotsessi ja vähendada inimese poolt tehtud manuaalset tööd jättes inimesele rohkem aega keskenduda ülesannetele, mille lahendamiseks tehnoloogilised lahendused võimelised ei ole. Rahapesu tõkestamise protsess vajab kindlasti ka inimese osalust, sest tehisintellektil puudub sotsiaalne komponent, mis on lõpliku otsuse tegemisel kriitilise tähtsusega. Sellest lähtuvalt saab tehisintellekt pakkuda inimesele otsustustuge ning aidata manuaalsete ja rutiinsete toimingute tegemisel.

Magistritöö tulemuste kinnitamiseks, ümber lükkamiseks või edasi arendamiseks on võimalik analüüsida ka teiste rahapesu tõkestamise valdkonnas tegutsevate asutuste rahapesu tõkestamise protsesse ja hinnate tehisintellekti lahenduste kasutamise võimlust nende süsteemides. Lisaks on võimalik viia sarnane töö läbi uuesti lähimate aastate jooksul, kuna regulatsioonide vastuvõtmine ning vajalike lahenduste arendamine on praegusel hetkel alles algusjärgus.

**Viidatud allikad**

1. Adeoye-Olatunde, O. A., & Olenik, N. L. (2021). Research and scholarly methods: Semi-structured interviews. *JACCP: JOURNAL OF THE AMERICAN COLLEGE OF CLINICAL PHARMACY*, *4*(10), 1358–1367. https://doi.org/10.1002/jac5.1441
2. Adeyeri, T. B. (2024). Enhancing Financial Analysis Through Artificial Intelligence: A Comprehensive Review. *Journal of Science & Technology*, *5*(2), 102–120.
3. Alexandre, C. R., & Balsa, J. (2023). Incorporating machine learning and a risk-based strategy in an anti-money laundering multiagent system. *Expert Systems with Applications*, *217*, 119500. https://doi.org/10.1016/j.eswa.2023.119500
4. Alhajeri, R., & Alhashem, A. (2023). Using Artificial Intelligence to Combat Money Laundering. *Intelligent Information Management*, *15*(4), 284–305. https://doi.org/10.4236/iim.2023.154014
5. Alkhalili, M., Qutqut, M. H., & Almasalha, F. (2021). Investigation of Applying Machine Learning for Watch-List Filtering in Anti-Money Laundering. *IEEE Access*, *9*, 18481–18496.
6. Alotibi, J., Almutanni, B., Alsubait, T., Alhakami, H., & Baz, A. (2022). Money Laundering Detection using Machine Learning and Deep Learning. *International Journal of Advanced Computer Science and Applications*, *13*. https://doi.org/10.14569/IJACSA.2022.0131087
7. Alsuwailem, A. A. S., & Saudagar, A. K. J. (2020). Anti-money laundering systems: A systematic literature review. *Journal of Money Laundering Control*, *23*(4), 833–848. https://doi.org/10.1108/JMLC-02-2020-0018
8. Angelov, P. P., Soares, E. A., Jiang, R., Arnold, N. I., & Atkinson, P. M. (2021). Explainable artificial intelligence: An analytical review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *11*(5), e1424.
9. Baader, G., & Krcmar, H. (2018). Reducing false positives in fraud detection: Combining the red flag approach with process mining. *International Journal of Accounting Information Systems*, *31*, 1–16. https://doi.org/10.1016/j.accinf.2018.03.004
10. Bakry, A., Alsharkawy, A., Farag, M., & Raslan, K. (2023). Automatic suppression of false positive alerts in anti-money laundering systems using machine learning. *The Journal of Supercomputing*, *80*, 1–21. https://doi.org/10.1007/s11227-023-05708-z

11. (Bodescu) Cotoc, C.-N., Nițu, M., Șcheau, M. C., & Cozma, A.-C. (2021). Efficiency of Money Laundering Countermeasures: Case Studies from European Union Member States. *Risks*, *9*(6), 120. https://doi.org/10.3390/risks9060120
12. Borghezio, M. (2013). Money laundering, banks and finance. *Euroopa Parlament*. Kasutatud 02.04.2024, https://www.europarl.europa.eu/meetdocs/2009_2014/documents/crim/dv/borghezio_ml_/borghezio_ml_en.pdf
13. Canhoto, A. I. (2021). Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. *Journal of Business Research*, *131*, 441–452. https://doi.org/10.1016/j.jbusres.2020.10.012
14. Cassella, S. D. (2018). Toward a new model of money laundering: Is the "placement, layering, integration" model obsolete? *Journal of Money Laundering Control*, *21*(4), 494–497. https://doi.org/10.1108/JMLC-09-2017-0045
15. Chamola, V., Hassija, V., Sulthana, A. R., Ghosh, D., Dhingra, D., & Sikdar, B. (2023). A Review of Trustworthy and Explainable Artificial Intelligence (XAI). *IEEE Access*, *11*, 78994–79015. https://doi.org/10.1109/ACCESS.2023.3294569
16. Chen, C.-C., Huang, H.-H., & Chen, H.-H. (2020). *NLP in FinTech Applications: Past, Present and Future*. arXiv. https://doi.org/10.48550/arXiv.2005.01320
17. Chen, Z., Van Khoa, L. D., Teoh, E. N., Nazir, A., Karuppiah, E. K., & Lam, K. S. (2018). Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: A review. *Knowledge and Information Systems*, *57*(2), 245–285. https://doi.org/10.1007/s10115-017-1144-z
18. Choi, R. Y., Coyner, A. S., Kalpathy-Cramer, J., Chiang, M. F., & Campbell, J. P. (2020). Introduction to Machine Learning, Neural Networks, and Deep Learning. *Translational Vision Science & Technology*, *9*(2), 14. Kasutatud 05.04.2024, https://tvst.arvojournals.org/article.aspx?articleid=2762344
19. Clark, N. (1995). The Impact of Recent Money Laundering Legislation on Financial Intermediaries. *Journal of Financial Crime*, *3*(2), 131–147. https://doi.org/10.1108/eb025694
20. Du-Harpur, X., Watt, F. M., Luscombe, N. M., & Lynch, M. D. (2020). What is AI? Applications of artificial intelligence to dermatology. *British Journal of Dermatology*, *183*(3), 423–430. https://doi.org/10.1111/bjd.18880

21. EUR-Lex. (10.06.1991). *Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering.* Kasutatud 15.03.2024, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A31991L0308
22. EUR-Lex. (23.10.2018). *Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law.*. Kasutatud 03.04.2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L1673
23. Euroopa Komisjon kodulehekülg. (22.02.2024). Commission welcomes the selection of Frankfurt as the seat for the Authority for Anti-Money Laundering and Countering the Financing of Terrorism. Kasutatud 01.04.2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_972
24. Euroopa Nõukogu kodulehekülg. (21.05.2024). Artificial Intelligence (AI) act: Council gives final green light to the first worldwide rules on AI. Kasutatud 21.05.2024, https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/
25. Euroopa Parlamendi kodulehekülg. (kuupäev puudub). Artificial Intelligence Act. Kasutatud 19.05.2024. https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(COD)%26l=en
26. FATF (2012-2023). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.* Prantsusmaa: Pariis. Kasutatud 21.03.2024, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html
27. FATF. (2021). *Opportunities and Challenges of New Technologies for AML/CFT*. Prantsusmaa: Pariis. Kasutatud 05.03.2024, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.inline.pdf
28. Finantsinspektsiooni kodulehekülg. (kuupäev teadmata). Eesti krediidiasutused. Kasutatud 19.03.2024, https://www.fi.ee/et/pangandus-ja-krediit/krediidiasutused

29. Finantsinspektsiooni kodulehekülg. (26.03.2018). Versobank ASi tegevusluba tunnistati kehtetuks. Kasutatud 02.04.2024, https://www.fi.ee/et/uudised/versobank-asi-tegevusluba-tunnistati-kehtetuks
30. Finantsinspektsiooni kodulehekülg. (19.02.2019). Finantsinspektsioon tegi Danske Bankile ettekirjutuse lõpetada Eestis tegevus. Finantsinspektsioon. Kasutatud 02.04.2024, https://www.fi.ee/et/uudised/finantsinspektsioon-tegi-danske-bankile-ettekirjutuse-lopetada-eestis-tegevus
31. Finantsinspektsiooni kodulehekülg. (19.03.2020a). Swedbank saab trahvi ja ettekirjutuse rahapesu vastu võitlemise reeglite rikkumise eest. Finantsinspektsioon. Kasutatud 02.04.2024, https://www.fi.ee/et/uudised/swedbank-saab-trahvi-ja-ettekirjutuse-rahapesu-vastu-voitlemise-reeglite-rikkumise-eest
32. Finantsinspektsiooni kodulehekülg. (25.06.2020b). AS SEB Pank sai rahapesu tõkestamise reeglite rikkumise eest trahvi. Kasutatud 02.04.2024, https://www.fi.ee/et/uudised/seb-pank-sai-rahapesu-tokestamise-reeglite-rikkumise-eest-trahvi
33. Finantsinspektsiooni kodulehekülg. (28.08.2023). Finantsinspektsioon trahvis AS-i LHV Pank ligi miljoni euroga. Kasutatud 02.04.2024, https://www.fi.ee/et/uudised/finantsinspektsioon-trahvis-i-lhv-pank-ligi-miljoni-euroga
34. Finantsinspektsiooni kodulehekülg. (19.01.2024). Finantsinspektsioon piirab AS-i TBB pank tegevust. Kasutatud 02.04.2024, https://www.fi.ee/et/uudised/finantsinspektsioon-piirab-i-tbb-pank-tegevust
35. Gerlings, J., & Constantiou, I. (2022). Machine Learning in Transaction Monitoring: The Prospect of xAI. arXiv. https://doi.org/10.48550/arXiv.2210.07648
36. Georgieva, N. (2020). Concept, definition and characteristics of the money laundering phenomenon. *Journal of Process Management. New Technologies*, *8*, 23–37. https://doi.org/10.5937/jouproman8-26220
37. Guidotti, R., Monreale, A., Ruggieri, S., Turini, F., Giannotti, F., & Pedreschi, D. (2019). A Survey of Methods for Explaining Black Box Models. *ACM Computing Surveys*, *51*(5), 1–42. https://doi.org/10.1145/3236009
38. Han, J., Barman, U., Hayes, J., Du, J., Burgin, E., & Wan, D. (2018). NextGen AML: Distributed Deep Learning based Language Technologies to Augment Anti Money Laundering Investigation. *Proceedings of ACL 2018, System Demonstrations*, 37–42.

Melbourne, Australia: Association for Computational Linguistics. https://doi.org/10.18653/v1/P18-4007

39. Han, J., Huang, Y., Liu, S., & Towey, K. (2020). Artificial intelligence for anti-money laundering: A review and extension. *Digital Finance*, *2*(3), 211–239. https://doi.org/10.1007/s42521-020-00023-1
40. Hassija, V., Chamola, V., Mahapatra, A., Singal, A., Goel, D., Huang, K., … Hussain, A. (2024). Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence. *Cognitive Computation*, *16*(1), 45–74. https://doi.org/10.1007/s12559-023-10179-8
41. He, Y., & Chen, J. (2022). AMLChain: Supporting Anti-money Laundering, Privacy-Preserving, Auditable Distributed Ledger. In W. Meng & S. K. Katsikas (Eds.), *Emerging Information Security and Applications* (pp. 50–67). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-93956-4_4
42. Juhend kahtlaste tehingute tunnuste kohta. (25.04.2022). *Rahapesu Andmebüroo*. Kasutatud 15.03.2024, https://fiu.ee/sites/default/files/documents/2023-09/Juhend%20kahtlaste%20tehingute%20tunnuste%20kohta.pdf
43. Jullum, M., Løland, A., Huseby, R. B., Ånonsen, G., & Lorentzen, J. (2020). Detecting money laundering transactions with machine learning. *Journal of Money Laundering Control*, *23*(1), 173–186. https://doi.org/10.1108/JMLC-07-2019-0055
44. Korejo, M. S., Rajamanickam, R., & Md. Said, M. H. (2021). The concept of money laundering: A quest for legal definition. *Journal of Money Laundering Control*, *24*(4), 725–736. https://doi.org/10.1108/JMLC-05-2020-0045
45. Koster, H. (2020). Towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework. *Journal of Money Laundering Control*, *23*(2), 379–386. https://doi.org/10.1108/JMLC-09-2019-0073
46. Kute, D. V., Pradhan, B., Shukla, N., & Alamri, A. (2021). Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering–A Critical Review. *IEEE Access*, *9*, 82300–82317. https://doi.org/10.1109/ACCESS.2021.3086230
47. Labanca, D., Primerano, L., Markland-Montgomery, M., Polino, M., Carminati, M., & Zanero, S. (2022). Amaretto: An Active Learning Framework for Money Laundering Detection. *IEEE Access*, *10*, 41720–41739. https://doi.org/10.1109/ACCESS.2022.3167699

48. Labib, N., Rizka, M., & Shokry, A. (2020). *Survey of Machine Learning Approaches of Anti-money Laundering Techniques to Counter Terrorism Finance*. https://doi.org/10.1007/978-981-15-3075-3_5
49. Levi, M., & Reuter, P. (2006). Money Laundering. *Crime and Justice*, *34*(1), 289–375. https://doi.org/10.1086/501508
50. Levi, M., & Soudijn, M. (2020). Understanding the Laundering of Organized Crime Money. *Crime and Justice*, *49*, 579–631. https://doi.org/10.1086/708047
51. Lokanan, M. E. (2024). Predicting Money Laundering Using Machine Learning and Artificial Neural Networks Algorithms in Banks. *Journal of Applied Security Research*, *19*(1), 20–44. https://doi.org/10.1080/19361610.2022.2114744
52. Lowe, R. J. (2017). Anti-money laundering – the need for intelligence. *Journal of Financial Crime*, *24*(3), 472–479. https://doi.org/10.1108/JFC-04-2017-0030
53. McGrath, C., Palmgren, P. J., & Liljedahl, M. (2019). Twelve tips for conducting qualitative research interviews. *Medical Teacher*, *41*(9), 1002–1006. https://doi.org/10.1080/0142159X.2018.1497149
54. Mekpor, E. S., Aboagye, A., & Welbeck, J. (2018). The determinants of anti-money laundering compliance among the Financial Action Task Force (FATF) member states. *Journal of Financial Regulation and Compliance*, *26*(3), 442–459. https://doi.org/10.1108/JFRC-11-2017-0103
55. Milon, M. N. U. (2024). Gravitating towards Artificial Intelligence on Anti-Money Laundering A PRISMA Based Systematic Review. *International Journal of Religion*, *5*(7), 303–315. https://doi.org/10.61707/py0fe669
56. Mugarura, N. (2014). Customer due diligence (CDD) mandate and the propensity of its application as a global AML paradigm. *Journal of Money Laundering Control*, *17*(1), 76–95. https://doi.org/10.1108/JMLC-07-2013-0024
57. Olev, A., & Alumäe, T. (2022). Estonian Speech Recognition and Transcription Editing Service. *Baltic Journal of Modern Computing*, *10*(3). https://doi.org/10.22364/bjmc.2022.10.3.14
58. Pavlidis, G. (2023). Deploying artificial intelligence for anti-money laundering and asset recovery: The dawn of a new era. *Journal of Money Laundering Control*, *26*(7), 155–166. https://doi.org/10.1108/JMLC-03-2023-0050

59. Rahapesu Andmebüroo. (2006). *Rahapesu Andmebüroo aastaraamat 1995-2005*. Kasutatud 06.03.2024, https://fiu.ee/sites/default/files/documents/2020-12/rab_aastaraamat_1995-2005.pdf
60. Rahapesu Andmebüroo. (2020). *Rahapesu Andmebüroo aastaraamat 2019*. Kasutatud 06.03.2024, https://fiu.ee/sites/default/files/documents/2020-12/rab_aastaraamat_2019.pdf
61. Rahapesu Andmebüroo. (2021). *Rahapesu Andmebüroo aastaraamat 2020*. Kasutatud 06.03.2024, https://fiu.ee/sites/default/files/documents/2021-06/rahapesu%20aastaraamat%202020%20est_2.pdf
62. Rahapesu Andmebüroo. (2022). *Rahapesu Andmebüroo aastaraamat 2021*. Kasutatud 06.03.2024, https://fiu.ee/rahapesu-andmeburoo-aastaraamat-2021
63. Rahapesu Andmebüroo. (2023). *Rahapesu Andmebüroo aastaraamat 2022*. Kasutatud 06.03.2024, https://fiu.ee/rahapesu-andmeburoo-aastaraamat-2022
64. Rahapesu Andmebüroo. (2024). *Rahapesu Andmebüroo aastaraamat 2023*. Kasutatud 06.04.2024, https://fiu.ee/rahapesu-andmeburoo-aastaraamat-2023
65. Rahapesu Andmebüroo koduleheküIg. (kuupäev puudub). *Tüpoloogiateated*. Kasutatud 04.05.2024, https://fiu.ee/aastaraamatud-ja-uuringud/tupoloogiateated#tupoloogiateade-7tt2
66. Rahapesu Andmebüroo tagasiside krediidiasutustele. (2024). *Rahapesu Andmebüroo*. Kasutatud 06.04.2024, https://fiu.ee/aastaraamatud-ja-uuringud/tagasiside-teatajatele#tagasiside-krediidia
67. Rahapesu ja terrorismi rahastamise tõkestamise seadus. (01.01.2024). *Riigi Teataja*. Kasutatud 05.03.2024, https://www.riigiteataja.ee/akt/106072023071
68. Reznik, O., Utkina, M., & Bondarenko, O. (2021). Financial intelligence (monitoring) as an effective way in the field of combating money laundering. *Journal of Money Laundering Control*, *26*(1), 94–105. https://doi.org/10.1108/JMLC-09-2021-0102
69. Riigikohtu koduleheküIg. (22.03.2023). Riigikohus: pank võib tarbijaga sõlmitud põhimakseteenuse lepingu lõpetada vaid erandjuhul. Kasutatud 22.04.2024, https://www.riigikohus.ee/et/uudiste-arhiiv/riigikohus-pank-voib-tarbijaga-solmitud-pohimakseteenuse-lepingu-lopetada-vaid

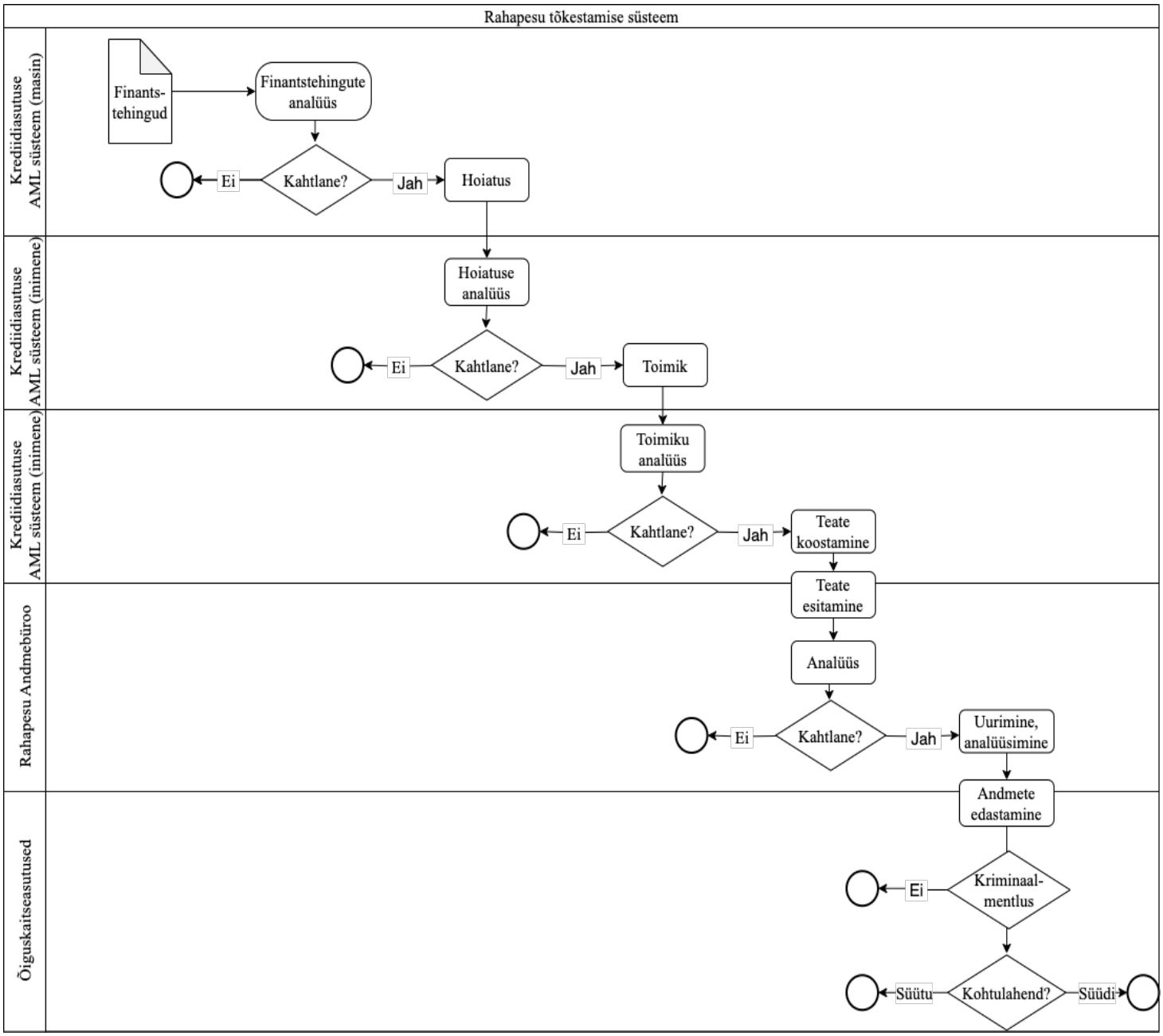
70. Scherer, M. U. (2015). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2609777
71. Schmidt, A. (2020). Interactive Human Centered Artificial Intelligence: A Definition and Research Challenges. *Proceedings of the International Conference on Advanced Visual Interfaces*, 1–4. Salerno Italy: ACM. https://doi.org/10.1145/3399715.3400873
72. Sheikh, H., Prins, C., & Schrijvers, E. (2023). Artificial Intelligence: Definition and Background. In H. Sheikh, C. Prins, & E. Schrijvers (Eds.), *Mission AI: The New System Technology* (pp. 15–41). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-21448-6_2
73. Shust, P. M., & Dostov, V. (2020). Implementing innovative customer due diligence: Proposal for universal model. *Journal of Money Laundering Control*, *23*(4), 871–884. https://doi.org/10.1108/JMLC-01-2020-0007
74. Siau, K., & Wang, W. (2018). Building Trust in Artificial Intelligence, Machine Learning, and Robotics. *Cutter Business Technology Journal*, *31*, 47–53.
75. Silva, P. G. (2019). Recent developments in EU legislation on anti-money laundering and terrorist financing. *New Journal of European Criminal Law*, *10*(1), 57-67. https://doi.org/10.1177/2032284419840442
76. Sobh, T. S. (2020). An Intelligent and Secure Framework for Anti-Money Laundering. *Journal of Applied Security Research*, *15*(4), 517–546. https://doi.org/10.1080/19361610.2020.1812994
77. Teichmann, F. (2020). Recent trends in money laundering. *Crime, Law and Social Change*, *73*(2), 237–247. https://doi.org/10.1007/s10611-019-09859-0
78. Thommandru, A. (2023). Smurfing in Electronic Banking: A Legal Investigation of the Potential for Transnational Money Laundering. *International Journal of Legal Information*, *51*(1), 69–76. https://doi.org/10.1017/jli.2023.13
79. Tiwari, M., Gepp, A., & Kumar, K. (2020). A review of money laundering literature: The state of research in key areas. *Pacific Accounting Review*, *32*(2), 271–303. https://doi.org/10.1108/PAR-06-2019-0065
80. Unger, B. (2013). Can Money Laundering Decrease? *Public Finance Review*, *41*(5), 658-676. https://doi-org.ezproxy.utlib.ut.ee/10.1177/1091142113483353

81. United Nations. (1988). *United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*. Kasutatud 11.03.2024, https://www.unodc.org/pdf/convention_1988_en.pdf
82. Verhage, A. (2009). Between the hammer and the anvil? The anti-money laundering-complex and its interactions with the compliance industry. *Crime, Law and Social Change*, *52*(1), 9–32. https://doi.org/10.1007/s10611-008-9174-9
83. Villányi, B. (2021). Money Laundering: History, Regulations, and Techniques. *Oxford Research Encyclopedia of Criminology and Criminal Justice*. https://doi.org/10.1093/acrefore/9780190264079.013.708
84. Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. *Journal of Industrial Information Integration*, *23*, 100224. https://doi.org/10.1016/j.jii.2021.100224
85. Zhang, Y., & Trubey, P. (2019). Machine Learning and Sampling Scheme: An Empirical Study of Money Laundering Detection. *Computational Economics*, *54*(3), 1043–1063. https://doi.org/10.1007/s10614-018-9864-z
86. Weber, M., Chen, J., Suzumura, T., Pareja, A., Ma, T., Kanezashi, H., Kaler, T., Leiserson, C.E., & Schardl, T.B. (2018). Scalable Graph Learning for Anti-Money Laundering: A First Look. ArXiv, abs/1812.00076.
87. Yasaka, N. (2017). Data mining in anti-money laundering field. *Journal of Money Laundering Control*, *20*(3), 301–310. https://doi.org/10.1108/JMLC-09-2015-0041

## Lisad

Lisa A.

Rahapesu tõkestamise süsteem (Allikas: autori poolt modifitseeritud Han et al., 2020; Kute et al 2021; põhjal)



Lisa B.

Intervjuuplaan (Allikas: autori koostatud)

| | |
|---|---|
| **I teema**: AI termin ja rakendamise eeldused | 1. Kuidas mõistate terminit „tehisintellekt“?<br>2. Milline on Teie arusaam reeglipõhistest meetoditest rahapesu tõkestamisel ja kuidas need erinevad masinõppest, sealhulgas juhendatud ja juhendamata õppest, ja süvaõppest?<br>- *Kuidas hindate nende erinevate lähenemisviiside efektiivsust rahapesu tõkestamisel?*<br>3. Millised eeldused peaksid asutusel olema täidetud, et tehisintellekti oleks võimalik rakendada? |
| **II teema**: Rahapesu tõkestamise probleemkohad | 4. Millised on Teie hinnangul praegused probleemkohad ja väljakutsed rahapesu tõkestamisel? |
| **III teema**: AI tugevused ja rakendamine | 5. Millised on Teie arvates peamised tehisintellekti kasutamisega seotud tugevused (eelised võrreldes inimesega) rahapesu tõkestamise valdkonnas?<br>6. Millistesse rahapesu tõkestamise protsessides oleks kõige rohkem vaja tehisintellekti rakendada (st masina tulemus ületaks korduvalt inimese võimekust)?<br><br>*Võimalusel*:<br><br>7. *Kas Teie asutuse strateegia hõlmab endas kaasaegsete tehnoloogiate rakendamist töö lihtsustamiseks või parendamiseks?*<br>8. *Kas Teie asutuses on olemas pädevus tehisintellekti arendamiseks ja treenimiseks?*<br>9. *Kas Teie asutus on teinud investeeringuid tehisintellekti arendamisse?* |
| **IV teema**: AI rakendamisega seotud probleemkohad | 10. Millised on Teie arvates tehisintellektiga seotud probleemkohad/puudused/piirangud/väljakutsed rahapesu tõkestamisel?<br>11. Millised on tehisintellekti kasutamisega seotud riskid rahapesu tõkestamisel? |
| **V teema**: AI ja inimene | 12. Kas tehisintellekt saab mingil määral asendada inimtöötajat rahapesu tõkestamise protsessides?<br>13. Kas Teie arvates on selliseid rahapesu tõkestamise protsesse, kus tehisintellekt ei saa asendada inimtöötajat?<br>14. Kuidas tasakaalustaksite automaatseid tehisintellekti otsuseid inimkontrolli ja -sekkumisega? Milline oleks ideaalne tasakaal tehisintellekti võimete ja inimspetsialisti oskuste vahel? |
| **VI teema**: AI tulevikuväljavaated | 15. Kuidas näete tehisintellekti rolli muutumist rahapesu tõkestamise valdkonnas lähitulevikus? |

Lisa C.

Intervjuu valim (Allikas: autori koostatud)

| | **Intervjueeritav** | **Ametikoht** | **Asutus** | **Toimumise aeg** | **Toimumise koht** | **Intervjuu kestvus** | **Trans-kribeering** |
|---|---|---|---|---|---|---|---|
| 1 | Intervjueeritav 1 | Vastavuskontrolli juht | Krediidiasutus A | 15.04.2024 | Google Meet | 35 min 15 sek | 9 lk |
| 2 | Intervjueeritav 2 | AML ja vastavuskontrolli juht | Krediidiasutus B | 18.04.2024 | Microsoft Teams | 23 min 36 sek | 6 lk |
| 3 | Intervjueeritav 3 | Vastavuskontrolli juht | Krediidiasutus C | 17.04.2024 | Kontor | 39 min 1 sek | 9,5 lk |
| 4 | Intervjueeritav 4 | Andmeteadlane | | | | | |
| 5 | Intervjueeritav 5 | AML strateegia grupijuht | Krediidiasutus D | 19.04.2024 | Google Meet | 46 min 20 sek | 11,5 lk |
| 6 | Intervjueeritav 6 | Juhtivanalüütik | Valitsusasutus A | 16.04.2024 | Kontor | 19 min 42 sek | 5,5 lk |
| 7 | Intervjueeritav 7 | Infotehnoloogia juht | Valitsusasutus A | 17.04.2024 | Kontor | 44 min 57 sek | 15 lk |
| 8 | Intervjueeritav 8 | Juhtivanalüütik | | | | | |
| 9 | Intervjueeritav 9 | Andmejuht | Valitsusasutus A | 16.04.2024 | Microsoft Teams | 55 min 43 sek | 12,5 lk |
| **Kokku** | | | | | | **264 min 34 sek** | **69 lk** |

Lisa D.
Kodeerimistabel (Allikas: autori koostatud kasutades NVivo tarkvara)

| **Koodid ja kategooriad** | **Intervjuude arv** | **Tsitaatide arv** |
|---|---|---|
| **AI kasutamise eeldused** | | |
| Teadvustamine | 2 | 3 |
| Regulatsioonidele vastavus | 3 | 4 |
| Riskihinnang | 4 | 5 |
| Andmete olemasolu ja kvaliteet | 6 | 17 |
| Andmekaitse | 3 | 6 |
| Tehnilised lahendused ja teadmised | 6 | 16 |
| Finantsiline võimekus | 6 | 11 |
| **AI tugevused** | | |
| Massandmete analüüs | 5 | 8 |
| Kiirus | 4 | 6 |
| Ühetaolisus | 3 | 4 |
| **AI rakendamise väljakutsed** | | |
| Vähene selgitatavus („must kast“) | 5 | 9 |
| Kontekst | 3 | 4 |
| Loovus | 3 | 3 |
| Treeningandmestik | 4 | 8 |
| **AI rakendamise võimalused** | | |
| Tööprotsesside automatiseerimine | 5 | 10 |
| Monitoorimine | 5 | 8 |
| Otsustustugi | 2 | 4 |
| **AI ja inimene** | | |
| Otsustamine | 6 | 17 |
| Lihtsustamine | 5 | 9 |
| Järelkontroll | 3 | 6 |

TEHISINTELLEKTI KASUTAMISE VÄLJAVAATED RAHAPESU TÕKESTAMISEL EESTI KREDIIDIASUTUSTE NÄITEL

**Summary**

Prospects of Using Artificial Intelligence in Anti-Money Laundering: The Case of Estonian Credit Institutions

Ketlin Saar

Money laundering is a serious financial crime, which prevention has over time become increasingly complex. The rapid advancement of technology has highlighted the crucial role of Artificial Intelligence (AI) in combating money laundering. While various AI solutions and their combinations have been discussed in scientific literature for preventing money laundering, these discussions are highly technical and there is limited research on the implementation of such solutions within institutional anti-money laundering (AML) systems. Consequently, the primary goal of this Master's thesis is to explore the experiences and perspectives of experts in the AML field regarding the opportunities and challenges associated with using AI in AML systems.

Financial institutions must understand and mitigate the money laundering risks associated with their operations by developing and implementing effective AML systems. Investments in these systems are crucial not only for risk mitigation but also for regulatory compliance and reputation management. Generally, AML systems rely on the principle of knowing your customer and monitoring financial transactions. Traditionally, rule-based systems are used for monitoring financial transactions as these are easily understandable by humans, but they are not enough to detect new money laundering methods and complex transaction patterns. AI, particularly machine learning (ML) and deep learning (DL) techniques, offers capabilities to handle large datasets, detect complex patterns, and continuously update with new data, making them potentially more effective than rule-based systems for monitoring financial transactions. Furthermore, AI can quickly and accurately process data from various sources, significantly reducing the manual workload and improving the speed and quality of analysis, thus supporting human decision-making.

In the empirical section, the author conducted interviews with representatives from Estonian credit institutions and government agency to understand experts' views on using AI in AML. It emerged that rule-based systems are the current standard in monitoring financial transactions due to their ease of justification to regulators. A major challenge with ML and DL methods is their lack of explainability, making their use in strictly regulated AML

systems complicated. Furthermore, the effectiveness of ML solutions is limited by insufficient data. Training data scarcity and the lack of feedback on actual money laundering transactions limit the development of effective AI models. Despite these challenges, combining rule-based and AI methods could enhance the detection of complex transaction patterns. This approach allows for the identification of transaction patterns previously undetected by humans and the creation of new rules based on the information obtained. AI can also automate simple, time-consuming tasks, improving analysis speed and reducing manual labor, allowing human experts to focus on more complex decisions where social context and judgment are crucial. The AML process still requires human involvement, as AI lacks the social component crucial for final decision-making. Thus, AI can provide decision support and assist with manual and routine tasks.

TEHISINTELLEKTI KASUTAMISE VÄLJAVAATED RAHAPESU TÕKESTAMISEL EESTI KREDIIDIASUTUSTE NÄITEL

**Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks**

Mina, Ketlin Saar,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose „Tehisintellekti kasutamise väljavaated rahapesu tõkestamisel Eesti krediidiasutuste näitel“, mille juhendaja on professor Maaja Vadi, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 4.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Ketlin Saar
**21.05.2024**