TARTU ÜLIKOOL

Majandusteaduskond

Enrik Lillemaa

# RAHAPESU JA TERRORISMI RAHASTAMISE TÕKESTAMINE EESTI SUURPANKADES

Bakalaureusetöö

Juhendaja: lektor Maire Nurmet

Tartu 2024

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

**Sisukord**

## Sissejuhatus

Rahapesu ja terrorismi rahastamise tõkestamine (RTRT) on üks kõige jälgitumaid ning olulisemaid regulatsioone finantssektoris. Rahapesu ja terrorismi rahastamise tõkestamise eesmärgiks on ära hoida olukorda, kus kriminaalse tegevuse käigus muudetakse raha seaduslikuks ehk antud finantsvahenditel näiliselt puuduks ühendus kriminaalse tegevusega (Eesti Pangaliit, kuupäev puudub). Ebaefektiivne reguleerimine mõjutab ühiskonda ja majandust negatiivsetel viisidel. Üheks suurimaks tagajärjeks ühiskonna ebaefektiivse reguleerimisega ja majanduse suhtes on kuritegevuse suurenemine. Riikidel ja erinevatel ühendustel näiteks Euroopa Liidul on kohustus jälgida ning luua erinevaid korraldusi, et ära hoida rahapesu ja terrorismi tõkestamine, mida peamiselt reguleerib Euroopa parlamendi ja nõukogu direktiiv 2015/849. Rahapesu ja terrorismi rahastamise tõkestamist Eestis reguleerib rahapesu ja terrorismi rahastamise tõkestamise seadus (RahaPTS), mille eesmärgiks on suurendada ettevõtluskeskkonna usaldusväärsust ja läbipaistvust, takistades Eesti Vabariigi rahandussüsteemi ja majandusruumi kuritarvitamist rahapesu ja terrorismi rahastamise eesmärgil (RiigiTeataja, 2022). Suurim vastutus jääb pankadele – finantseerimisasutused peavad jälgima, et nende finantstegevuses ei toimuks ebaseaduslike tehinguid ja luua ennetavaid eeskirju, et vähendada riske rahapesu ja terrorismi rahastamiseks.

Rahapesu ja terrorismi rahastamise tõkestamine on aktuaalne probleem tänapäevases ühiskonnas. Olulisustegurid on rahapesu ja terrorismi rahastamisel laialdased nagu näiteks ausa finantssüsteemi loomine, finantssüsteemi turvalisus, mis tagab rahvusvahelise ja siseriikliku julgeoleku. Eesti meedias on viimastel aastatel kajastatud kahte ebaseaduslike tehingute süüdistust; Danske Banki rahapesu juhtumit ja Swedbanki rahapesu kahtlust. Riikides esinevad ebaseaduslike tehingute juhtumid seavad riigi ja riigi finantssüsteemi usaldusväärsuse kahtluse alla. Riskifaktoriks on e-residentsuse pakkumine, mistõttu tuleb pankadel ja riigil olla oma eeskirjade ja järelevalve suhtes eriti tähelepanelik, et ära hoida ebaseaduslikke tehinguid.

Tartu Ülikooli digitaalarhiiv DSpace'is on avaldatud Tartu Ülikooli bakalaureusetööd rahapesu ja terrorismi rahastamise tõkestamisega seotud teemad on olnud õigusteaduspõhised lähtudes Eesti Vabariigi kriminaalseadustikust ning Euroopa Liidu andmekaitseseadusest. Bakalaureusetöö läheneb rahapesu ja terrorismi rahastamise tõkestamisele läbi intervjuude, et avastada, kuidas suurpangad orienteeruvad läbi keeruliste regulatsioonide ehk riigi ja majanduslike ühenduste poolt ette antud eeskirjade ning seaduste.

Käesoleva bakalaureusetöö eesmärgiks on välja selgitada, milliseid rahapesu ja terrorismi rahastamise tõkestamise regulatsioone pangad kasutavad.

Autor seadis tööle järgnevad uurimisülesanded:

1) Analüüsida erinevaid teaduslikke allikaid ja õigusakte rahapesu ja terrorismi rahastamise tõkestamise kohta.
2) Viia läbi intervjuu Eesti suurpankade esindajatega, et selgitada välja, kuidas pankades toimib rahapesu ja terrorismi rahastamise tõkestamine.

Vastavalt uurimisülesannetele on autor on püstitanud järgnevad uurimisküsimused:

1) Mis on rahapesu ja terrorismi rahastamise tõkestamine?
2) Milliseid regulatsioone kasutavad pangad rahapesu ja terrorismi rahastamise tõkestamiseks?
3) Milliseid meetmeid kasutavad pangad rahapesu ja terrorismi rahastamise tõkestamiseks?
4) Milline on rahapesu ja terrorismi rahastamise ebaefektiivsel tõkestamisel tekkiv kahju?

Bakalaureusetöö koosneb teoreetilisest ja empiirilisest osast. Teoreetilises osas kajastatakse rahapesu ja terrorismi rahastamise tõkestamise olemust – mis see on ning kes ja kuidas seda reguleerib. Kajastatakse rahapesu ja terrorismi rahastamise tõkestamise olulisust majanduslikul tasemel ehk mõju riigi majanduskasvule ning panganduse tasemel ehk millised on juriidilised karistused antud tegevuse tagajärjel ja milliseid meetmeid kasutavad pangad, et ära hoida rahapesu ja terrorismi rahastamine. Empiirilises osas viib autor läbi süvaintervjuud Eesti suurpankade kontaktisikutega ning uurib, kasutades avatuid küsimusi kuidas suurpangad tegelevad rahapesu ja terrorismi rahastamise tõkestamisega.

Autor kasutab bakalaureusetöös kvalitatiivseid uurimismeetodeid ehk viib läbi süvaintervjuud Eesti suurpankade kontaktisikutega. Samuti kasutab autor teadusallikaid andmebaaside *ScienceDirect*'i ning *Google Scholar*'i, mille vahendusel olulisemateks allikateks on Maailmapank (*World Bank Group*) ja Ciphertrace, nii Euroopa Liidu direktiive ehk Euroopa Liidu poolt loodud õigusakte, mida liikmesriigid peavad rakendama, eriti direktiivi 2015/849, kuid ka Eestis olevaid seaduseid rahapesu ja terrorismi rahastamise tõkestamiseks nii Riigi Teataja (RT), Finantsinspektsiooni (FI), Rahapesu Andmebüroo poolt antud allikatest (Rahapesu Andmebüroo, 2023). Autor võttis ühendust Eesti kolme suurima pangaga, kellest SEB pank andis nõusoleku avalikult kasutada toimunud intervjuud teadustööks, anonüümseks jääv pank andis loa kasutada intervjuud teadustööks tingimusel, et tagatakse panga anonüümsus, kolmas pank, kellega autor võttis ühendust, ei soovinud

intervjuud anda. Antud intervjuudes osalesid SEB *KYC* (*Know Your Customer* ehk tunne oma klienti) tiimijuht Kristo Keldre ning anonüümseks sooviva jääda panga rahapesu tõkestamise osakonna juhataja. „Tunne oma klienti“ on regulatsioon pankade poolt, mis aitab tuvastada klienti ja tema tehingute põhimõtteid ning sellega veenduda, et klient ei sooritaks ebaseaduslike tehinguid. Andmete paremaks analüüsiks kasutab autor intervjuude analüüsimiseks *Cross-case* analüüsi, mille käigus autor kogus intervjuudest olulisemad tekstiosad ja võrdles neid omavahel.

# 1. Rahapesu ja terrorismi rahastamise tõkestamise raamistik

## 1.1. RTRT mõiste, regulatsioonide eesmärgid ja tähtsus

Rahapesu ja terrorismi rahastamise tõkestamine on pankadele äärmiselt oluline tegevus, mis mõjutab pankade usaldusväärsust ja mainet. Rahapesu ja terrorismi rahastamise tõkestamine on meetmete, regulatsioonide, õigusaktide ja juhendite kogum, mis takistab kurjategijatel ebaseadusliku raha seaduslikuks muuta või kasutada raha terrorismi toetamiseks. Rahapesu on ebaseaduslik tegevus, kus kurjategijad proovivad ebaseaduslikult teenitud raha muuta seaduslikuks. Analüütikud prognoosivad, et aastas muudetakse umbes 2 triljoni dollari väärtuses ebaseaduslikult teenitud raha seaduslikuks läbi panganduse, mis moodustab umbes 2-5% maailma sisemajanduse kogutoodangust (KPMG, 2022). Rahapesu ja terrorismi rahastamine tõkestamine on valitsuse poolt antud regulatsioonide täitmine finantseerimisasutuste poolt. (RiigiTeataja, 2022). Eelnevalt nimetatud definitsioon on kasutatav karistusseadustikus, kuid ka Finantsinspektsiooni soovituslikus juhendi „Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks“. Karistusseadustik nimetab rahapesu liike kolmeks nii: a) isikut, kes tegeles rahapesuga, keda karistatakse kuni viieaastalise karistusega või rahalise karistuse, b) finantseerimisasutuse töötajat, kes jätab teavitama isiku, kes ei läbinud isikutuvastamise protsessi, keda karistatakse rahalise karistusega või c) finantseerimisasutuse juhti või kontaktisikut, kes jättis ebaõigete andmete esitamise või rahapesu kahtlusest teavitama, keda karistatakse kuni üheaastalise vangistusega või rahalise karistusega (RiigiTeataja, 2022). Vastavalt Eesti seadustele on oluline tagada regulatsioonide toimimine pangas nii juriidilistel, kuid ka ärilistel põhjustel.

Pankadele on kehtestatud erinevad regulatsioonid, et tagada rahapesu ja terrorismi rahastamise tõkestamine. Vastavalt Euroopa Liidu direktiividele peavad liikmesriikides olevad finantseerimisasutused kasutama Euroopa Liidu direktiivide juhiseid rahapesu ja terrorismi rahastamise režiimi parandamiseks, eelkõige kindlates valdkondades, kus peab rakendama tõhustatud meetmeid; vajaduse korral teha kindlaks sektorid või valdkonnad, kus

rahapesu ja terrorismi rahastamise oht on väiksem või suurem; kasutada direktiive rahapesu ja terrorismi rahastamise tõkestamiseks vajalike ressursside eraldamisel ja prioriteetide seadmisel; tagada, et iga sektori või valdkonna jaoks koostatakse asjakohased eeskirjad vastavalt rahapesu ja terrorismi rahastamise riskidele; tegema kohustatud isikutele viivitamata kättesaadavaks asjakohase teabe, et hõlbustada nende endi rahapesu ja terrorismi rahastamise riskianalüüside tegemist (The European Parliament and The Council of The European Union, 2015). Direktiiv suunab finantseerimisasutusi tugevdama kohustusi klientide tuvastamisel ja hoolsusmeetmete rakendamisel. Lisaks rõhutakse koostööle liikmesriikide vahel, et tagada tõhusad meetmed rahapesu ja terrorismi tõkestamise vastu.

Olulisimaks rahvusvaheliseks regulatsiooniks on Euroopa parlamendi ja Euroopa Liidu Nõukogu direktiiv 2015/849. mille peamisteks eesmärkideks on: a) riskipõhine lähenemine rahapesu ja terrorismi rahastamise tõkestamisel ehk finantseerimisasutused peavad hindama oma klientide rahapesu ja terrorismi rahastamise riske ning võtma vastavalt sellele meetmeid; b) kõrgendatud kliendi tuvastamise nõuded riskantsete tehingute, klientide või geograafiliste piirkondade puhul; c) liikmesriikidel peavad olema tõhusad, proportsionaalsed ja ranged karistused rikkumiste korral; d) finantseerimisasutustel peavad olema süsteemid ning meetmed finantstehingute jälgimiseks ja kahtlaste tehingute tuvastamiseks (Euroopa Liidu Teataja, 2018).

Euroopa Liidu Nõukogu on välja andnud rahapesu ning kriminaaltulu avastamise, arestimise ja konfiskeerimise konventsiooni, mille eesmärgiks on tagada efektiivsed meetmed rahapesu ja kriminaaltulu vastu võitlemiseks. Meetmeteks on konfiskeerimine ning liikmesriikide omavaheline abistamiskohustus kriminaaltulu leidmiseks. Konventsioon tagab rahvusvahelise koostöö ja koordineerimise rahapesu vastu võitlemisel. (Council of Europe, 1990) Konventsiooni loob selged kohustused ja korraldused liikmesriikidele, et leida kriminaalset tulu ja ära hoida rahapesu.

Euroopa Parlamendi ja Nõukogu direktiiv 2009/110/EÜ eesmärkideks on: a) Tagada ühtne elektroonilise raha õigusraamistik kogu Euroopa Liidus; b) Seada meetmed elektroonilise raha kasutamise potentsiaalsete maksupettuste ja rahapesu vastu, näiteks kahtlustatud kuritegevusliku raha külmutamine ehk raha omanikul ei ole võimalik kasutada pangas olevaid finantsvahendeid; c) Julgustada elektroonilise raha asutusi tegutsema piiriüleselt, tagades teenuste vaba liikumise Euroopa Liidu sees (Official Journal of the European Union, 2009). Direktiiv 2009/110/EÜ seab kindlad reeglid Euroopa Liidu liikmesriikide finantseerimisasutustele. Direktiiv julgustab liikmesriikide panku kasutama elektroonilist raha, kuid jälgima, et seda kasutatakse seaduslikeks tehinguteks.

Euroopa Liidu Nõukogu otsus nr 2000/642/JSK eesmärgiks on võimaldada finantsluure üksustel kiiresti ja efektiivselt saada liikmesriikidelt informatsiooni isikute kohta, keda kahtlustatakse rahapesus ja/või terrorismi rahastamises, samas pidades kinni andmekaitse seadustest (Official Journal of the European Communities, 2000). Eestis on finantsluure üksuseks Rahapesu Andmebüroo. Direktiiv rõhutab Euroopa Liidu liikmesriike aktiivsele finantsluure üksuste vahelisele koostööle ja informatsioonivahetuse tähtsusest. Koostööd tehes on rahapesu ja terrorismi rahastamise vastu võitlemine efektiivsem ja kergemini avastavam.

Euroopa Liidu Nõukogu direktiiv 2014/42/EL eesmärkideks on: a) peatada üle piiride toimuv kuritegevus; b) tutvustada meetmeid ja kohustusi, mis aitavad ennetada ja avastada terrorismi rahastamist. Antud direktiivis olulisimaks meetmeks on finantsvarade konfiskeerimine ning selle kasutamine avalikudeks teenusteks; c) suunata liikmesriike rangelt karistama isikuid, keda on süüdi mõistetud terrorismi rahastamises (Official Journal of the European Union, 2014). Direktiiv on loodud, et vähendada terrorismi rahastamist ning võtta ära terroristidelt ressursse. Peale kuritegevusega võitlemisega, on see oluline ka ühiskonnale, sest konfiskeerides terrorismi toiminguteks mõeldud raha saab suunata avalikesse teenustesse.

Eesti Vabariigi rahapesu ja terrorismi rahastamise tõkestamise seadus on alus rahapesu ja terrorismi rahastamise tõkestamises, mille eesmärkideks on: a) tõkestada rahapesu ja terrorismi rahastamist Eesti rahandussüsteemis; b) reguleerida rahapesu ja terrorismi rahastamisega kaasnevate riskide juhtimise, maandamine ja hindamise põhimõtteid; c) reguleerida Rahapesu Andmebüroo tegevust; d) reguleerida karistusi rahapesu ja terrorismi rahastamise eest; e) suunata finantseerimisasutusi hindama riske ja kohandama erinevaid meetmeid kui esineb kahtlus rahapesu ja terrorismi rahastamisel; f) suunata finantseerimisasutusi teavitama Rahapesu Andmebürood võimalikest rahapesu ja terrorismi rahastamise kahtlustest (RiigiTeataja, 2022). Eesti Vabariigi rahapesu ja terrorismi rahastamise tõkestamise seadus on oluline õigusakt, mis määratleb selged kohustused finantseerimisasutustele rahapesu ja terrorismi rahastamise vastu võitlemisel. Seadus nõuab ranget klientide tundmaõppimist, klientide tehingute jälgimist ning kriitilist hindamist, keda endale kliendiks võetakse. Samuti sätestab seadus karistused rikkumiste eest.

Rahapesu Andmebüroo põhimääruse eesmärk on reguleerida Rahapesu Andmebüroo organisatsiooni struktuuri, ülesandeid ja töökorraldust, mis tagab efektiivse toimimise ja hoides ära rahapesu ja terrorismi rahastamise Eesti finantseerimisasutustes. Rahapesu

Andmebüroo peab olema ka finantsjärelevalveasutus ehk koguma ning analüüsima informatsiooni ja vajadusel jagama seda teiste avalike asutustega (Riigi Teataja, 2020).

Ebaseaduslike tehingute sooritamine on tervele majandusele negatiivse mõjuga, kuna ebaseaduslikud tehingud õõnestavad õiguspärast erasektorit, kahjustavad finantsturge, vähendavad majanduspoliitika rolli, suurendavad majanduslikku ebastabiilsust. Riik kaotab tulusid, kuna rahapesu tulemusel ei maksta, tekivad erastamispüüdluste ohud ning tekitab riigile ka maineriski (U.S. Department of State, 2001). Aastatel 2000-2009 kaotasid pangad üle 350 miljardi euro ehk umbes 15% pankade koguväärtusest trahvide maksmisega, milles ebaseaduslike tehingute ärahoidmine oli peamine väärkäitumise põhjus (Busetto, Gardó, & Klaus, 2019). Maailmapanga makroökonoomika ja kasvu osakond esitles 2016-ndal aastal oma uuringu, kuidas ebaseaduslikud tehingud ning sealt tulenev kuritegevus mõjutab majandust Kolumbias. Uuringus leiti, et kuritegevusega teenitud vara akumuleeritakse väga vähe võrreldes puhta rahaga. (World Bank Group, 2016) See mõjutab riigi majandusnäitajaid negatiivselt, kuna illegaalselt teenitud raha aeglustab majanduskasvu ning muudab majandust ebastabiilsemaks. Riik kaotab sellega maksutulusid, kuna rahapesust tulenevat raha ei ole võimalik maksustada. Rahapesu ja terrorismi rahastamise tõkestamise efektiivne reguleerimine ning kontroll regulatsioonide täitmise üle vähendab rahapesu tekkimise riski, tehes ebaseaduslike tehingute sooritamise kurjategijatele keeruliseks ja seega väldib riik negatiivseid tagajärgi, mis võivad olla riigi majandusele ning mainele kaaluka negatiivse mõjuga (International Monetary Fund, 2023).

Tänapäevane tehnoloogiale arenenud maailm pakub palju võimalusi, millest ka pangad vastavalt enda huvidele kasutavad. Üheks selleks on automatiseerimine ja tehisintellekti areng. Rahapesu andmebüroo peab automatiseerimist oluliseks, et suurendada rahapesu tõkestamise efektiivsust (Rahapesu Andmebüroo, 2020). Pankadele teeks automatiseerimine lihtsamaks tehingute jälgimise ning kahtlaste tehingute jälgimise. Ebatavalised tehingud või tegevused viitavad majanduslikult ebatavalistele või ebaloogilistele olukordadele ning juhtumitele, mis on eluliselt raskesti usutavad, osutades võimalikele seostele rahapesu, ebaseadusliku tulu varjamise või muu illegaalse tegevusega (Rahapesu andmebüroo, 2022). Automatiseerimine on pankadele äriliselt kasulik, kuna pangad säästavad tööjõukuludelt, sest personali, kes esimese ning teise kaitseliiniga ei läheks antud juhul enam nii palju vaja. Jaanuaris 2018 ilmus artikkel, kus analüüsiti, kuidas automatiseerimine võiks aidata rahapesu ja terrorismi rahastamise tõkestamisele kaasa. Leiti, et praegune automatiseeritud süsteem finantseerimisasutustes, ei ole väga efektiivne – puudub kontaktlüli automatiseerimise ja inimeste vahel ning automatiseeritud süsteemid ei

ole suutnud väga edukalt tuvastada kahtlaseid tehinguid. Artikli autorid uurisid erinevaid viise, kuidas saaks pettust ning rahapesu tuvastamist ühendada ning mõtlesid välja mitme agendi süsteemi (*multiagent system* ehk MAS), mis oleks efektiivne ning toetaks inimeste ning tehisintellekti koostööd. Mitme agendi süsteem arendamiseks, kasutati tehisintellektil tuvastada riskigruppe ning luua iga kliendile omane tehingute põhine profiil ehk kui toimuks tehing, mis ei vasta kliendi profiilile, edastatakse info pangatöötajale ning pangatöötaja analüüsib, kas tegemist oli kahtlase tehinguga või mitte. MAS süsteem kasutab usk, soov, kavatsus ehk DBI (*Belief, Desire, Intention*) mudelit, kus tehisintellekt uurib profiili, jälgides profiili eelnevaid tehinguid ning rahapesule või pettusele omaseid tehinguid ning edasi teeb tehisintellekt otsuse, et kas tehing võib olla seotud pettuse, rahapesu, terrorismi toetamisega, siis edastatakse, antud profiil pangatöötajale üle vaatamiseks. Antud meetod kasutaks ise õppimissüsteemi ehk masin suudaks ajaga leida kiiremini ja efektiivsemalt kahtlaseid tehinguid. (Balsa & Alexandre, 2018) Tehisintellekt ning automatiseerimine toob palju võimalusi pankadele. Paljud pangad kasutavad tänapäeval automatiseeritud tehnoloogiaid, kuid need ei pruugi olla alati kõige efektiivsemad. Pankadel ning riikidel tasuks panustada rohkem ressursse tehnoloogiliste viiside arendamisele, mis aitaksid kaasa rahapesu efektiivsema tuvastamiseni.

Eestil on olnud negatiivseid kogemusi rahapesuga. Üks suurimaid nendest oli Danske Panga skandaal 2017 aastal, kus peamiselt Eestis toimus antud illegaalne tegevus, sai aastal 2022 ka kohtu poolt lõpplahenduse – Danske Pank mõisteti süüdi rahapesus osalemisega ning mõisteti trahviks 2 miljardit dollarit (Danske Bank). Pankadele võib olla antud suuruses trahvid ettevõtet hävitavad, eriti kuna saadud tulu, mida pangad võisid teenida vältides rahapesu ja terrorismi rahastamise regulatsioone, on vaid väga väikene summa võrreldes potentsiaalsete trahvidega, seepärast on pankadele oluline pidevalt oma töötajaid koolitada ning tagada julgeolek, et kurjategijad ei oleks suutelised pangas tegeleda rahapesuga ega terrorismi rahastamisega.

Pankade vahel puudub otsene kliendiandmete jagamise õigus, kuna see on keelatud vastavalt isikuandmete seadusele, kuid kui tegemist on kahtlaste tehingutega, siis antakse pangale võimalus jagada andmeid teiste pankadega (Euroopa Andmekaitsenõukogu, 2020). Euroopa Andmekaitsenõukogu (EDPB) on avaldanud avalduse Euroopa Komisjoni tegevuskava kohta rahapesu ja terrorismi rahastamise tõkestamise poliitika kohta. Tegevuskava loomisel võeti arvesse andmekaitse-eeskirju, eriti Euroopa Liidu isikuandmete kaitse üldmäärusega (GDPR). Rahapesu ja terrorismi rahastamise vastane võitlus on oluline, kuid samavõrra tähtsaks tuleb pidada ka andmekaitset. Kõik rahapesu ja terrorismi

rahastamise tõkestamiseks võetavad meetmed peavad vastama GDPR-ile. Uute tehnoloogiate, näiteks tehisintellekti kasutamine rahapesu ja terrorismi rahastamise vastases võitluses võib kujutada endast märkimisväärset ohtu inimeste õigustele ja vabadustele. (Euroopa Andmekaitsenõukogu, 2020) Pankade vahel otsene informatsiooni omavahel jagamise puudumine muudab rahapesu tõkestamise ebaefektiivsemaks, seepärast tuleb otsida erinevaid viise, kuidas oleks võimalik saavutada informatsiooni jagamine pankade vahel.

Tänapäevane digimaailm on loonud palju uusi võimalusi ning ohte. Ühelt poolt pakub tänapäevane digimaailm võimalusi näiteks e-residentsus, kiired makseid ning uusi tegevusvaldkondi panganduses nagu näiteks *peer-lending* crypto. Teiselt poolt pakub digimaailm uusi ohte, eriti pettuste osas. Internetis on väga levinud erinevad internetipettused, kuid ka pangapettused, kus proovitakse jõuda kannatanu pangakontole või kannatanu pangakaardi andmetele ning pärast edukat petturlust proovitakse antud raha legaliseerida.

Krüptoraha on olnud viimastel aastal aktuaalne teema. Aina rohkem pangad, ettevõtted ning rahavahendus ettevõtted on hakanud krüptoraha aktsepteerima ning krüptorahaga võivad kaasneda suured rahapesuohud. Veelgi tõenäolisemaks, et kurjategijad eelistavad kasutada krüptovarasid, on seetõttu, et *dark web*-is mustal turul arveldatakse krüptorahaga. Panganduse võtmes, kui pank suudab edukalt kontrollmehhanisme rakendada krüptorahale, siis sellega nad vähendavad rahapesu toimumise riski ning loovad võimaluse krüptoraha turvaliseks kasutamiseks (Utkina, 2023). Ciphertrace kvantitatiivse analüüsi ajaperioodist 9.jaanuarist 2009 20. septembrini 2018 järgi 97% 20 enim kasutatud krüptovahendite tehingud sooritati riikides, kus on rahapesu regulatsioonid nõrgad ehk nendes riikides on väga keeruline või isegi võimatu leida, kes antud tehingu oli sooritanud. *US State Department* on hinnanud, et 219 riigist 79-ndal riigil on nõrgad rahapesu ja terrorismi rahastamise tõkestamise regulatsioonid. Ciphertrace raporti autorid leidsid, et nendes riikides, kus rahapesu regulatsioonid olid nõrgad, oli sooritatud 4,7% tehingutest kriminaalselt viisil teenitud rahaga ning võrreldes riikidega, kus rahapesu oli reguleeritud on kindlaks tehtud, et 0,12% tehingutest olid sooritatud ebaseaduslikult teenitud rahaga. (Ciphertrace, 2018) Pankadel tuleb pidevalt kohaneda kiiresti muutuvas maailmas ning lubades uusi võimalusi pangas, peavad nad olema veelgi enam kohanemisvõimelised, et tagada turvaline pangandus kõigile. Krüptovarasid on hakanud pangad aina rohkem kasutama investeerimismeetodina, kuid ka maksevahendina, millel on negatiivne pool – krüptoraha on enamasti reguleerimata ning sellega on võimalik sooritada rahapesu ning terrorismi rahastamist lihtsamalt kui tavarahaga.

### 1.2. RTRT-se tuvastamise protsess ja meetmed

Rahapesu tuvastamine on keeruline protsess. Ettevõtte tasandil ei ole kerge ebaseaduslike tehinguid tuvastada, kuna rahapesuga ei tule kaasa rahalisi kulusid ja seetõttu on keeruline tõestada, et kes oli rahapesus süüdi. Ebaefektiivsel rahapesu ja terrorismi rahastamise tõkestamisel on pangale kahjud suured. Kui pangas toimub rahapesu ja/või terrorismi rahastamine, siis: a) tekib mainekahju ehk finantseerimisasutus ei ole olnud suuteline tegelema efektiivselt rahapesu ja/või terrorismi rahastamise ärahoidmisega ning see muudab terve panga usaldusväärsuse küsitavaks. Usaldusväärsuse langedes võivad aktsionärid müüa oma osakuid või/ning kliendid lõpetada oma koostöö pangaga, mis mõjutab tugevalt panga finantstulemusi; b) rahalised trahvid ehk riik trahvib finantseerimisasutust, et polnud suuteline regulatsioonide, juhendite ja soovituste jälgimisega. Aastal 2020 ainuüksi maksid pangad 14,1 miljardit dollarit trahvideks ebaefektiivse RTRT eest (KPMG, 2022).Rahapesu ja terrorismi rahastamise tõkestamise meetmeid on mitmeid, need tulenevad Eesti Vabariigi või Euroopa Liidu välja antud õigusaktidest, juhenditest ja soovitustest.

Rahapesu Andmebüroo (RAB) on andnud välja mitmeid juhendeid, kuidas ära hoida rahapesu ja terrorismi rahastamist. Üheks nendeks on juhend kahtlaste tehingute kohta, mis suunab finantseerimisasutusi teavitama Rahapesu Andmebüroole rahapesu kahtluse, ebahariliku tehingu, kohustusliku sularahateate, kui rahaline nõue on suurem kui 32 000 eurot, ebahariliku tegevuse ning terrorismi rahastamise kahtluse korral. Rahapesu tuvastamise teate tuleb esitada, kui tekib rahapesu kahtlus, antud olukorras peab peale teate esitamist kohaldada tugevdatud hoolsusmeetmed, et kontrollida kas tegemist oli rahapesuga või mitte. Kahtluse korral on keelatud äritehinguid sooritada antud osapoolega. Ebahariliku tegevuse teate peab esitama kui kohustatud isik on tuvastanud äripartneri korduvad ebaharilikud tegevused. Samuti tuleb peale teavitamist kohaldama tugevdatud hoolsusmeetmeid, et mõista, mis oli ebahariliku tegevuste taga. Erinevalt rahapesu kahtlusest tohib ebahariliku tegevusega äripartneritega jätkata tehinguid tingimusel, et sellest on Rahapesu Andmebürood varasemalt teavitatud. Sularahatehingu teate peab esitama kui antud rahaline nõue on ületanud üle 32 000 euro ning peab silmas pidama, et see ei kehti ainult ühekordse tehingu korral, vaid ka kogusummana. Krediidiasutus peab teavitama igast üle 32 000 euro tehingust juhul kui krediidiasutusel puudub tehingus oleva isikuga ärisuhe. Terrorismi rahastamise kahtluse korral jagunevad teated kaheks – TFR-1 ja TFR- 2 ehk terrorismi rahastamise riski teade ning terrorismi rahastamise kahtluse teade. Riski teate (vt Lisa A) peab esitama kui äripartneril tekib kahtlus riskiriigist (vt Lisa B) pärinevatest ebaharilikest asjaoludest. Antud olukorras võib tehingute sooritamist jätkata. Terrorismi rahastamise kahtluse teate korral tuleb teada

anda olukorrast, kus on tunnused, et tehingul on seos terrorismi rahastamisega ja antud juhul tuleb tehingud peatada kuni pädeva institutsiooni ehk näiteks Rahapesu andmebüroo edasiste juhisteni ja tuleb kahtlustavate konto peatada. (Rahapesu andmebüroo, 2022) Rahapesu ja terrorismi rahastamise kahtluse korral tuleb pangal kiirelt tegutseda ning teavitada julgeolekuasutusi.

Tehingute maht, kliendi profiil, riikidevahelised maksed, riikliku taustaga isik, tehingute jadad aitavad otsustada, kas tegemist on kahtlase tehinguga või mitte. Kahtlaste tehingute tunnuseid eristatakse erinevate olukordade suhtes: a) isiku kohta, kelle usaldusväärsus on kaheldav. Kirjeldab olukordi, kus äriühingu omandistruktuur ei ole selge või isiku vastu on varasemalt kahtlustatud tegutsemas kellegi teise nime all; b) isik käitub ebaharilikult. Kirjeldab olukordi, kus isik esitab ebatavalisi küsimusi panga rahapesu ja terrorismi rahastamise tõkestamise kohta või paistab välja nagu isik varjaks midagi; c) isiku on esitatud mitte tavapärased dokumendid. Kirjeldab olukordi, kus on kaheldav isikut tõendavat dokumentide või andmete õigsus; d) ebaharilik tegevus panga teenuste tellimisel. Kirjeldab olukordi, kus tekib vastuolu isiku või äriühingu andmete ja panga teenuste tellimise vahel. Näiteks ettevõtte soovib võtta laenu, kuid laenu võtmise põhjendus ei ole vastavus ettevõtte tegevusvaldkonnaga; e) ebaharilik tehing sularahaga. Kirjeldab olukordi, kus isiku või ettevõtte käibed ei lähe vastavusse suurte mahuliste sularaha tehingutega või soovitakse ebaharilike soove, näiteks valuuta vahetuse sooritamine suurtes kupüürides; f) Ebaharilik tehing kontol. Kirjeldab olukordi, kus tehingud kontol ei ole vastuolus ettevõtte või isiku käivetega; g) ebaharilik tehing krüptorahaga. Kirjeldab olukordi, kus virtuaalvääringuga seotud tehingud on suuremad kui 32 000 eurot; h) ebaharilik tehing väärtpaberitega. Viitab olukordadele, kus väärtpaberitega seotud tehingud sooritakse ebatavalisel viisil, näiteks sularahas või krüptovaluutaga; i) ebaharilik tegevus tehingu tegemisel. Kirjeldab olukordi, kus isik või ettevõtte ei suuda selgelt seletada tehingu tegemise põhjuseid, kasutatud raha päritolu kohta või esitab segaseid andmeid; j) ebaharilik tehing kinnisvaraga. Viitab olukordadele, kus tehingu eest tasub mitteseotud isik või kinnivarahind ei sobitu reaalse kinnivara turuhinnaga; k) hasartmängude mängimisel tekkiv ebatavaline tegevus. Kirjeldab olukordi, kus isik võidab pidevalt suuri summasid (Rahapesu andmebüroo, 2022).

Kõrgendatud hoolsusmeetmed pankade poolt aitavad kaasa rahapesu vähendamisele. Kliendi hoolsuskohustuse (CDD) protseduuride läbiviimise on eriti oluline. Kliendi olulistemaks hoolsusmeetmete protseduurideks peetakse toiminguid, kus pangad: a) järgivad õigusakte ja juhendeid, mida on Eesti Vabariik ja Euroopa Liit välja andnud; b) hindavad oma riske ehk milliste klientide lepinguid sõlmitakse; c) ei seo end isikutega, kellel on

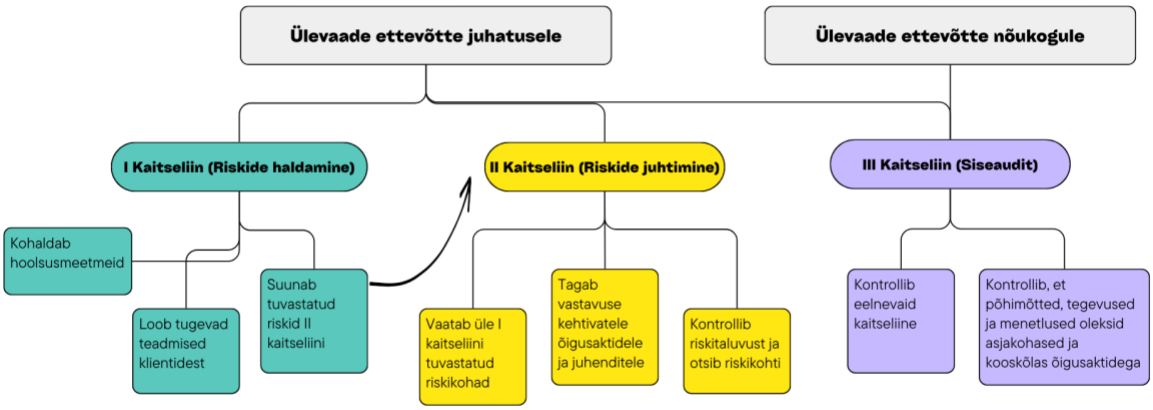
ebaselge rahaliste vahendite või tegevusvaldkond; d) kontrollivad, et riskijuhtimise mudel on efektiivne; e) tagavad, et kliendi andmed on korrektsed ja asjakohased; f) võimaldavad, et töötajad on teadlikud ning kohustatud teavitama Rahapesu Andmebürood kui tekib kahtlus, et pangas toimub rahapesu või terrorismi rahastamine (Eesti Pangaliit). Finantseerimisasutused peavad kehtestama ja haldama riskipõhiseid CDD-protseduure oma klientide, tegelike kasusaajate ja identiteedi kontrollimiseks. Tegelikuks kasusaajaks peetakse isikut, kes: a) täielikult omab äriühingu hääleõigust, osasid, aktsiaid või omab kontrolli äriühingu juhatuse üle; b) omab mõju toimingu või tehingu üle või teise isiku üle, kelle huvides tehing teostatakse; c) omab 25% või enam aktsiatest või kontrollib muul viisil ettevõtte juhtimist (Eesti Pangaliit, kuupäev puudub).

Pangad on kohustatud jälgima klientide tehinguid kahtlaste tegevuste suhtes ja teavitama kahtlastest tehingutest näiteks Rahapesu Andmebürood. Arvestuse pidamine kõigi tehingute ja kliendi tuvastamise andmete kohta on äärmiselt oluline. Rahapesu reeglite järgimise tagamiseks ning rahapesu avastamiseks ja tõkestamiseks tuleb kehtestada sisekontrollid ja protseduurid. See hõlmab töötajate koolitust tagamaks, et töötajad mõistavad rahapesuga seotud eeskirju, protseduure ja riskijuhtimist. (Finantsinspektsioon, 2018) Riskijuhtimine on panga riskide haldamine, vastavalt finantseerimisasutuse suurusele ja teenuste ning tegevuste laadile (Rahapesu Andmebüroo, 2022). Rahapesu ja terrorismi rahastamise tõkestamise seadus lõi rahapesu ja terrorismi rahastamise tõkestamise valitsuskomisjoni, kelle ülesanneteks on koordineerida riikliku riskihinnangut, koostada riske maandavaid süsteeme, korraldada ja kontrollida tegevusplaani järgimist, suurendada riigisisest koostööd (RiigiTeataja, 2022). Eestis olevate seaduste ja soovituslike juhenditega ning Euroopa Liidus olevate direktiivide on põhjalikult reguleeritud rahapesu ja terrorismi rahastamise tõkestamine.

„Tunne oma klienti“ protseduur on üks olulisemaid regulatsioone rahapesu ja terrorismi rahastamise tõkestamisel. „tunne oma klienti“ kohustus, kus finantseerimisasutused on kohustatud jälgima klientide tehinguid ning teadma, kellega pangad koostööd teevad, et eristada kurjategijaid tavainimestest (Eesti Pangaliit, kuupäev puudub). Üks esimesi samme on klientide identiteedi kontrollimine. See võib hõlmata riigi poolt väljastatud isikut tõendava dokumendi küsimist ja selle teabe kontrollimist avalikes andmebaasides. Finantseerimisasutused peavad kontrollima ka rahaliste vahendite allikat, et tagada nende õiguspärasus. Teine oluline samm on klientide riskianalüüside läbiviimine. See hõlmab erinevate tegurite, näiteks kliendi ameti, asukoha ja tehingute ajaloo analüüsimist, et määrata kindlaks nende tekitatud riskitase. Klientide suhtes, kes tegelevad kõrge riskiga

tegevustega, nagu rahvusvahelised tehingud või tehingud, mis hõlmavad suuri sularahasummasid, tuleb kohaldada tõhustatud hoolsusmeetmeid. Lisaks nendele sammudele tuleb jälgida ja salvestada klienditehinguid. Selle alla kuulub teabe salvestamine, näiteks rahavoogude allikad, tehingute eesmärgid ja tehingu asjaosalised. Täpset arvestust pidades saavad finantseerimisasutused paremini mõista oma kliente ja tuvastada võimalike riske. (Rahapesu Andmebüroo, 2022) „Tunne oma klienti“ protseduuri kasutamine aitab pangal paremini mõista, kellega nad ärisuhtesse asuvad ja sellega vähendada riski, et nende pangas toimuks kuritegevuslikud tegevused. Pankadel tuleb olla tähelepanelik, et kliendi poolt saadud andmed on korrektsed, neil puudub varasem rahapesu või terrorismi rahastamisega seos, luua kliendiprofiil ning sekkuda kui tekib kahtlaseid tehinguid.

FERMA ehk *Federation of European Risk Management Associations* on tungivalt soovitanud pankadel kasutada kolme kaitseliini süsteemi rahapesu ja terrorismi rahastamise tõkestamiseks, pidades kolme kaitseliini süsteemi oluliseks tööriistaks integreerimisel, koordineerimisel ning ühtlase tugifunktsiooni loomisel (Federation of European Risk Management Associations, 2011). Selleks on finantseerimisasutustel kohustus kasutada kolme kaitseliini süsteemi (vt *Joonis 1*.). Pankade tagatoaüksused ehk kaitseliinid, kus esimeses kaitseliinis tegeletakse kliendiandmete valideerimisega ning küsitakse klientidelt lisaküsimusi kui tekivad vastuolud kliendi poolt antud andmetega või toimuvad kahtlased tehingud. Kahtlasteks tehinguteks peetakse tehinguid, mis on toime pandud vastuolus kliendi poolt antud andmetele ehk näiteks kui klient kellel on madal sissetulek, hakkab liigutama suurtes summades raha või kui tehakse tehinguid kõrge riskiga riikidesse näiteks Türki, Indiasse või Iraani. Seda loetakse punaseks lipuks ning võib viidata rahapesule, terrorismi rahastamisele või kliendi petmisele. Teise kaitseliini tegevuseks on selliste juhtumite uurimine ja menetlemine. Samuti koostab teine kaitseliin metodoloogiat, et minimaliseerida rahapesu ja terrorismi rahastamisega seotud riske, kuidas paremini hinnata klientide riskitaset või millised tehinguid millistesse riikidesse peetakse kahtlasteks tehinguteks. Teises kaitseliinis töötab ka rahapesu andmebüroo töötaja, kes korraldab rahapesu kahtlusega isikute menetlemist ning jagab informatsiooni edasi rahapesu andmebürooga kui kahtlused võivad osutuda tõeks. Kolmandaks kaitseliini tööks on kontrollida esimest ja teist kaitseliini ja anda neile soovitusi ja nõu oma töö kohta.  (Finantsinspektsioon, 2018)




*Joonis 1*. Kolme kaitseliini ülesanded, autori koostatud
Allikas: Rahapesu Andmebüroo (https://fiu.ee/media/291/download)

Esimese peatüki esimene alapeatükk kajastab: mis on rahapesu; mis on rahapesu ja terrorismi tõkestamine; milliseid regulatsioone kasutatakse rahapesu ja terrorismi rahastamise tõkestamiseks; mis on nende regulatsioonide eesmärgid; mis on rahapesu ja terrorismi rahastamise tähtsus. Rahapesu ja terrorismi rahastamise tõkestamine on pangasektoris oluline tegevus, mõjutades pankade mainet ja usaldusväärsust. Selle eesmärk on rakendada meetmeid ja regulatsioone, mis takistavad kurjategijatel ebaseaduslikult teenitud raha seaduslikuks muutmist või selle kasutamist terrorismi rahastamiseks. Analüütikute prognooside kohaselt on aastas ligikaudu 2 triljoni dollari väärtuses ebaseaduslikult teenitud raha seaduslikuks muutmine panganduse kaudu, moodustades märkimisväärse osa maailma sisemajanduse kogutoodangust. Pangad peavad järgima Euroopa Liidu ja Eesti Vabariigi regulatsioone, mis sisaldavad nii direktiive, õigusakte kui ka Finantsinspektsiooni soovituslike juhendeid.

Euroopa Liidu direktiivide kohaselt on pankadele kehtestatud ranged regulatsioonid rahapesu ja terrorismi rahastamise tõkestamiseks. Need nõuavad finantseerimisasutustelt Euroopa Liidu juhiste järgimist, tõhustatud meetmete rakendamist riskantsete klientide suhtes ning efektiivset koostööd julgeolekuettevõtete vahel. Direktiivide eesmärkideks on tugevdada klientide tuvastamise ja hoolsusmeetmete kohustusi ja suunata liikmesriike rangelt karistama isikuid, kes rikuvad seadust rahapesu ja terrorismi rahastamisega.

Eesti Vabariigi rahapesu ja terrorismi rahastamise tõkestamise seadus määratleb finantseerimisasutuste kohustused nende vastutuses rahapesu ja terrorismi rahastamise vastu võitlemisel. Finantseerimisasutused peavad õppima tundma oma kliente, jälgima tehinguid ja kasutama hoolsusmeetmeid kui tuvastatakse rahapesu ja terrorismi rahastamise kahtlus.

Rahapesu Andmebüroo põhimäärus reguleerib Rahapesu Andmebüroo struktuuri ja ülesandeid, tagades selle tõhusa toimimise ning aktiivse rolli rahapesu ja terrorismi rahastamise tõkestamisel. Rahapesu Andmebüroo peab olema finantsjärelevalveasutus, kelle juurde pangad saavad pöörduda kui avastatakse rahapesu ja terrorismi rahastamise kahtlus.

Ebaseadusliku raha seaduslikuks muutmine avaldab negatiivset mõju majandusele, kahjustades erasektorit, finantsturge ning suurendades majanduslikku ebastabiilsust. Selle tulemusena kaotab riik tulusid ning satub maineriski.

Pankade ebaefektiivsel rahapesu ja terrorismi rahastamise tõkestamisel peavad pangad maksma suuri trahve riigile.

Tehisintellekti ja automatiseerimise kasutamine võib olla võtmeteguriks rahapesu ja terrorismi rahastamise vastases võitluses, kuid senised automatiseeritud süsteemid pole olnud piisavalt efektiivsed.

Pangad seisavad silmitsi väljakutsega jagada infot kahtlaste tehingute osas, kuid andmekaitse reeglid piiravad kliendiandmete jagamist.

Krüptoraha kasutuselevõtt ja panganduses aktsepteerimine tõstavad esile uued rahapesuohud, eriti kui kurjategijad eelistavad krüptovarasid nende reguleerimatuse tõttu. Pangad peavad olema valmis kohanema kiiresti muutuva keskkonnaga, tagades samal ajal turvalise panganduse kõigile klientidele.

Esimese peatüki teine alapeatükk seletab milliseid meetmeid kasutavad pangad, et ära hoida rahapesu ja terrorismi rahastamine. Rahapesu tuvastamine ettevõtte tasandil on keeruline, kuna sellega ei kaasne alati otsest rahalist kulu, mistõttu süüdlase tuvastamine on keeruline. Ebaefektiivne rahapesu ja terrorismi rahastamise tõkestamine toob pangale suured kahjud, kaasnedes mainekahjuga ja suurte finantstrahvidega.

Rahapesu Andmebüroo (RAB) juhendab finantsasutusi kahtlaste tehingute tuvastamisel ja teavitamisel, kehtestades selged reeglid rahapesu, ebahariliku tegevuse ja terrorismi rahastamise kahtluse korral. Peale teate esitamist kohaldatakse tugevdatud hoolsusmeetmeid, eristades kahtlaste tehingute tunnuseid, nagu ebaharilik käitumine, ebatavalised dokumendid ja mitmesugused ebaharilikud tehingud. Rahapesu ja terrorismi rahastamise kahtluse korral on pangal kohustus kiiresti tegutseda, teavitades julgeolekuasutusi ning kasutades erinevaid teguriteid.

Kõrgendatud hoolsusmeetmed, mida pangad rakendavad, on olulised vahendid rahapesu vähendamisel, eriti klientide hoolsuskohustuse protseduuride tõhusa läbiviimise kaudu. Pangad järgivad õigusakte ja juhendeid, hindavad riske, ei seondu ebaselgete rahaliste vahenditega isikutega ning tagavad, et nende riskijuhtimise mudel on efektiivne. Järeldusena on rahapesu vastase võitluse tõhusus seotud pangandussektori võimekusega rakendada põhjalikke hoolsusmeetmeid ja järgida kehtivaid regulatsioone.

Äärmiselt oluline on pidada arvestust kõigi tehingute ja kliendi tuvastamise andmete kohta ning kehtestada sisekontrollid ja protseduurid rahapesu reeglite järgimiseks. Finantsasutuste riskijuhtimine on kohandatud vastavalt nende suurusele ja tegevuste laadile. Rahapesu ja terrorismi rahastamise tõkestamise seadus on Eestis loonud valitsuskomisjoni, mis koordineerib riiklikku riskihinnangut ja suurendab riiklikku koostööd, tagades seeläbi põhjaliku reguleerituse rahapesu ja terrorismi rahastamise vastases võitluses.

"Tunne oma klienti" protseduur on oluline meetod rahapesu ja terrorismi rahastamise tõkestamisel, kohustades finantsasutusi jälgima klientide tehinguid ja teadma, kellega nad koostööd teevad. Esimese sammuna toimub klientide identiteedi kontroll, mille käigus küsitakse riiklikult väljastatud isikut tõendavat dokumenti ja kontrollitakse selle teavet avalikes andmebaasides. Lisaks tuleb kontrollida rahaliste vahendite õiguspärasust. Teine oluline samm hõlmab klientide riskianalüüside läbiviimist, võttes arvesse erinevaid tegureid nagu amet, asukoht ja tehingute ajalugu. Kõrge riskiga klientidele tuleb kohaldada tõhustatud hoolsusmeetmeid, ning finantsasutused peaksid jälgima ja salvestama klienditehinguid, aidates seeläbi paremini mõista kliente ja tuvastada võimalikke riske. See protseduur aitab pangal ärisuhtes olevaid isikuid paremini mõista, vähendades samas kuritegevusega seotud riske ja tagades, et kliendiandmed on korrektsed ning puudub varasem seos rahapesu või terrorismi rahastamisega.

FERMA on soovitanud pankadel kasutada kolme kaitseliini süsteemi rahapesu ja terrorismi rahastamise tõkestamiseks. See süsteem hõlmab esimeses kaitseliinis kliendiandmete valideerimist ja lisaküsimuste esitamist kahtlaste tehingute korral, teises kaitseliinis kahtlaste juhtumite uurimist ja metodoloogia koostamist riskide minimaliseerimiseks ning kolmandas kaitseliinis esimese ja teise kaitseliini kontrollimist ja nõustamist. See struktuur on oluline integreerimisel, koordineerimisel ja ühtlase tugifunktsiooni loomisel, võimaldades pankadel tõhusamalt tuvastada ja ennetada rahapesu ja terrorismi rahastamist.

Empiirilises osas tuleb täpsemalt uurida ja üle kinnitada erinevate pankade kontaktisikutelt, milliseid regulatsioone ja meetmeid pangad kasutavad, et tagada rahapesu ja terrorismi rahastamise tõkestamine.

## 2. Eesti suurpankade kontaktisikute intervjuu analüüs

Autor võttis ühendust pankade kontaktisikutega, kellega sai leida sobivad isikud intervjuu läbiviimiseks. Sobivate isikute leidmiseks seati kriteeriumid, milleks olid intervjueeritava pikaajaline kogemus rahapesu ja terrorismi rahastamise tõkestamisel ning pangas juhtival positsioonil olemine. Intervjuud viidi läbi digikanalite (*Zoom* ja *Teams*), kuna see oli nii autorile kui ka intervjueeritavatele kõige mugavam lahendus. Intervjuud olid poolstruktureeritud individuaalintervjuud. Varasemates uuringutes on kasutatud samuti individuaalintervjuusid, kus intervjueerijad küsisid näost-näkku ühelt Negara Malaisia panga esindajalt ja kolmelt vastavuskontrolli spetsialistilt küsimusi Malaisia panganduse institutsioonide rahapesuriskide hindamisest (Isa, Sanusi, Haniff, & Barnes, 2015). Vastavuskontrolli spetsialist on finantseerimisasutuses töötav isik, kes tegeleb nõuetele mittevastavusest äriühingu riskide hindamise, kindlaksmääramise, nõustamise ja järelevalvega (European Securities and Markets Authority, 2012). Käesoleva bakalaureusetöö intervjuudes küsiti erinevaid küsimusi, mis aitavad autoril sooritada nii teoreetilist, kuid ka empiirilist uuringut. Küsimused oli grupeeritud kolme liiki. Esimeseks liigiks oli RTRT regulatsioonide kohta. Teiseks liigiks oli RTRT panganduse suhtes. Kolmandaks liigiks oli liigitamata küsimused ehk esitati üks poliitiline, teine juriidiline ja kolmas tehnoloogiline küsimus. Küsimused andsid täpsema ülevaate, milliseid regulatsioone pangad kasutavad, milliseid meetmeid pangad kasutavad, kas pangad teevad koostööd rahapesu ennetamisel, kes tegelevad pangas rahapesu ja terrorismi ärahoidmisega ehk milline on pangas struktuur rahapesu ja terrorismi rahastamise tõkestamisega, milliseid võimalusi pakub rahapesu ennetamisel, kuid ka võimalusi kuritegijatele tänapäevane digimaailm ning kiiresti kasvav tehnoloogiaareng ehk e-residentsuse ja krüptovaluutade riskid, kuidas pangad tuvastavad kahtlaseid tehinguid, mis kahju võib rahapesu tuua pankadele või riigile, millised karistused võivad kaasneda kui rahapesu toimub pangas, kas pangad võivad äriliselt võita rahapesust ehk kas riskantsete klientide võtmine, tasub ennast ära?

Antud intervjuu vastuseid kasutatakse järgnevates peatükkides analüüside koostamisel. Intervjuud kestsid keskmiselt 35 minutit 30 sekundit, kus lühim intervjuu kestis 34 minutit ja 48 sekundit ning pikim 36 minutit ja 12 sekundit. Intervjuud transkribeeriti autori poolt (vt Lisa C ja Lisa D). Intervjuudest lähtudes koostas autor *Cross-case* analüüsi ehk horisontaalset analüüsi (vt Lisa E) (Kalmus, Masso, & Linno, 2015).

### 2.1.Ebaefektiivse RTRT-se kahju pankadele

Intervjuudest selgus, et rahapesu on tegevus, kus kuritegelik raha liigutakse läbi pangandussüsteemide, proovides seda legaalseks teha. Pangad ise ei tegele rahapesuga kui just pole kindlaks tehtud, et teatud pangatöötaja on sellega saanud tulu. Rahapesu pankades toob kaasa pankadele negatiivse mõju, kahjustades ka panga mainet, mis on majanduse vereringe ehk ka langetab usaldusväärsust eraklientide, äriklientide, kuid ka aktsionäride vaatenurgast kui tegemist on börsil oleva ettevõttega. See väljendub ka aktsiahindades, kus näiteks samal päeval, kui tuli uudis välja Danske Panga rahapesuskandaalist, kukkus Danske Panka aktsiahind 3%, pikemaajalises perspektiivis oli aktsiahinna kukkumine tunduvalt suurem (Milne, 2018). Aastal 2020 ainuüksi pidid pangad maksma üle 10,4 miljardi USA dollari kahjutasu rahapesu reeglite rikkumise eest (The Economist, 2021). Rahapesust tekkiv mainekahju jääb nii riigile, kuid ka pangale aastateks külge ning seda unustada on väga raske.

> *Keldre: „ (...) Kuna pangad on majanduse vereringe, siis rahapesu laiemalt on majandusele pärssiva mõjuga, kuna nüüd kuritegudes, mis on nagu rahapesu mõte, on kuritegelikul teel saadud tulu üritamine legaliseerida või raha nagu valgeks pesta, et see loob majanduses mõnedele osalejatele ebaõiglase konkurentsieelise.“ (Transkriptsioon SEB panga kontaktisikuga)*

> *Anonüümse panga esindaja: „ (...) Mis juhtus Danske aktsiaga näiteks või mis juhtus Swedbanki aktsiaga, kui need uudised avalikuks said? See väljendub nagu otseselt aktsiahinnas, kui on tegemist avaliku ettevõttega, et aktsionärid saavad, eks ole, aktsionäride vara haihtub.“ (Transkriptsioon anonüümseks sooviva jääva panga kontaktisikuga)*

Rahapesul on ka suuremaid kahjusid peale pankade mainekahju. Eelnevalt sai mainitud, et rahapesu loob kurjategijatele ebaõiglase konkurentsieelise, kuid peale selle on ka teisi faktoreid, mis mõjutab riiki negatiivselt. Rahapesu rikuvad peale finantseerimisasutuse maine ka riigi mainet ja usaldust nendesse – võivad tekkida olukorrad, kus suuremad kokkulepped või välisinvesteeringud jäävad toimumata, kuna riigis olevas pangas on toimunud rahapesuskandaal ja riik paistab silma ebaadekvaatsena regulatsioonide reguleerimisel ja nende täitmise kontrollimisel. Peale ebaõnnestumise reguleerimises ning kontrollimises võivad tekkida ka korruptsioonikahtlused, kuna riik lasi sellistel sündmustel juhtuda – see kõik hävitab usalduse riiki.

*Anonüümse panga esindaja: „ (...) Mingil määral võib see kuidagimoodi mõjutada välisinvesteeringute mahtu, aga noh, ma arvan, et see on pigem niisugune teoreetiline hüpotees (...) Jah, ma arvan, et otsene ja oluline mõju pankade jaoks ongi needsamad seotud isikud, et tippjuhtkond ja seotud otseselt isikud nende isikute personaalvastutusega ikkagi täiesti olemas ja, ja Eestis on nii, et kui, kui sinu suhtes on ikkagi algatatud juba kriminaalmenetlused, siis sa enam edaspidi kontroll funktsioonidel ja juhtivatel kohtadel finantssüsteemis töötada ei saa, et see on tuleviku jaoks välistus.“ (Transkriptsioon anonüümseks sooviva jääva panga kontaktisikuga)*

Eesti riigil on olnud kogemus rahapesuga pankades, nii Danske Pangas, kui ka Swedbank-ga oma. Danske Panka kajastati põhjalikult meediakanalites, ka Swedbank oli osaline rahapesus, kuid Swedbanki ei kajastatud meedias niimoodi nagu Danske Panka rahapesu ja see hoidis Swedbanki mainekahjust ning usalduse kaotamisest.

*Keldre: „ (...) Skandaale on olnud, kindlasti me oleme nendest skandaalidest ka õppinud võib olla tänu nende skandaalidele ka Eesti pangad on mõnevõrra rohkem panustanud rahapesu tõkestamiseks kui meie kolleegid üle piiri.“ (Transkriptsioon SEB panga kontaktisikuga)*

*Anonüümse panga esindaja: „ (...) Esiteks on ühtepidi Eesti asukoht kaardil on nagu väga halb, et me jääme alati lääne-idapiirile ehk et see kuritegelik raha vist nagu ida poolt üritab tulla, et see, see üritab ikkagi siseneda Euroopa pangandussüsteemide läbi nende piiririikide, et see risk on nagu alati olemas. Teistpidi Eesti on hästi läbipaistev (...) suuremaid summad, mis on kuritegelikul teel teenitud läbi finantssüsteemi juhtida ja, ja kui nad suurenevad, summad hakkavad liikuma läbi väikese finantssüsteemi nagu Eesti on või siis paratamatult hakkab silma ja tekitab küsimusi, et miks see nii on.“ (Transkriptsioon anonüümseks sooviva jääva panga kontaktisikuga)*

Pankade vahel puudub otsene kliendiandmete jagamise õigus, kuna see on keelatud vastavalt isikuandmete seadusele, kuid kui tegemist on kahtlaste tehingutega, siis antakse pangale võimalus jagada andmeid teiste pankadega (Euroopa Andmekaitsenõukogu, 2020). Isikuandmete kaitse on oluline, kuid vahel võib olla erandite tegemine vajalik, et ära hoida

kuritegevust, antud juhul rahapesu ja terrorismi rahastamist, mis võib nii riigile ja seega ka kodanikele tunduvalt halvemate tagajärgedega kui isikuandmete käsitlemine.

> *Anonüümse panga esindaja: „ (...) Eestis meil on natuke üle aasta tegutsenud selline suurepärane vahetusplatvorme, mille on arendanud välja kohalik startup, Salv (...) Salv on selline platvorm nagu bridge. Ja tegelikult selle alusel pangad vahetavad infot küsivadki (...) et kontol on toimunud mingi tehing mis on tulnud mingisugust teisest pangast, tehing tekitab küsimusi, et selle platvormi asele platvormi kaudu on võimalik siis pankadel omavahel suhelda, et pank üks saab pank kahelt küsida, et, et me saime, nägime sellist tehingut, raha tuli sinu pangast, et palun selgita, mis sa selle kliendi kohta teavad, milline on nagu kogu aeg kogemus olnud, milliseid riske sa näed, et selles mõttes selline info vahel siis täitsa toimib.“ (Transkriptsioon anonüümseks sooviva jääva panga kontaktisikuga)*

Pangal on võimalik teenida kasumit, kui pangas toimuvad ebaseaduslikud tehingud. Sellisel juhul finantsmahud suurenevad ning pank teenib selle pealt tulu. Ometi peab arvestama sellega, et mainerisk ning trahvid võivad olla tunduvalt kulukamad võrreldes selle tuluga, mida pank teenib ebaseaduslike tehingute pealt.

> *Anonüümse panga esindaja: „ (...) See on sihuke lühiajaline benefit, et täna läheb hästi, aga kuid tegevus jõuab nagu riigiasutuste uurimisasutuste uurimisorbiiti, siis, siis see on läinud, sa kaotad tegelikult oluliselt rohkem.“ (Transkriptsioon anonüümseks sooviva jääva panga kontaktisikuga)*

Rahapesu tagajärjel mõjutab see peale panga, kes võib saada suured trahvid, kaotada oma litsentsi, ka tippjuhtkonda ning otseselt seotud isikuid ja nende vastu võidakse esitada kriminaalmenetlused, millele järgnevad trahvid või vanglakaristus. Samuti võib see hävitada töötaja karjääri – kui töötaja vastu on algatatud kriminaalmenetlus, siis tulevikus antud töötaja ei saa töötada finantssüsteemi ettevõttete kontrollfunktsioonidel ning üleüldiselt kõrgetel juhtivatel positsioonidel.

> *Keldre: „ (...) Nii pangana juriidilise isikuna kui panga juhtkonnale kui pangatöötajatele, kes rahapesu tõkestamise eest vastutavad on, saab vastutusele võtta*

*nii väärteomenetluse kui kriminaalkorras.“ (Transkriptsioon SEB panga kontaktisikuga)*

Globaalne digitaliseerimine on avanud uue maailma pettustele. Kurjategijatel on interneti kaudu tekkinud palju uusi võimalusi kuritegude sooritamiseks nagu näiteks pettuste, võltsimise või rahapesu sooritamisel. Kriminaalselt teenitud raha seaduslikuks muutmine läbi internetipanganduse on suurimaid ohukohti rahapesu ja terrorismi rahastamise tõkestamisel juba 2000.aastail (Financial Action Task Force, 2008). Praegusel ajal on pettuste, võltsimise ja rahapesu sooritamine tehtud kurjategijatele raskeks, sest pangad on kohustatud järgima Eesti Vabariigi ja Euroopa Liidu regulatsioone, juhendeid ja soovitusi.

*Keldre: „ (...) Digimaailm on muutnud seda, kuidas kuritegevus toimib ja lisades sinna ka täiesti uusi kuriteoliike või noh ka viimasest ajast võtta siin kas või näiteks kõikvõimalikke pettusid ja pangapettusid või investeerimis petuskeeme ja nii edasi, et siis ka sealt saadav raha pettuse teel, kelmuse teel saadud raha, et mis vajab puhtaks pesemist.“ (Transkriptsioon SEB panga kontaktisikuga)*

Rahapesu on kuritegelik tegevus, kus eesmärgiks on muuta ebaseaduslik raha läbi pangandussüsteemi legaalseks. Pangad kogevad sellest negatiivseid tagajärgi, mõjutades pankade mainet ja usaldusväärsust eraklientide, äriklientide ja aktsionäride silmis.

Rahapesu on laialt levinud probleem, millest tulenevad kahjud on märkimisväärsed, näidates vajadust tõhusate ennetusmeetmete ja järelevalve järele. Rahapesu mõjutab negatiivselt mitte ainult panku, vaid ka majandust tervikuna, luues ebaõiglase konkurentsieelise kuritegelikult saadud tulude seaduslikuks muutmisel.

Rahapesul on mitmekülgsed kahjulikud tagajärjed, ulatudes pankade mainekahjustustest kuni riigi maine ja usalduse halvenemiseni, mis võib takistada suuremaid kokkuleppeid ja välisinvesteeringuid ning tekitada kahtlusi korruptsioonis. Intervjuus tunnistas SEB kontaktisik, et skandaalidest õpiti ning Eesti pangad on rohkem investeerinud rahapesu tõkestamisse kui välismaised kolleegid. Anonüümse panga esindaja märkis, et Eesti asukoht ja läbipaistvus võivad muuta riigi atraktiivseks kuritegeliku raha sissemurdmiseks Euroopa pangandussüsteemi.

Anonüümse panga esindaja toob välja Eesti startupi Salv arendatud platvormi, mis võimaldab pankadel vahetada infot kahtlaste tehingute kohta, rõhutades suhtluse olulisust riskide hindamisel.

Ebaseaduslikud tehingud võivad pankadele lühiajaliselt kasumlikud olla, tuleb arvestada pikaajaliste riskidega, sealhulgas mainekahjustuse ja võimalike trahvidega, mis võivad negatiivselt mõjutada panga tulevikku ja finantsseisu, seetõttu on finantseerimisasutustele järgida õigusakte.

Rahapesu võib põhjustada mitmekülgsed tagajärjed, hõlmates panga suuri trahve, litsentsikaotust, juhtkonna karistamist ning otseste osaliste, sealhulgas töötajate, kriminaalmenetlusi koos võimalike trahvide või vanglakaristustega, kahjustades samal ajal nende tulevikuvõimalusi finantssüsteemi ettevõtetes ja kõrgematel juhtivatel positsioonidel.

Globaalne digitaliseerimine on avanud kurjategijatele uusi võimalusi kuritegude, sealhulgas pettuste, võltsimise ja rahapesu sooritamiseks, kuid tänapäeval on pangad kohustatud järgima rangelt regulatsioone ja juhendeid, mis muudab kuritegevuse raskeks. SEB panga kontaktisiku sõnul on digimaailm muutnud kuritegevust ning kelmuse teel saadud raha puhtaks pesemine on endiselt oluline probleem.

### 2.2. RTRT Eesti pankades

Pankades on loodud meeskonnad, kes tegelevad rahapesu ja terrorismi ärahoidmise eest. Intervjuud andsid ülevaate, et mitte ainult spetsiaalsed meeskonnad ei tegele rahapesu ja terrorismi rahastamise tõkestamisega, vaid seda teevad kõik pangatöötajad. Näiteks klienditeenindajad ja kliendihaldurid tegelevad kliendiandmetega ja nende valideerimisega – neil on esmane kontakt kliendiga ja nende õige tähelepanu võib ära hoida rahapesu ning terrorismi rahastamist, seepärast nad võivad kanda isegi kõige olulisemat rolli rahapesu ja terrorismi rahastamise tõkestamisel.

> *Keldre: „ (...) Vähemal või rohkemal määral tegelenud sellega kõik pangatöötajad eks, sest mis on nagu oluline eriti pankade puhul või kõige teiste turuosaliste puhul, mis on nagu oluline kriteerium rahapesu tõkestamine on „tunne oma klienti“ meetmete rakendamine või oma kliendi parim tundmine, et selles mõttes siin on suur roll eesliinil, kliendihalduritel, nõustajatel kontoris, kes otseselt klienti teenindavad, kes otseselt kliendiga suhtlevad.“ (Transkriptsioon SEB panga kontaktisikuga)*

> *Anonüümse panga esindaja: „(...) Esimese kaitseliin (...) tegelevad sellise perioodilise kliendi ülevaatusega võtavad noh, nagu ütlesin näiteks kõrge riskiga klientide puhul kord aastas ette kogu kliendi andmestikku kogu kliendi ärivõrgustiku pagasi [uuendamine](...) Teise kaitseliini profiil on natukene sarnane, et noh, seal on samamoodi selliseid uurija profiiliga inimesed. Kes päeva lõpuks otsustavad, eks ole,*

*et kas kas mingisugune kahtlase tehingu teatis tuleb endast rahapesu andmebüroole või mitte (...) Ja auditis, kolmas kaitseliin, noh nagu nagu audiitorid ikka, et ega nendel on pigem selline homogeensem profiil, et normidele nõuetele vastavuse hindamine oleks kõik kõik kolm kaitseliini.“ (Transkriptsioon anonüümseks sooviva jääva panga kontaktisikuga)*

Pangad on ajaga aina rohkem automatiseerimise poole liikumas. Automatiseerimine on programmi loomine, mis tuvastab kliendikäitumise ning sealt leiab ülesse kahtlaseid tehinguid. Automatiseeritud süsteemid suudavad kiiresti ja täpselt analüüsida suuri andmemahtusid, võimaldades pankadel ja finantseerimisasutustel tuvastada mustreid ja kõrvalekaldeid, mis võivad viidata rahapesule. See võib hõlmata tehinguandmete ja klienditeabe, et tuvastada võimalikke riske. Automatiseeritud süsteemid suudavad jälgida klientide käitumist reaalaja jooksul, võimaldades pankadel tuvastada ebatavalise või kahtlase tegevuse võimalikult kiiresti, näiteks kui klient hakkab ootamatult tegema suuri tehinguid või kasutama uut kontot, võib automatiseeritud süsteem märgistada selle potentsiaalselt kahtlasena ja hoiatada pangatöötajaid edasiseks uurimiseks. Samuti kui automatiseeritud süsteem märkab, et kliendi andmed võivad olla väärad. Automatiseeritud protsessid aitavad pankadel kliendi identiteeti kontrollida ja võimalikke riske hinnata. (Baader & Krcmar, 2018) Paljud pangad kasutavad automatiseeritud süsteeme, ometi pankade kontaktisikud on öelnud need pole senimaani olnud väga efektiivsed ning vajavad arendamist. Pangad kasutavad hetkel eelkõige automatiseerimist kliendiandmete kogumiseks ja uuendamiseks, kuid pangad on ka huvitatud tulevikus võimalikult palju automatiseeritusele üleminekuks.

*Keldre: „ (...) automatiseerimine kui selline või see alati kliendi riskihindamisest kuni nende klienditegevuste jälgimiseni, seal see on väga selline andmetel põhinev protsess, et andmete kogumine, töötlemine, analüüsimine seal sellist automatiseeritud on samamoodi üha rohkem juurde tulemas.“ (Transkriptsioon SEB panga kontaktisikuga)*

Peale kahtlaste tehingute tunnuste, tuleb pangal jälgida, mis toimub kliendi kontol ehk vastavalt kliendi konto profiili alusel saab kahtlaseid tehinguid paremini hinnata. Seda nii pettuste osas, kuid ka rahapesu ja terrorismi rahastamise osas. Suur roll on täita pankadel, kes peavad hoolikalt läbi vaatama, keda juriidilisest- või eraisikutest nad lubavad oma panka arveldama ning jälgima, et kliendi kontol ei toimu „kahtlased tehingud“.

*Keldre: „ (...) kindlasti on maht [oluline näitaja], aga see kui ütleme tehingu summa, aga siin ei saa vaadata ka ühte tehingu summat või jääda kinni sellesse ühe tehingu summasse (...) Sõltuvad väga palju kui kõrgeks klientidele on meie kliendirisk hinnatud ja mis on need põhjused, miks me seda riski oleme nii kõrgeks hinnanud (...) osades suuremate kohalike omavalitsuste juhtorgani liige niinimetatud riikliku taustaga isik ehk PEP, siis tema puhul on need markerid või on need kriteeriumid, mida maksetes otsida, tänu põhilisele riskile, mis on korruptsioonirisk, on mõnevõrra erinevad, kui me räägime näiteks terrorismi rahastamisest. (...) Terrorismi rahastamine võib endas tähendada ka seda korjatakse kokku väga väikestes summades raha või siis nagu isikute panuseid selleks, et seda terrorist või terroriakti siis nagu organiseerida seda terrorismi toetada.“ (Transkriptsioon SEB panga kontaktisikuga)*

*Anonüümse panga esindaja: „Kahtlaste tehingute tuvastamiseks on kõige parem dokument rahapesu andmebüroo kahtlaste tehingute tunnuste juhend, kus on kahtlased tunnused välja toodud mingil määral on lahti kirjeldatud ka Finantsinspektsiooni põhi AML juhendis selles põhijuhendis lisades, õigemini punaste lippude, noh aga need on kaks põhilist sellist allikat ega pangad midagi võib-olla kirjutavad ka ise täpsemaks, aga ütleme, need mõlemad viidatud suunised on nagu piisavalt mahukad.“ (Transkriptsioon anonüümseks sooviva jääva panga kontaktisikuga)*

Rahapesu ja terrorismi efektiivseks tõkestamiseks on riik, kuid ka Euroopa Liit loonud erinevaid seaduseid, juhendeid ning direktiive. Eestis üks enimkasutatuim on rahapesu ja terrorismi rahastamise tõkestamise seadus ja Euroopa Liidu direktiivide seas neljas direktiiv. Rahvusvaheliselt on kõige tuntum on FATF (*Financial Action Task Force*) ehk PAP, kes annab pankadele üldiseid soovitusi, konkreetsete klientide põhiseid, kuid ka sektoripõhiseid soovitusi. Rahapesu Andmebüroo on välja andnud dokumendi, kus antakse soovitusi pankadele riski juhtimise ja hoolsusmeetmete kohta. Riskiisu määramise ehk kui palju ja millise taustaga isikuid pank võtab endale kliendiks, riskiprofiili loomine klientide suhtes ning milliseid hoolsusmeetmeid kasutada keerulistes osades on osa Rahapesu Andmebüroo mahukas juhendis. Peamisteks soovitusteks on teada saada, kellega finantseerimisasutused ärisuhtesse astuvad, kontrollida nende põhjuseid ja vajadusel sekkuda

kui märgatakse, et toimub ebaharilik tegevus, mis ei vasta kliendi profiilile või tekib kahtlus, et klient on oma esitatud andmetes valetanud. (Rahapesu Andmebüroo, 2022) Pankadele on kasuks tulnud ka Finantsinspektsiooni ehk pankade järelvalvaja soovituslik juhend, kus ettepanekud muudavad rahapesu jälitamise efektiivseks – olgugi, et tegemist on soovitusliku juhendit, kuid kui pangad neid ettepanekuid ei jälgi, siis finantseerimisasutused peavad aru andma, miks nad seda ei tee.

> *Keldre: „ (...) Võib-olla, mis nüüd meie või Eesti pankade tegevust kõige otsesemalt mõjutavad, on Euroopa direktiivid, kus me täna oleme jõudnud juba kuuenda direktiivi arutelu juurde, et kõige nagu kõige suurema mõjuga viimastest aegadest oli neljas direktiiv.“ (Transkriptsioon SEB panga kontaktisikuga)*

> *Anonüümse panga esindaja: „Pankades on ülesse ehitatud keerukas hoolsusmeetmete riskijuhtimise süsteem, et pankades täpsemalt neid nõudeid edastab, kirjeldab lahti Finantsinspektsiooni soovituslik juhend. Aga ütleme, oluline on see, et kontrollmeetmed on ja ütleme ka kontrollmeetmete rakendamine ja ütleme siis kontrolli nende meetmete rakendamise üle, et see on nagu mõistlikult optimaalselt laiali jagatud erinevate struktuuriüksuste lõikes ja seda kutsutakse siis kolme kaitseliinipõhiseks lähenemiseks.“ (Transkriptsioon anonüümseks sooviva jääva panga kontaktisikuga)*

Pangad kasutavad *KYC* metoodikat, et hinnata kliendiriske. Osad pangad peavad seda tugisambaks kliendiriskide hindamisel, kuna see annab turuosalistele hea raamistiku ning riskifaktorid. Negatiivseks kohaks *KYC* protseduuris võib jääda see, et klient võib tunda ennast ülekoormatuna kui klientidelt hakatakse lisaküsimusi küsima. „Tunne oma klienti“ protseduur seisneb kliendi andmete kogumises, valideerimises, vara päritolu selgitamises ja rikkuse päritolu tuvastamises. KYC andmeteks, mida pangad koguvad on: a) Tegevusala ehk finantseerimisasutus peab mõistma, millega klient majanduslikul tasemel tegeleb ning mis on selle riskitase; b) Maksetavad ehk pank peab välja uurima, kas ning millistel põhjustel ja tingimustel klient tehinguid teeb ja kuidas see kooskõlastub kliendi profiiliga, millest saab hinnata kliendiriske; c) olulisemaid partnerid ehk finantseerimisasutus peab välja selgitama, mis partneritega klient tehinguid teeb tuvastama partnerite riskid (Rahapesu Andmebüroo, 2022).

*Keldre: „ “Tunne oma klienti“ metoodika või nagu protsessi tugevus on see, et see võimaldab seda klienti rahapesu riski palju adekvaatsem adekvaatsemalt ja detailsemalt hinnata, kogu mõte „tunne oma klienti“ protsessi mõte ongi see, et me saame aru, kes see klient on, miks ta tahab just meiega äri teha.“ (Transkriptsioon SEB panga kontaktisikuga)*

Pangad peavad rahapesu tõkestamiseks kasutama valitsuse regulatsioone. Finantssektor on rahapesurite peamine sihtmärk ja pangad peavad selle ohuga võitlemiseks tegema tihedat koostööd valitsusasutustega. Valitsuse ette antud juhised annavad pankadele raamistiku, mida rahapesu tõkestamiseks järgida. Need eeskirjad sisaldavad konkreetseid juhised ja eeskirjasid, mida pangad peavad kahtlase tegevuse tuvastamiseks ja sellest teatamiseks järgima. Pankade ja valitsusasutuste vahelise informatsiooni jagamine on eriti oluline. Pangad peavad kahtlasest tegevusest vastavatele asutustele teatamisel olema kiired, et saavutada võimalik kõrge efektiivsus tõkestamisele. (Federal Financial Institutions Examination Council , 2021) Eesti riik on seadnud kindlad regulatsioonid pankadele rahapesu ja terrorismi rahastamise tõkestamise osas, kuid peale selle on Eesti riik esitanud ka soovituslike juhendeid, mida paljud pangad aktiivselt kasutavad. Suurim erinevus pankade vahel on riskiisu ehk kuivõrd suure riskiga kliente lubatakse oma panka.

*Keldre: „ (...) iga pank defineerib ära millisesse klientidega tema ja seda ma mõtlen siis nii-öelda kui rahapesu riski mõttes, et ühelgi pangal ei ole tõenäoliselt riskiisu rahapesu osas, et vot ma tahaks nii palju pesta, seda, mitte onju, et pigem klientide riskisuse osas.“ (Transkriptsioon SEB panga kontaktisikuga)*

*Anonüümse panga esindaja: „ (...) Nõuded põhimõtteliselt kõigile samasugused (...) aga noh, see, kuidas rakendad neid, kuidas iga pank seaduse nõuetest aru saab, see on tõesti erinev.“ (Transkriptsioon anonüümseks sooviva jääva panga kontaktisikuga)*

Rahapesu kahtluse korral hakkavad pangatöötajad kahtlasi tehinguid uurima, võtavad kliendiga ühendust ning küsi küsimusi kahtlaste tehingute kohta ja vajadusel teavitavad rahapesu toimumise riskist Rahapesu Andmebürood.

*Keldre: (...) kui tuleb meile uus ettevõte, tahab kliendiks saada, siis me teeme kindlaks tema omandistruktuuri ja kes siis on need isikud, kes mõtlen, et eraisikute füüsilisi*

*isikuid, kes me peame lõplikult seda ettevõtted omavad või sellest ettevõttest kasu saavad. Ja nende kohta me, me tahame ka kokku koguda andmeid, et siis saad aru, mis on nende isikute varasem kogemus.“ (Transkriptsioon SEB panga kontaktisikuga)*

Krüptoraha on toonud rahapesemisele uued võimalused. Rahvusvaheline Valuutafond peab krüptovaluutat kõige suurimaks ohuks rahapesus (International Monetary Fund, 2023). Pangad peavad välja töötama tugevad rahapesu tõkestamise regulatsioone, mis käsitlevad krüptovaluutadega seotud spetsiifilisi riske. Üks väljakutsetest, millega pangad silmitsi seisavad, on krüptovaluutatehingute läbipaistvuse puudumine. Krüptovaluutad töötavad detsentraliseeritud võrkudes ehk pilvepõhises keskkonnas, mille suhtes ei kohaldata samasugust regulatiivset järelevalvet nagu traditsioonilistes finantssüsteemides - see muudab pankadel kahtlase tegevuse tuvastamise ja sellest teatamise keeruliseks. Teine väljakutse on krüptovaluutatehingute anonüümsus. Paljud krüptovaluutad võimaldavad kasutajatel jääda anonüümseks, mistõttu on pankadel keeruline tehinguga seotud osapooli tuvastada. (Lemire, 2022). See kõik muudab krüptovaluutaga tegelemise pankadele väga riskantseks ning pangad peavad leidma viise, kuidas minimaliseerida neid riske. Eesti panganduse suhtes see ei ole hetkel veel ohuallikas, sest Eesti pangad ei ole kasutusele võtnud krüptovaluutat, välja arvatud LHV pank. LHV pank on hoidnud selles oma riskid minimaalsena, pakkudes ainult ostu ja müümis võimalust. Tulevikuperspektiivis, kui rohkem Eesti panku hakkab pakkuma oma klientidele krüptovaluuta võimalusi, võib see ohukohaks tulla ka Eestile kui Euroopa Liit ei otsusta veelgi rohkem reguleerida krüptovaluutat, mis kaotaks ära krüptovaluuta erilise omaduse – anonüümsuse. Reguleerides krüptovaluutat on ka Eesti pankadel võimalus hakata oma klientidele pakkuma krüptovaluutat.

*Anonüümse panga esindaja: „(...) Krüpto on hetkel jah, mõnevõrra vähem reguleeritud, eks ole, kui nii-öelda tavapärane raha maksevahendina. Aga krüptoga seonduvalt ka, et Euroopa Liit on järgmine aasta jõustamasi uut direktiivi, MiCa direktiiv (...), et sellega seonduvalt tegelikult pannakse peale krüpto vahendamisele päris karmid nõuded. Et sisuliselt noh, võib öelda seda, et selline anonüümsus kui selline järgmise pooleteise kahe aasta jooksul kaob ära, mis siiamaani andis nagu eelise rahapesijad, et hetkel selline jah, eelis on veel olemas, aga ka see pigem on nagu kadumas.“ (Transkriptsioon anonüümseks sooviva jääva panga kontaktisikuga)*

Rahapesu ja terrorismi rahastamise tõkestamisega kaasneb suur vastutus nii riigile, kuid ka pangale endale – on mõlema parimates huvides rahapesu toimumise riske minimaliseerida. Rahapesu on Eesti riigis põhjalikult reguleeritud. Pankadele on antud ette kindlad juhised, kuidas tuvastada rahapesu ja terrorismi rahastamise ohtu, kuidas seda ohtu minimaliseerida ning kuidas tuvastada kahtlaseid tehinguid. Ainukene osapool, kes saab kontrollida turvalise pangandussüsteemi on pangad ise, vastavalt enda riskiisule.

Eesti on olnud viimastel aastatel rahapesuskandaalide keskel, kuid on näha, et antud skandaalidest on õpitud ning on hakatud regulatsioone tõsisemalt ning rangemalt käsitlema.

Eestis on kasutusel mitmed erinevad regulatsioonid rahapesu tõkestamiseks, selleks on rahapesu ja terrorismi rahastamise tõkestamise seadus, Euroopa Liidu poolt välja antud direktiivid, Finantsinspektsiooni soovituslik juhend „Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks“, kolme kaitseliini mudel, riigikogu seadused, hoolsusmeetmete riski juhtimise süsteem ning rahvusvaheliselt *Financial Action Task Force*, kust pangad saavad ka soovitusi.

Koostööd saab pidada üheks olulisimaks viisiks, kuidas tagada minimaalne rahapesu ja terrorismi rahastamine. Olgugi, et andmekaitseseadusega on minimaliseeritud koostöö pankade vahel, on neli Eesti suurimat panka leidnud legaalse võimaluse, kuidas pangad saavad üheskoos hinnata paremini kahtlaseid tehinguid ning seal edasi tuvastada rahapesuakte.

Digimaailm on pakub ohte, kuid ka võimalusi rahapesuga seoses. Ohtudeks on petmised ning uued tegevusvaldkonnad ning tööstusharud, kuigi viimast saaks pidada ka digimaailma võimaluseks. Rahapesu ja terrorismi rahastamist saab tõkestada luues automatiseeritud süsteeme, mis tuvastavad efektiivsemalt ja kiiremini kahtlaseid tehinguid.

Vastavalt leitud empiirilistele uuringutele ning läbi viidud uuringutele peab autor Eestis olevat rahapesu ja terrorismi rahastamise tõkestamist edukalt koordineerituks kui jätkatakse tehnoloogiliste viiside abil kahtlaste tehingute tuvastamist, rahapesu ja terrorismi rahastamise tõkestamise regulatsioonide edasiarendamist nii pankade, riigi, kuid ka suuremate institutsioonide poolt.

## Kokkuvõte

Käesoleva bakalaureusetöö koosneb teoreetilisest osast ja empiirilisest osast. Bakalaureusetöö eesmärgiks oli välja selgitada, milliseid rahapesu ja terrorismi rahastamise tõkestamise regulatsioone ja meetmeid pangad kasutavad.

Töö sisuline osa koosneb kahest peatükist, mis on liigendatud alapeatükkideks. Teoreetilise osa alapeatükkideks on rahapesu ja terrorismi rahastamise tõkestamise mõiste,

liigid ja tähtsus ning rahapesu ja terrorismi rahastamise tuvastamise regulatsioonid. Empiirilise osas viis autor läbi süvaintervjuu Eesti suurpankade kontaktisikutega, et saada täpsemat informatsiooni, kuidas pangad antud regulatsioone järgivad. Empiirilise osa alapeatükkideks on rahapesust tulenev kahju ja rahapesu ja terrorismi rahastamise tõkestamine panga ning riigi tasandil.

Teoreetilise poole esimene alapeatükk selgitab, mis on rahapesu ja terrorismi rahastamise tõkestamine, mis regulatsioone pangad järgivad ja miks on rahapesu ja terrorismi tõkestamine oluline.

Teoreetilise poole teine alapeatükk selgitab, kuidas tuvastatakse rahapesu ja milliseid meetmeid pangad järgivad, et ära hoida rahapesu ja terrorismi rahastamine.

Empiirilise poole esimene alapeatükk kasutab süvaintervjuust kontaktisikutelt saadud informatsiooni, et selgitada, milliseid kahjusid võib rahapesemine tekitada.

Empiirilise poole teine alapeatükk selgitab rahapesu ja terrorismi rahastamise regulatsioone pankades, kasutades süvaintervjuust Eesti suurpankade kontaktisikutelt saadud informatsiooni.

Teaduslikest artiklitest, peamiselt tuli *ScienceDirect*'i ja *Google Scholar*'i, välja kui oluline on rahapesu ja terrorismi rahastamise tõkestamine nii riigile, kuid ka finantseerimisasutustele. Suutmatus rahapesu ja terrorismi rahastamist reguleerida toob kaasa kuriteo kasvu, vähendab riigile eelarvet nii: kuritegevuse suurenemise ja vähesema maksude laekumise tõttu. Samuti ka mõjutab negatiivselt riigi majandusnäitajaid - mis kõik omakorda mõjutavad nii majandust kui ka kodanike heaolu.

Juriidilistest dokumentidest ehk Euroopa Liidu direktiividest, Riigikogu riiklikest seadustest, Finantsinspektsiooni juhenditest ning Rahapesu Andmebüroo juhenditest selgus, et pankadel on suur vastutas tagada, et pankades ei juhtuks rahapesu ja terrorismi rahastamist. Rahapesu ja terrorismi rahastamise tõkestamise üks suurimaid raskuseid pankadele on vähese informatsiooni omamine ehk vastavalt Euroopa Liidu andmekaitse direktiivile, peavad olema isikuandmed kaitstud ning neid antakse välja ainult hädavajalikel juhtumitel. Vähese informatsiooniga on pankadel keeruline leida kahtlaseid tehinguid, mis viitavad rahapesu ja terrorismi rahastamisele.

Läbiviidud süvaintervjuust erinevate Eesti suurpankade kontaktisikutega tuli välja, et pankades võib esineda rahapesu ja terrorismi rahastamise juhtumid kui pangad võtavad vastu kõrge riskiga kliente, töötajaid aktiivselt ei koolitata ning vähene informatsioon klientide osas. Pankadele on loodud kindlad regulatsioonid ja juhendid, kuid pankadel on vabadus ise

otsustada, kuidas nad neid rakendavad, mille tõttu osades pankades on võimalus olla ühenduses rahapesu ja terrorismi rahastamisega suurem kui teistes finantseerimisasutustes.

**Viidatud allikad**

1. Anonüümne. (21. detsember 2022. a.). Transkriptsioon anonüümseks sooviva panga kontaktisikuga. (E. Lillemaa, Intervjueerija)
2. Baader, G., & Krcmar, H. (detsember 2018. a.). Reducing false positives in fraud detection: Combining the red flag approach with process mining. International Journal of Accounting Information Systems, lk 1-3, 12-13. (kasutamise kuupäev 13.01.2024)
3. Balsa, J., & Alexandre, C. (22. jaanuar 2018. a.). A Multi-Agent System Based Approach to FightFinancial Fraud: An Application to MoneyLaundering. Allikas: reasearchgate.net: https://www.researchgate.net/publication/322652154_A_Multi-Agent_System_Based_Approach_to_Fight_Financial_Fraud_An_Application_to_Money_Laundering (kasutamise kuupäev 20.01.2023)
4. Busetto, F., Gardó, S., & Klaus, B. (november 2019. a.). Implications of bank misconduct costs for bank equity returns and valuations. Allikas: ecb.europa.eu: https://www.ecb.europa.eu/pub/financial-stability/fsr/focus/2019/html/ecb.fsrbox201911_03~511ae02cc5.en.html (kasutamise kuupäev 22.01.2023)
5. Ciphertrace. (2018). Cryptocurrency Anti-Money Laundering Report. Allikas: ciphertrace.com: https://ciphertrace.com/wp-content/uploads/2019/01/crypto_aml_report_2018q3.pdf (kasutamise kuupäev 20.01.2023)
6. Council of Europe. (8. november 1990. a.). Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime. Allikas: www.coe.int: https://rm.coe.int/168007bd23 (kasutamise kuupäev 13.01.2024)
7. Danske Bank. (kuupäev puudub). Resolution in terms of the Estonia matter. Allikas: danskebank.com: https://danskebank.com/about-us/corporate-governance/resolution-in-terms-of-the-estonia-matter (kasutamise kuupäev 4.01.2023)
8. Eesti Pangaliit. (kuupäev puudub). Rahapesu ja terrorismi rahastamise tõkestamise ning finantssanktsioonide rakendamise poliitika ja suunised. Allikas: www.pangaliit.ee: https://www.pangaliit.ee/rahapesu-tokestamine/hoolsusmeetmed (kasutamise kuupäev 6.01.2024)
9. Eesti Pangaliit. (kuupäev puudub). Rahapesu ja terrorismi tõkestamine. Allikas: pangaliit.ee: https://www.pangaliit.ee/rahapesu-tokestamine (kasutamise kuupäev 3.01.2024)

10. Euroopa Andmekaitsenõukogu. (15. detsember 2020. a.). Avaldus rahapesu ja terrorismi rahastamise tõkestamisega seoses töödeldavate isikuandmete kaitse kohta. Allikas: europa.eu: https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_20201215_aml_actionplan_et.pdf (kasutamise kuupäev 10.05.2023)
11. Euroopa Liidu Teataja. (30. mai 2018. a.). EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV (EL) 2018/843. Allikas: www.europa.eu: https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32018L0843&qid=1607943852053&from=EN (kasutamise kuupäev 23.12.2023)
12. European Securities and Markets Authority. (25. juuni 2012. a.). Suunised finantsinstrumentide turgude direktiivis (MiFID) sätestatud vastavuskontrolli funktsiooni käsitlevate nõuete teatud aspektide kohta. Allikas: www.fi.ee: https://www.fi.ee/sites/default/files/2018-08/0finantsinstrumentide_turgude_direktiivis_MiFID_satestatud_vastavuskontrolli_funktsiooni_kasitlevate_nouete_teatud_aspektide_kohta.pdf (kasutamise kuupäev 3.01.2024)
13. Federal Financial Institutions Examination Council . (november 2021. a.). Bank Secrecy Act/ Anti-Money Laundering Examination Manual . Allikas: gettechnicalinc.com: https://gettechnicalinc.com/wp-content/uploads/2021/12/2021-FFIEC-BSA-AML-Exam-Manual-NOVEMBER-Updates.pdf (kasutamise kuupäev 18.01.2023)
14. Federation of European Risk Management Associations. (27. september 2011. a.). Audit and Risk Committees News from EU Legislation and Best Practices. Allikas: ferma.eu: https://www.ferma.eu/app/uploads/2019/02/eciia_ferma_brochure_v8.pdf (kasutamise kuupäev 18.01.2023)
15. Financial Action Task Force. (18. juuni 2008. a.). Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems. Allikas: www.fatf-gafi.org: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Moneylaunderingterroristfinancingvulnerabilitiesofcommercialwebsitesandinternetpaymentsystems.html (kasutamise kuupäev 26.12.2023)
16. Finantsinspektsioon. (november 2018. a.). Finantsinspektsiooni soovituslik juhend „Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks“. Allikas: fi.ee:

https://www.fi.ee/sites/default/files/2018-11/FI_AML_Soovituslik_juhend.pdf (kasutamise kuupäev 13.01.2024)

17. International Monetary Fund. (4. september 2023. a.). Money Laundering Poses a Risk to Financial Sector Stability. Allikas: imf.org: https://www.imf.org/en/Blogs/Articles/2023/09/04/money-laundering-poses-a-risk-to-financial-sector-stability (kasutamise kuupäev 13.01.2024)
18. International Monetary Fund. (september 2023. a.). Nordic-Baltic Technical Assistance Project Financial Flows Analysis, AML/CFT Supervision, and Financial Stability. Allikas: www.imf.org: https://www.imf.org/-/media/Files/Publications/CR/2023/English/1EUREA2023003.ashx (kasutamise kuupäev 13.01.2024)
19. Isa, Y. M., Sanusi, Z. M., Haniff, M. N., & Barnes, P. A. (28. oktoober 2015. a.). Money Laundering Risk: From the Bankers' and Regulators Perspectives. Allikas: www.sciencedirect.com: https://www.sciencedirect.com/science/article/pii/S2212567115010758 (kasutamise kuupäev 4.01.2024)
20. KPMG. (jaanuar 2022. a.). Anti-Money Laundering/Financing Terrorism Compliance Risk Rating: A Data Science Approach . Allikas: www.kpmg.com: https://assets.kpmg.com/content/dam/kpmg/ae/pdf-2021/11/anti-money-laundering-financing-terrorism-compliance-risk-rating.pdf (kasutamise kuupäev 5.01.2023)
21. Kalmus, V., Masso, A., & Linno, M. (2015). Kvalitatiivne sisuanalüüs. Allikas: samm.ut.ee: https://samm.ut.ee/kvalitatiivne-sisuanalyys (kasutamise kuupäev 11.11.2023)
22. Keldre, K. (14. detsember 2021. a.). Transkriptsioon SEB panga kontaktisikuga. (E. Lillemaa, Intervjueerija)
23. Lemire, K. A. (26. september 2022. a.). Cryptocurrency and anti-money laundering enforcement. Allikas: reuters.com: https://www.reuters.com/legal/transactional/cryptocurrency-anti-money-laundering-enforcement-2022-09-26/ (kasutamise kuupäev 9.05.2023)
24. Milne, R. (4. Juuli 2018. a.). Danske Bank shares fall on money laundering allegations . Allikas: ft.com: https://www.ft.com/content/50f338fe-7f5c-11e8-bc55-50daf11b720d (kasutamise kuupäev 23.01.2023)
25. Official Journal of the European Communities. (24. oktoober 2000. a.). concerning arrangements for cooperation between financial intelligence units of the Member

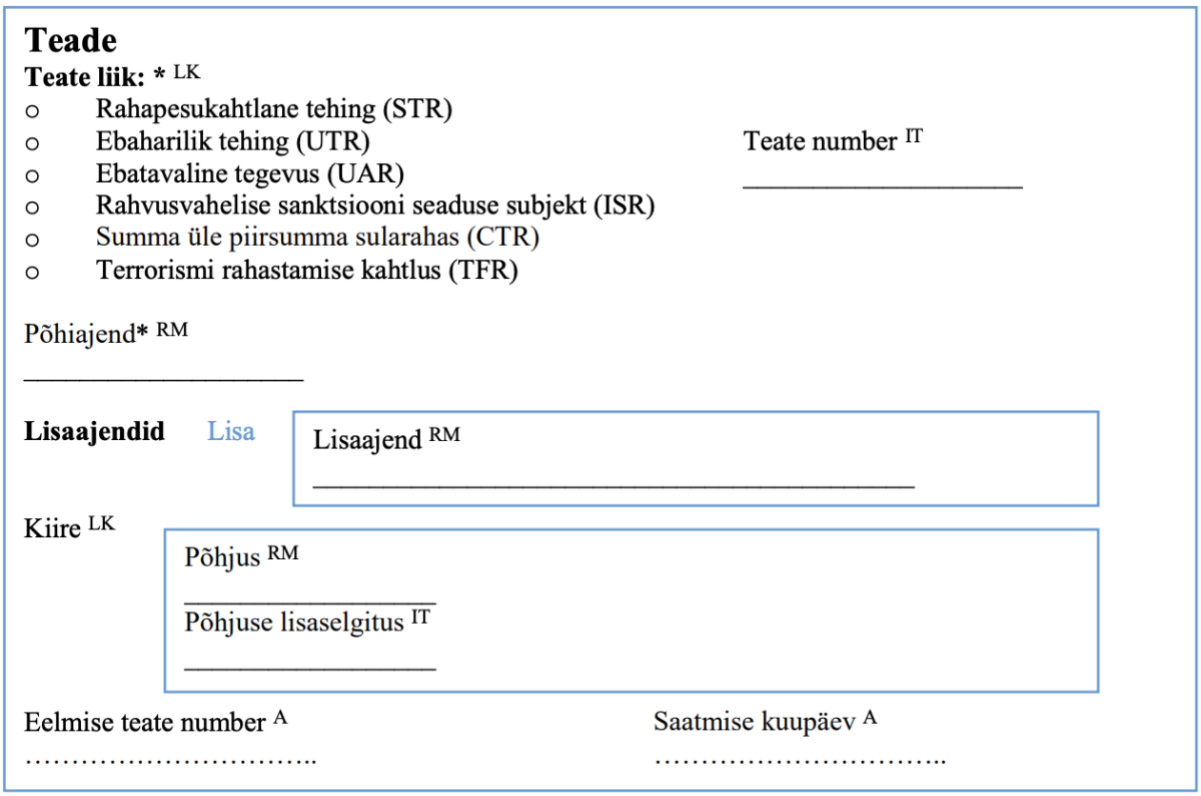
States in respect of exchanging information. Allikas: www.fiu.ee: https://fiu.ee/media/104/download (kasutamise kuupäev 8.01.2024)

26. Official Journal of the European Union. (16. september 2009. a.). DIRECTIVE 2009/110/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Allikas: www.europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=ET (kasutamise kuupäev 8.01.2024)
27. Official Journal of the European Union. (3. aprill 2014. a.). DIRECTIVE 2014/42/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Allikas: www.europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0042&from=ET (kasutamise kuupäev 8.01.2024)
28. Rahapesu Andmebüroo. (2020). Aastaraamat 2020. Allikas: fiu.ee: https://fiu.ee/aastaraamatud-ja-uuringud/aastaraamatud (kasutamise kuupäev 4.01.2023)
29. Rahapesu Andmebüroo. (31. juuli 2023. a.). Rahvusvahelised õigusaktid. Allikas: fiu.ee: https://fiu.ee/oigusaktid-ja-juhendid/rahvusvahelised-oigusaktid (kasutamise kuupäev 6.01.2024)
30. Rahapesu Andmebüroo. (mai 2022. a.). Rahapesu ja terrorismi rahastamise riskide juhtimine ning hoolsusmeetmete kohaldamine Rahapesu Andmebüroo järelevalvatavatele kohustatud isikutele. Allikas: www.fiu.ee: https://fiu.ee/media/291/download (kasutamise kuupäev 13.01.2024)
31. Rahapesu andmebüroo. (25. aprill 2022. a.). Juhend kahtlaste tehingute tunnuste kohta. Allikas: www.fiu.ee: https://www.fiu.ee/media/264/download (kasutamise kuupäev 13.01.2024)
32. Riigi Teataja. (6. november 2020. a.). Rahapesu Andmebüroo põhimäärus . Allikas: www.riigiteataja.ee: https://www.riigiteataja.ee/akt/122022023021?leiaKehtiv (kasutamise kuupäev 13.01.2024)
33. Riigi Teataja. (1. November 2022. a.). Karistusseadustik. Allikas: riigiteataja.ee: https://www.riigiteataja.ee/akt/129122011190 (kasutamise kuupäev 13.01.2024)
34. Riigi Teataja. (15. märts 2022. a.). Rahapesu ja terrorismi rahastamise tõkestamise seadus. Allikas: riigiteataja.ee: https://www.riigiteataja.ee/akt/112032022019 (kasutamise kuupäev 13.01.2024)

35. The Economist. (12. aprill 2021. a.). The war against money-laundering is being lost. Allikas: economist.com: https://www.economist.com/finance-and-economics/2021/04/12/the-war-against-money-laundering-is-being-lost (kasutamise kuupäev 22.01.2023)
36. The European Parliament and The Council of The European Union. (20. mai 2015. a.). DIRECTIVE (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Allikas: eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849 (kasutamise kuupäev 13.01.2024)
37. U.S. Department of State. (mai 2001. a.). THE FIGHT AGAINST MONEY LAUNDERING. Allikas: ait.org.tw: https://web-archive-2017.ait.org.tw/zhtw/DOCS/ijee0501.pdf (kasutamise kuupäev 16.01.2023)
38. Utkina, M. (30. mai 2023. a.). Leveraging Blockchain Technology for Enhancing Financial Monitoring: Main Challenges and Opportunities. European Journal of Interdisciplinary Studies, 141. Allikas: www.ejist.ro: https://www.ejist.ro/files/pdf/530.pdf (kasutamise kuupäev 16.01.2023)
39. World Bank Group. (Veebruar 2016. a.). Illicit Activity and Money Laundering from an Economic Growth Perspective A Model and an Application to Colombia. Allikas: worldbank.org: https://documents1.worldbank.org/curated/en/696421467996735910/pdf/WPS7578.pdf (kasutamise kuupäev 18.01.2023)

LISA A

Rahapesu Andmebüroole esitatava teate vorm




*Joonis 2*. Rahapesu Andmebüroole esitatava teate vorm

Allikas: Rahapesu Andmebüroo (https://www.fiu.ee/media/241/download)

LISA B

Kõrgema terrorismi rahastamise riskiga riigid ehk nn riskiriigid

Tabel 1

*Kõrgema terrorismi rahastamise riskiga riigid ehk nn riskiriigid, autori koostatud*

| | Riik | Alus |
|---|---|---|
| 1 | Afganistan | EL, ÜRO, riiklikult pädevad asutused |
| 2 | Alžeeria | riiklikult pädevad asutused |
| 3 | Araabia Ühendemiraadid | FATF, riiklikult pädevad asutused |
| 4 | Burkina Faso | riiklikult pädevad asutused |
| 5 | Egiptus | riiklikult pädevad asutused |
| 6 | Iraak | EL, ÜRO, riiklikult pädevad asutused |
| 7 | Iraan | EL, ÜRO, riiklikult pädevad asutused |
| 8 | Jeemen | EL, ÜRO, FATF, riiklikult pädevad asutused |
| 9 | Jordaania | FATF, riiklikult pädevad asutused |
| 10 | Kongo Demokraatlik Vabariik | ÜRO, riiklikult pädevad asutused |
| 11 | Liibanon | ÜRO, riiklikult pädevad asutused |
| 12 | Liibüa | ÜRO, riiklikult pädevad asutused |
| 13 | Lõuna-Sudaan | ÜRO, riiklikult pädevad asutused |
| 14 | Mali | ÜRO, FATF, riiklikult pädevad asutused |
| 15 | Maroko | FATF, riiklikult pädevad asutused |
| 16 | Mosambiik | riiklikult pädevad asutused |
| 17 | Nigeeria | riiklikult pädevad asutused |
| 18 | Niger | riiklikult pädevad asutused |
| 19 | Pakistan | EL, FATF, riiklikult pädevad asutused |
| 20 | Palestiina Omavalitsus | riiklikult pädevad asutused |
| 21 | Põhja-Korea (Korea Rahvademokraatlik Vabariik) | EL, ÜRO, riiklikult pädevad asutused |
| 22 | Saudi Araabia | riiklikult pädevad asutused |
| 23 | Venemaa Föderatsiooni Põhja-Kaukaasia föderaalringkond | ÜRO, riiklikult pädevad asutused |
| 24 | Somaalia | ÜRO, riiklikult pädevad asutused |
| 25 | Sudaan | ÜRO, riiklikult pädevad asutused |
| 26 | Süüria | EL, ÜRO, FATF, riiklikult pädevad asutused |
| 27 | Tuneesia | ÜRO, riiklikult pädevad asutused |
| 28 | Türgi | ÜRO, FATF, riiklikult pädevad asutused |
| 29 | Usbekistan | riiklikult pädevad asutused |

Allikas: Rahapesu Andmebüroo (https://www.fiu.ee/media/275/download)

LISA C
Transkriptsioon SEB panga kontaktisikuga

Nimi: Kristo Keldre
Pank: SEB
Intervjuu kestus: 36 minutit ja 12 sekundit
Formaat: Süvaintervjuu
Toimumiskoht: Teams
Toimumisaeg: 14. detsember

**K: Tere!**
V: Tere!
**K: Ma koostan bakalaureusetöö teemal „Rahapesu ja terrorismi rahastamise tõkestamine Eesti suurpankades“. Intervjuu kestab orienteeruvalt 30 minutit ning selle raames küsin Teilt peamiselt küsimusi, kuidas rahapesu ja terrorismi rahastamise tõkestamine pangas toimib. Kas Teile sobiks kui ma salvestan antud intervjuu?**
V: Lase, aga käia
**K: Ideaalne, siis võime alustada.**

**K: Kuidas rahapesu mõjutab pangandust?**
V: Kuidas rahapesu ise mõjutab, ta mõjutab pankade usaldusväärsust, mõjutab pankade reputatsiooni, kuna pangad on majanduse vereringe, siis rahapesu laiemalt on majandusele pärssiva mõjuga, kuna nüüd kuritegudes, mis on nagu rahapesu mõte, on kuritegelikul teel saadud saadud tulu üritamine legaliseerida või raha nagu valgeks pesta, et see loob majanduses mõnedele osalejatele ebaõiglase konkurentsieelise.

**K: Milliseid meetmeid või regulatsioone te kasutate rahapesu ja terrorismi rahastamise tõkestamiseks?**
V: Siin on nagu keeruline need mingit kitsast loetelu tuua, et rahapesu tõkestamise terrorismi rahastamise vastu võitlemise regulatsioonid – need hakkavad pihta juba aastakümnete tagant. Võib-olla, mis nüüd meie või Eesti pankade tegevust kõige otsesemalt mõjutavad, on Euroopa direktiivid, kus me täna oleme jõudnud juba kuuenda direktiivi arutelu juurde, et kõige nagu kõige suurema mõjuga viimastest aegadest oli neljas direktiiv, aga need on üle võetud ka Eesti seadusandluses ehk siis rahapesu terrorismi rahastamise tõkestama seadusesse. Ehk raha PTS-i, aga lisaks sellele on kõikvõimalikke erinevaid valitsuste üleseid organisatsioone, kes aitavad, võib-olla siis ütleks, niimoodi, aitavad turuosalistel oma neid rahapesu riske paremini tuvastada ja siis vastavaid meetmeid kasutusele võtta. Võib-olla nagu rahvusvaheliselt kõige tuntum või nagu kõige enim jälgitav on FATF ehk PAP, kes siis annab nii üldiseid soovitusi kui ka sektoripõhiseid või mingit konkreetset klientide põhiseid soovitusi. Sama on ka, ütleme nagu eesti tasemele tulla, et siis lisaks rahapesu tõkestamise seadusele. Nii võtab vastu ka riigikogu, eks on finantsinspektsioon ehk siis pankade järelevalvaja andnud omakorda välja väga mahuka soovitusliku juhendi. Ta nimi on soovituslik juhend, aga kuna need ettepanekud on väga mõistlikud ja välja on antud väga austusväärse organisatsiooni poolt ja nendega nagu soovituslikku juhendit, siis staatus on selline, et täida või selgita ehk siis nad on ikkagi üldjuhul on täitmiseks.

**K: Kes tegeleb teil pangas rahapesu ja terrorismi rahastamise tõkestamisega? Kuidas nende igapäevatöö välja näeb?**
V: Siin on natuke keeruline, on nagu vahet sisse tõmmata, et kes nagu tegutseb, sest kes tegeleb rahapesu tõkestamisega ja kes mitte, vähemal või rohkemal määral tegelenud sellega

kõik pangatöötajad eks, sest mis on nagu oluline eriti pankade puhul või kõige teiste turuosaliste puhul, mis on nagu oluline kriteerium rahapesu tõkestamine on „tunne oma klienti“ meetmete rakendamine või oma kliendi parim tundmine, et selles mõttes siin on suur roll eesliinil, kliendihalduritel, nõustajatel kontoris, kes otseselt klienti teenindavad, kes otseselt kliendiga suhtlevad ja siis on mingisugused spetsiifilisemad tegevused juba konkreetsemalt näiteks siis kõrgema riskiga klientidele tugevdatud hoolsusmeetmete rakendamine või siis maksete või tehingute jälgimine monitooringust, kust otsida välja jällegi kõrgema riskiga või mingit kahtlust äratavaid tehinguid ja nende uurimine. Ütleme nagu tagatoaüksused, kes selliste spetsiifilisemate tegevustega tegelevad, et need on nüüd ajas märkimisväärselt kasvanud - need üksused ise, ütleme viimase kolme aasta jooksul.

**K: Kas teil pangas esineb automatiseeritus või tehisintellekt?**
V: Tehisintellekti märkimisväärne või tehisintellekti kasutamisel ja me ei ole veel jõudnud, aga automatiseerimine kui selline või see alati kliendi riskihindamisest kuni nende klienditegevuste jälgimiseni, seal see on väga selline andmetel põhinev protsess, et andmete kogumine, töötlemine, analüüsimine seal sellist automatiseeritud on samamoodi üha rohkem juurde tulemas, võib-olla tehisintellekt on ka järgmine samm, kuhu astuda?

**K: Kuidas te tuvastate kahtlase tehingu?**
V: See läheb jube või päris laiaks see teema, et kindlasti on maht, aga see kui ütleme tehingu summa, aga siin ei saa vaadata ka ühte tehingu summat või jääda kinni sellesse ühe tehingu summas, et see võib olla ka mitmete järjestikuste või mitmed mingisuguse perioodi jooksul toimuvate tehingute jada, kindlasti on oluline, kes selle maksja teeb, kellele ta selle maksude, kuhu riiki makse läheb või kust riigist laekub ja see on sama nagu ka klientidele tugevdatud hoolsusmeetmete rakendamisele, et need stsenaariumid, mille järgi kahtlaseid tehinguid tuvastatakse, sõltuvad väga palju kui kõrgeks klientidele on meie kliendirisk hinnatud ja mis on need põhjused, miks me seda riski oleme nii kõrgeks hinnanud ja nendest põhjustest tulenevalt, siis võib ka selle nagu maksekäitumisest otsida erinevat riski, näiteks kui on tegemist kliendi mõttes, on tegemist riikliku taustaga isikuga, kes on siis näiteks riigikogu liige, minister, osades suuremate kohalike omavalitsuste juhtorgani liige niinimetatud riikliku taustaga isik ehk PEP, siis tema puhul on need markerid või on need kriteeriumid, mida maksetes otsida, tänu põhilisele riskile, mis korruptsioonirisk, on mõnevõrra erinevad, kui me räägime näiteks terrorismi rahastamisest. Terrorismi rahastamise puhul sõltuvalt jälle millises, millises konkreetset faasi terrorismi rahastamises me otsime on summa, ei pruugi olla üldse oluline. Terrorismi rahastamine võib endas kätkeda ka seda korjatakse kokku väga väikestes summades raha või siis nagu isikute panuseid selleks, et seda terrorist või terroriakti siis nagu organiseerida seda terrorismi toetada, et ütleme, pikem jutt, mis need põhjused olla või põhjused olla võivad või milliste, milliste reeglite või milliste loogika järgi, et summa võib olla näitajad, ei pruugi olla näitaja.

**K: Viimastel aastatel on kuulda olnud mitmest Eestis toimust rahapesuskandaalist. Milline on Eestis olev olukord rahapesuga?**
V: Nõus. Skandaale on olnud, kindlasti me oleme nendest skandaalidest ka õppinud võib olla tänu nende skandaalidele ka Eesti pangad on mõnevõrra rohkem panustanud rahapesu tõkestamiseks kui meie kolleegid üle piiri ja samas seal nende ütleme nendele skandaalidele anda sellist lõplikku hinnangut on paraku veel ikkagi vara, sellepärast et ütleme, et siin on erinevaid summasid välja toodud eilegi, kas või oli Ameerika Ühendriikide *Department of Justice* või siis nagu Justiitsministeerium tegi Danske Panga kaasuse osas ja seal on toodud välja erinevaid summasid erinevate pankade puhul, et mis, millises mahus on neid panku siis need läbinud kahtlased tehingud, aga me räägime rahapesu kahtlusest, et õiguskaitseorganid

veel tegelevad ja millises osas need rahapesu leiab kinnitust ja millises osas saab öelda, et need kahtlased tehingud tõesti ostsid rahapesuks seda natukene vara veel. Vara veel nagu kui välja tuua, aga kindlasti on Eesti tähelepanu saanud nende kaasuste tõttu ja kindlasti on ka sellest õpitud.

**K: Kuidas mõjutavad suuremad süüdistused panka, kas peale maineriski võib veel olla rängemaid tagajärgi?**
V: See kahju on mainele nii Eesti kui ka Eesti riiki laiemalt võtta siis maine võib mõjutada investeerimisotsuseid, majandus, Eesti majanduse laiemalt pankade puhul samamoodi ka kliendi usaldust partneri usaldust pankade, finantssektori mainet ja et sellel sellel kõigel, võib-olla ka siis otse raha, otsene rahaline mõju kui ka nagu maineriski küll keeruline hinnastada, aga tänu või tulenevalt sellest mõnevõrra kehvemast mainest ei ole välistatud, et mingisugused tehingud või või kokkulepped jäävad sõlmimata.

**K: Kas pankade vahel võivad regulatsioonid erineda? Kui võimalik, siis tooge näite.**
V: Väga konkreetset näidet ei oska tuua, need reeglid ja regulatsioonid on pankadele ikkagi samad. See sõltub nüüd, kuidas mõni pank on seda konkreetset nagu seadusandja või siis järelevalvaja ootust enda majas rakendanud, see on üks asi, teine asi on, Eesti puhul võib-olla ei saa kuna meil on neid turuosalisi suhteliselt vähe või panku kui selliseid ei saa nagu võib-olla väga konkreetset näidet tuua, aga ka rahapesu tõkestamise mõttes nagu erinevatel pankadel edendajatele turvalised võib olla erinev riskiisu. Ehk iga pank defineerib ära millisesse klientidega tema ja seda ma mõtlen siis nii-öelda kui rahapesu riski mõttes, et ühelgi pangal ei ole tõenäoliselt riskiisu rahapesu osas, et vot ma tahaks nii palju pesta, seda, mitte onju, et pigem klientide riskisuse osas, et kui palju, kui kõrge riskiga kliente me enda portfelli lubab, seal natuke seotud sellega, mis on võimekus, milline on ressurss teostada neid kontrollitoiminguid, klientide üle järelevalvet teostada ja nii edasi, aga riskiisu osas võib-olla lähenemine küll pangati erinev ja see on täitsa okei, sest kui isegi kui mõnel pangal kõrgem riskiisu kui teisel ehk et ta lubaks nagu riskantsemaid kliente, et samas suudab seda kontrollida, suudab sinna rakendada vastavaid meetmeid, noh siis on see aktsepteeritav äriotsus.

**K: Kas pangad võivad võita ka siis tegelikult rahapesust, kui see peaks nende pankades toimuma.**
V: Finantsiliselt mahtude pealt tõenäoliselt midagi teoreetiliselt jah, ikka, sest noh, kui me nagu pangad teevad makseid, siis raha liigub, maksed liiguvad teoreetiliselt on muidugi, muidugi siin ka tulude teenimise võimalus, aga arvestades seda maineriski ja kui kõrged või madalad on täna tavapäraselt maksete teenustasud, siis see oleks ikka väga kahtlane - väga kahtlane otsus.

**K: Millised tagajärjed võivad juhtuda kui pank ei ole suutnud ära hoida rahapesu?**
V: Ja ikka, nii pangana juriidilise isikuna kui panga juhtkonnale kui pangatöötajatele, kes rahapesu tõkestamise eest vastutavad on, saab vastutusele võtta nii väärteomenetluse kui kriminaalkorras. Kui sa vaatad rahapesu tõkestamise seadust näiteks või karistusseadustiku, siis see on see on tõesti ja ütleme ka neid pankadele nüüd mõtlen, et juriidiliste isikute, pangale endale võimalike trahvide määrasid on siin ka viimasel ajal tõstetud.

**K: Kuidas on tänapäevane digimaailm muutnud raha pesemist?**
V: Rahapesemisel on mõtet pesta musta raha, seda esmalt, et ehk peab raha peab olema saadud nagu kuritegevusest ja esmaspäevane digimaailm on muutnud seda, kuidas kuritegevus toimib ja lisades sinna ka täiesti uusi kuriteoliike või noh ka viimasest ajast võtta

siin kas või näiteks kõikvõimalikke pettusid ja pangapettusid või investeerimis petuskeeme ja nii edasi, et siis ka sealt saadav raha pettuse teel, kelmuse teel saadud raha, et mis vajab puhtaks pesemist. Ja teine sidend tehnoloogilise poole pealt on, et kuidas ettevõtted sealhulgas kuidas, kuidas pangad suhtlevad oma klientidega, digitaliseerimine teeb suhtlemist laialdasemaks, kiiremaks, sama on maksetega, et kui enamus makseid euromaksed, siis Euroopa liidus liiguvad reaalajas siis kõik, see toimub palju kiiremini. Pluss veel muidugi, täiesti uued tegevusvaldkonnad või tööstusharud, mis kannab ka Eesti puhul siin näiteid, me räägime ühisrahastusest, näiteks, siis kuidas hulk inimesi paneb raha kokku et rahastada mingit kinnisvaraarendust või siis *piir-lending crypto* valuutat – kõik see digimaailm tekitab keerukust. Teisest küljest on ka tänu sellele varem rääkisime automatiseerimisele, *machine learningule*, tehisintellektile - tänu sellele on ka võimalusi rohkem arendada ja, ja parendada oma tööriistu, millega seda sama kahtlaseid tehinguid ja võimalike raha võimalik rahapesu tuvastada.

**K: Tänapäeval on paljud pangad hakanud aktsepteerima krüptot, kas sellel on ka ohukohti?**
V: Ja absoluutselt, aga noh, sama on ka näiteks sularahaga, et krüpto liigutamine. Krüptovaluuta liigutamine või edasikandmine toimub väga palju kiiremini. Ja ei sõltu nagu asukohtadest aga noh riski mõttes on, teda võib teda võrrelda sularahaga või mõtestada sarnaselt nagu sularaha, et ta on anonüümne - üldjuhul on ta anonüümne. Krüptopuhul jah, on olemas töövahendid, on võimalus tuvastada tehingute jadasid aga, aga suures plaanis on ta anonüümne ja sealt eriti, kui me mõtleme nagu rahapesusüsteemi sissesaamise baasi, siis siis on ajalooliselt olnud sularaha, nüüd krüpto üks nagu õhuallikas. Aga noh nagu LHV on selle otsuse teinud ja ta tahab krüptot, või noh krüptovaluutat sellises osas nagu arveldada, seda aktsepteerida, siis nende kontroll kontrollimehhanismide osas olen ma olev vastav, et need riskid ära katta.

**K: Mis on „tunne mu klienti“ tugevused ja nõrkused?**
V: „Tunne oma klienti“ metoodika või nagu protsessi tugevus on see, et see võimaldab seda klienti rahapesu riski palju adekvaatsem adekvaatsemalt ja detailsemalt hinnata, kogu mõte „tunne oma klienti“ protsessi mõte ongi see, et me saame aru, kes see klient on, miks ta tahab just meiega äri teha, mis on tema ootused pangasuhtele kus ta oma tulu teenib, kus ta oma vahendid on saanud ettevõtete puhul, kes on seotud isikud, kes teda kontrollivad kes on omanikud ja, ja see teadmine või see need, need andmed laialdasemalt võimaldavad palju paremini siis kliendi riski hinnata. Võib-olla ütleme, negatiivne külg on pigem kliendipoolne, et, selleks, et seda riski hinnata, seda riski hinnata, pead ikkagi kokku koguma need andmed ehk et ta võib olla väga suurele hulgale klientidele, võib olla ebaproportsionaalselt koormav. Jah, siin on, on ka ütleme, nagu dünaamilisem KYC või, või kliendi tegevusalast lähtuv KYC või sellest, kus klient oma elutsüklis eraisik oma parasjagu on, et selle põhjal dünaamilisema KYC ülesehitamine, pluss see, et mis, nagu pärast hiljem toimub on nagu kliendi andmete valideerida, kliendi vara päritolu, rikkuse päritolu tuvastamine ja kõik see on nagu dünaamilisem, aga jah noh, lihtsalt me oleme näinud, näinud kriitikat, et osad kliendid vähemalt peavad neid küsimusi, mis me neile esitame, võib-olla liigselt koormavaks. Eriti kui nad on, nagu nad ju ise teavad, et nad ei tegele rahapesuga, aga me tahame selles ka veenduda ja teinekord nad tekitavad sellist frustratsiooni.

**K: Kuidas te siis täpsemalt kontrollite seda, et eraisikud ei tegele rahapesuga? Milliseid küsimusi te klientidelt küsite, et teada saada, kas ta tegeleb rahapesuga või mitte?**
V: See sõltub nüüd, kus etapis me parasjagu oleme, kasvõi see, et kui tuleb meile uus ettevõte, tahab kliendiks saada, siis me teeme kindlaks tema omandistruktuuri ja kes siis on

need isikud, kes mõtlen, et eraisikute füüsilisi isikuid, kes me peame lõplikult seda ettevõtted omavad või sellest ettevõttest kasu saavad. Ja nende kohta me, me tahame ka kokku koguda andmeid, et siis saad aru, mis on nende isikute varasem kogemus, mis riski nemad endas kätkevad, kui me räägime tehingute jälgimisest ning kahtluse tekkimisel?
Siis need küsimused võivad minna väga-väga laiali, mis selle, mis selle rahaülekande aluseks olev äritehingu oli, mis dokumentatsioon seda äritehingut kinnitab, toetab, kui see on mingi kaubavahetustehing, mis kaubad liikusid, kuidas liikusid, kuidas transporditi? See sõltub nagu asjaoludest, et ja noh niikaua me küsime neid küsimusi, kui nii, kui meil tekib endal see sisemine veendumus, et et siin on kõik korras.

**K: Kas pangad teevad omavahel koostööd ehk näiteks kas nad jagavad omavahel klientide andmeid?**
V: Pangad teevad ikka koostööd ja neid koostöö formaate on väga erinevaid, üks võimalus on, et mida väga mitmetes riikides tiikides praegu uuritakse ja mille eesmärk ongi teha kliendi jaoks sellise või esmase teda iseloomustava „tunne oma klienti“ informatsiooni esitamise pankadele lihtsamaks kõik võimalikud sellised süsteemid, mida nimetatakse *service utilities*, eks täiendavalt on näiteks Eestis on siukene startup, mille nimi on Salv ja kes kelle nagu tugevus või kelle ootused on just suunatud sinna, et parandada infovahetust pankade vahel, parandada sellist teadmiste edasiandmist ja nagu kliendikliendist parema arusaamise või tunnetuse tekitamist. Väga põnev lahendus ja noh, päris palju, et Eesti pangad kasutavad ka Salve sellist suhtlus tarkvara või omavahelise info jagamise tarkvara.
**K: Väga hästi. See on muidu minu küsimustega ühel pool. Suur aitäh küsimustele vastamise eest!**

LISA D

Transkriptsioon anonüümseks sooviva jääva panga kontaktisikuga

Nimi: Anonüümne
Pank: Anonüümne
Intervjuu kestus: 34 minutit 48 sekundit
Formaat: Süvaintervjuu
Toimumiskoht: Zoom
Toimumisaeg: 21. detsember 11.00

**K: Tere!**
V: Tervist!
**K: Ma koostan bakalaureusetöö teemal „Rahapesu ja terrorismi rahastamise tõkestamine Eesti suurpankades“. Intervjuu kestab orienteeruvalt 30 minutit ning selle raames küsin Teilt peamiselt küsimusi, kuidas rahapesu ja terrorismi rahastamise tõkestamine pangas toimib. Kas Teile sobiks kui ma salvestan antud intervjuu?**
V: Ja, pole probleemi.
**K: Ideaalne, siis võime alustada.**

**K: Kuidas rahapesu mõjutab pangandust?**
V: Meedias on eks ole räägitud ka sellest, et jah, et pangad pesitsevad raha, et see on niisugune ütleme, terminoloogiline viga, mida tihti kasutatakse, et pangad ei pese raha, et pangad lihtsalt vahendavad neid rahavooge, mis on seotud saadud kuritegelikul teel ja ja on seotud rahapesuga, eks ole. No kui just jah, ei ole tõestatud selline *case*, et mingi pangatöötaja saab sellest isiklikku kasu, sest mis see rahapesu on, et rahapesu eeldus on ju see, et on toime pandud mingisugune eelkuritegu, et peab olema teenitud tulu, mis on saadud kuritegelikul teel, et jah mõni pangatöötaja otseselt sellega seotud, et siis võib öelda jah, et pangatöötaja osales rahapesus, aga pangad jah, üldiselt pigem sõltuvalt oma kontrollsüsteemide nõrkusest võivad aidata kaasa ka siis sellele, et kuritegelik raha voolab läbi panga süsteemide. Aga mida ta pangandussüsteemile tähendab? Ühtepidi, eks ole, iga riigiasutus on äriettevõtte, eesmärk on nagu tulu teenida, kasumit teenida. Kui meenutame näiteks Danske saagat, eks ole, mõne aasta tagusest ajast, siis Danske puhul ka ju suure Danske grupivaatest Eesti äri, kui ma õigesti mäletan laenumaht ja hoiuste maht oli suhteliselt marginaalne grupivaatest, aga mingil ajahetkel see tulu, mis teeniti nende klientide pealt, oli kolmkümmend protsenti kontserni või grupi tuludest kokku, mis oli nagu üüratu proportsioon ehk et selline jah, kasumiahne eesmärk on teenida tulu. Aga loomulikult kui see realiseerub, ütleme avalikkuse ette see info, et pangad on aidanud kaasa kuritegeliku raha poole läbi pangandussüsteemi siis juhtub see, mida kui sa guugeldad, soovitan guugeldada aktsiahindasid, et mis juhtus Danske aktsiaga näiteks või mis juhtus Swedbanki aktsiaga, kui need uudised avalikkused said? See väljendub nagu otseselt aktsiahinnas, kui on tegemist avaliku ettevõttega, et aktsionärid saavad, eks ole, aktsionäride vara haihtub. Ega Danske panga hind, aktsia hind ei ole siiamaani jõudnud, ta kaugel, kaugel nendest tasemetest, kui oli skandaalieelne aeg. Et otsene aktsionäride vara kaotus, et noh, mis ilmselt tähendab see seda, et sellele järgneb tegelikult ilmselt võtmeisikute väljavahetamine pangas. Nõukogu liikmed, esimees, juhatuse esimees, juhatuse seotud liikmed, kontrolli funktsioonide esindaja. Et sellele on, sellel on teatud tagajärjed ja mainerisk loomulikult. Mainerisk loomulikult peegeldub ka maineriski realiseerumine peegeldub aktsiahinnas. Aga ega see negatiivne kuvandi, jääb külge kauaks, et Swedbank Eesti näitel, jah, võib-olla avalikkus seda nii palju ei seosta sellega, et oli, oli see teatud ka nagu ebaseaduslike rahavoogude liikumisega, aga

noh, Danskele, ma arvan, see plekk on küljes aastateks ja seda maha pesta ja seda *case*'i unustada, nagu ikkagi suhteliselt keeruline.

**K:** M**illiseid meetmeid või regulatsioone te kasutate rahapesu ja terrorismi rahastamise tõkestamiseks?**
V: Pankades on ülesse ehitatud keerukas hoolsusmeetmete riski juhtimise süsteem, et pankades täpsemalt neid nõudeid edastab, kirjeldab lahti finantsspektsiooni soovituslik juhend. Aga ütleme, oluline on see, et kontrollmeetmed on ja ütleme ka kontrollmeetmete rakendamine ja ütleme siis kontrollm nende meetmete rakendamise üle, et see on nagu mõistlikult optimaalselt laiali jagatud erinevate struktuuriüksuste lõikes ja seda kutsutakse siis kolme kaitseliinipõhiseks lähenemiseks. Võib-olla sa oled sellega juba kokku puutunud ka kirjutamise käigus, aga, aga noh, kolm kaitseliini, *three-lines of defence*, esimene kaitseliin ongi äri, äriüksus äriorganisatsioon, et panga puhul siis näiteks äriüksus, kes, kes teenindab ettevõtetes kliente või äriks, kes teenindavad varakaid, eraisikuid, eraisikutest kliente, et äriüksus aru saama, kas klinditegevus on nii-öelda, vastab sellele, mis klient neile on öelnud. Sest noh, iga kord, kui kliendid juba avatakse, kui klient tuleb panka, siis need küsimustikud, eks päris mahukad teevad kirjeldama seal, et mis ta, mis ta eesmärk on näiteks tal seda kontot vaja on, et kui suured käibed sealt hakkavad läbi käima, milliste riikidega, kui suur on, ma ei tea, sularaha osakaal ja näidata ja nii edasi ja nii edasi, et esimene kaitseliin ehk äri peabki aru saama selles, et sellest, et kas see, mis seal kliendi kontol toimub, kas see on vastavuses sellele, mis klient meile öelnud. Ja kui ta tuvastab siis midagi kahtlast, et on mingisugused tehingud, mingid vastaspooled, mingi kliendi käitumine, mis ei vastanud päris sellele, mis klient on öelnud siis ta peab kõigepealt tema aru saada. Et kas see on nagu sisuline kahtlus või mitte. Võib-olla küsib kliendi käest täiendavat infot, analüüsib dokumente. Kui ta seda kahtlust ei suuda nagu kõrvale heita ehk kliendi vastuseid ei ole ikkagi nagu piisavad, siis, siis ta edastab selle selle teema nii-öelda edasi teise kaitseliini, teine kaitseliinid kutsutaksegi, on selline vastavuskontroll vastavuskontrollifunktsioon ehk et vastavuskontrolli funktsioon tegelebki siis nende kaasuste uurimisega, mis esimene kaitseliin ehk äri edastab langetab lõpliku otsuse, et kas on tegemist kahtlusega või mitte. Ja vajadusel siis teavitab rahapesu andmebürood, et Eestis, eks ole selline üksus, kes menetleb sisulisi, selliseid kahtlasi kliente, kahtlasi tehinguid, eelmenetlus enne uurimisasutusi on rahapesu andmebüroo, teine kas kaitseliin otsustab, et kas seda teavitust koos on vaja täita või mitte ja lisaks siis teine kaitseliin, mis ta teeb, teine kaitseliin töötab välja ehk siis see vastavuskontrolli funktsioon töötab välja erinevad metoodikad, metodoloogiat. Kuidas hinnata rahapesu, rahapesuga seotud riske riskitaset organisatsioonis. Kuidas hinnata kliente, millised, milline riskitase kliendile külge anda kuidas hinnatavaid erinevaid riike, näiteks millega kliendid arveldavad? Ütleme, sellised üldised põhimõtted metodoloogiat ja ütleme, riskihinnangust tuleneb ka tegelikult selline naljakas termin nagu riskiisu. Et riskiisu tegelikult väljendubki nende riskide ulatust ja täpsemalt siis kliente või kliendigruppe keda pank on valmis teenindama või siis keda pank on valmis teenindama teatud ulatuses või mida pank üldse valmis tegema. Ja teine kaitseliin teostab siis kontrolli äri ehk esimese kaitseliini üle, et kas sisekord on rakendatud praktikas nii nagu vaja, sest et praktika on näidanud ajalugu ka seda tõestas ka Danske kaasused, sisekorrad, tegelikult sisedokumendid reeglid olid kirjutatud üsna hästi, aga nende rakendamine praktikas oli, oli hoopis midagi muud, et nad olid pigem selline suitsukate mitte sisuliselt rakendatav meetmestik. Kontrolli esimese kaitseliini üle ja jah, ütleme ka selline analüüsi pool sügavama analüüsi pool ja juhatuse teavitamine, et juhatus peab ka juhtorganid peavad olema alati kursis, millised, nagu riskid. Ja kolmas kaitseliin on siis siseaudit, et siseaudit omakorda hindab siis teise kaitseliini esimese kaitseliini tegevust ja siseaudit on eks, sõltumatu sõltumatu funktsioon, et sõltumatu panga juhatusest allub, allub nõukogule, tõmbaks andma siis sellise kõige objektiivsema

hinnangu, kuidas teine kaitseliin, esimene kaitseliin oma tegevusega hakkama saab. Ja mingisugune teooria on ka see, et, et ei ole mitte kolm kaitseliini aga on ka, neljas kaitseliin, neljas kaitseliin, tegelikult ongi siis juba riik, et riigi vastavad ametiasutused, kes, kes omakorda hindavad siis ettevõtete tegevust erinevate kontrollide rakendamise. Aga jah, kui korra veel rääkida, et mis kontrolle klientide suunal pank rakendab. Et noh, eks paljuski need nõuded on ette kirjutatud seadustest tulenevalt. Aga jah, panga ülesanne on aru saada, et millised on kliendiga seotud riskid. Sõltuvalt sellest antakse kliendile siis selline riskiskoor või riskistaatus külge ja omakorda sõltuvalt sellest, et kas klient näiteks kõrge riskiga või, või madala riskiga sellest sõltub ka tegelikult andmete ulatus ja kogus mida klient, mida pank kliendi kohta küsima. Ja ajaperiood, kui sagedasti seda uuendama peab. Üldine turupraktika on selline, et kui sul on kõrge riskiga klient siis sa pead uuendama tema andmeid kord aastas, kui madala riskiga klient, siis sa pead uuendama tema andmeid kolme kui kuni viie aasta jooksul sõltuvalt turupraktikast ja kõiki tehinguid. Kõik tehingud, mis pangas toimuvas neid kontrollitakse pangakontroll funktsioonide poolt, noh, see on selline nii-öelda radar radarilt väljas tegevus, eks ole, et et need kontrollid toimuvad kogu aeg. Üldiselt rakendatakse selle jaoks automaat, automaatseid, automaatset tarkvara, automaatkontrolle mingit tehingut kontrollitakse reaalajas, ehk et siis, kui tuvastatakse mingi kahtlus, tehing jääb kinni, vaadatakse tehing ülejäänud lastagi toimuda, kui kahtlus võrratud mingit tehingut kontrollitakse nii-öelda viitidega, et ega ja, ja ma arvan, see on suures plaanis selline süsteem, et suurest, kui, kui nagu süsteemi vaadata, et mis komponentidest koosneb, et ongi tegelikult kõik saab alguse riskihinnangust, et pank hindab finantskuritegevusega või rahapesuga seotud riskide riskide taset pangas lähtuvalt sellest saab defineerida, millist struktuurset organisatsioonilist vahendit vaja on. Milliseid ülesandeid struktuuri struktuuriüksused täidavad, kirjeldavad kirjeldatakse ära üldine sisekordade raamistik. Siis kolmas tase on, on selline jooksev, kutsutakse hoolsusmeetmed, hoolsusmeetmed või kontrollid nende rakendamine igapäevaselt. Ja viimane, neljas etapp ongi siis selline jooksev hindamine nende kontrollide osas, et noh, ongi see, mida, mida siseaudit ja, ja vastavuskontroll teevad ja see on nüüd selline aastane tsükkel, sest et riskihinnang pangaülene tuleks teha, tuleks uuendada vähemalt kord aastas.

**K: Kes tegeleb teil pangas rahapesu ja terrorismi rahastamise tõkestamisega? Kuidas nende igapäevatöö välja näeb?**

V: Eraldi meeskonnad on sama, sama nende kaitseliinide lõikes nagu, nagu ma rääkisin. Et eraldi mehitatud üksused on esimeses kaitseliinis ja teises kaitseliinis. Kui palju neid inimesi on? See nüüd tõesti iga panga spetsiifiline, et no kui me räägime Eesti suurematest pankadest, et siis ikkagi siin on tegemist kümnete inimestega, suuremates pankades, ilmselt sadade inimestega tegelevad nende kontrollide rakendamisega hindamisega, et seal on nagu hästi-hästi iga pangaspetsiifiline ja iga iga panga lõikes erinev.

See [tööülesanded] sõltub hästi sellest, et, milline, milline on konkreetse isiku töö profiil, sest et tegelikult see valdkond valdkond on hästi kiilustatud erinevate kompententside mõttes, et on inimesed, kes tegelevad kliendiandmete uuendamise valideerimisega, et vajadusel suhtlevad kliendiga küsivad lisainfot, et noh, andmed on selles mõttes nagu kõige alus. Andmed tuleb hoida ajakohased, sest et kui sul ei ole andnud ajakohaselt, siis sa tegelikult ei omaga kliendi kohta tõest infot ja ei saa rakendada kontrolle efektiivsel moel. On, on, ütleme neid klient neid töötajaid, kes jah, võib-olla kelle põhitöö ongi pigem nagu selline müük, toote müük klassikalises mõttes. Aga ikkagi ta peab nagu aru saama, et teda on koolitatud vastavalt, et ta peab aru saama sellistest noh, nimetame siis punastest lippudest, mis ei ole nagu aktsepteeritavad ja normaalsed. Et kui kliendi tegevuses midagi tuvastab kahtlast, siis ta edastab selle info juba vastavasse kontrollfunktsiooni. See esimese esimese kaitseliini kontrollfunktsioon ja seal ongi siis omaette inimesed, kes, kes noh, tegelevat sellise

perioodilise kliendi kliendi ülevaatusega võtavad noh, nagu ütlesin näiteks kõrge riskiga klientide puhul kord aastas ette kogu kliendi andmestikku kogu kliendi ärivõrgustiku pagasi, aga avalikele allikatele tuginedes või on siis seal selliseid uurijad uurijate tüüpi inimesed, kes Noh, eelkõige siis selliseid automaatseid, teavitusi, mis mis automaatselt kontrollisüsteemid annavad, on, on sellised inimesed ilmselt ka esimene kaitseliinis, kes kirjutamise eest ja kontrollivad ja kui nad oleks täidetud enda tiimide poolt, et suures plaanis, see on sihuke ja esimese kaitseliini tegevus. Teise kaitseliini profiil on natukene sarnane, et noh, seal on samamoodi selliseid uurija profiiliga inimesed. Kes päeva lõpuks otsustavad, eks ole, et kas kas mingisugune kahtlase tehingu teatis tuleb endast rahapesu andmebüroole või mitte, on inimesed, kes töötavad välja metodoloogiat riskide hindamiseks teevad siis mainitud vastavus auditeid. Esimese kaitseliini tegevus üle, nõustavad äri. Sest et esimese kaitseliinitöö on ka anda nõu ärile, et kui esimene kaitseliin ei ole kindel mingi otsuse suhtes või tegemist on mingisuguse spetsiifilise, kõrgema riskiga kliendiga siis esimene kaitseliin mõnikord ei saagi isenesest otsust vastu võtta, et kui, kui ei ole nagu täiendav nõustamine toimunud või täiendav *accept* antud. Et noh, pankades, mis kasutusel on sellised vastavad komiteed kus siis ostetakse kõrgema teatud tunnustele vastava kõrgema riskiga kliendid, klientide kliendisuhte alustamine ja kliendisuhte jätkamine, et noh, teine kaitseliin, esimene kaitseliin komiteesid üldjuhul veab. Teine kaitseliin siis osaleb seal töös ja nõustab, vajadusel sekkub, kui näeb, diskussioon kujuneb või suundub kuskile ebasoovitavas suunas. Ja auditis, kolmas kaitseliin, noh nagu nagu audiitorid ikka, et ega nendel on pigem selline homogeensem profiil. Et normidele nõuetele vastavuse hindamine oleks kõik kõik kolm kaitseliini, loomulikult seal on iga iga kaitseliini lõikes, on oluline vastav kaitseliinitööplaan ja tegevusplaan, et et võimalikult parima teadmise järgi ja võttes arvesse teadaolevaid riske. Tegelikult ikkagi nad peavad ettepoole hindama, et mida, mida ette võtta. Et lisaks sellisele jooksule tegevusele, et et millised on muud tegevused projektiku, kontrollid, mida nad iga aasta peaks tegema.

**K: Kas teil pangas esineb automatiseeritus või tehisintellekt?**
V: Jah, et tehingute jälgimine on automatiseeritud, toetavad protsessid on ka osaliselt automatiseeritud, aga noh, järjest rohkem automatiseerimise poole me läheme. Et just eelkõige seda, mis puudutab kliendiandmete kogumist ja uuendamist, et see on ka oluline ära automatiseerida, et eelkõige senisest efektiivsus vaatest oluline, et ja jah, praegu meie oleme liikumas sinnapoole, et teavituste edastamine rahapesu andmebüroole oleks nagu täiemahul automatiseeritud Eestis teadaolevalt me oleks neljas pank, kes kes sellist automatiseeritud XD portaali lähenemist hakkaks kasutama.

**K: Kuidas te tuvastate kahtlase tehingu?**
V: Kahtlaste tehingute tuvastamiseks on kõige parem dokument rahapesu andmebüroo kahtlaste tehingute tunnuste juhend, kus on kahtlased tunnused välja toodud mingil määral on lahti kirjeldatud ka finantsinspektsiooni põhi AML juhendis selles põhijuhendis lisades, õigemini punaste lippude, noh aga need on kaks, kaks põhilist sellist allikat ega pangad midagi võib-olla kirjutavad ka ise täpsemaks, aga ütleme, need mõlemad viidatud suunised on nagu piisavalt mahukad. Nad annavad tegelikult suuna kätte. Aga suures plaanis ongi, et lisaks nendele tunnustele kahtlase tehingu tunnustele , mis on mainitud juhendis välja toodud tuleb pank hindama ka jah, et see, mis kontol toimub, et on see nagu tavapärane arvestades kliendi profiili või, või ei ole. Kui ma ei tea, kui pensionär Lasnamäelt, kes siiamaani on kandnud raha ainult Eesti siseselt ja väikestes summades, et ta hakkab, hakkab raha kuskile kõrge riskiga riiki kandma näiteks nagu Türgi, et siis see ilmselt ei ole nagu tavapärane tegevus, et kas ta nagu pettuse ohver või seal mingit muud teemat taga, aga et see ei vasta nagu eelduslikult sellise sellise klindi tavapärasele või normaalsele käitumisele. Aga jah,

need juhendid mainitud juhendid, mis ma viitasin, et need annavad kõige laiema pildi, mis nagu kahtluse tunnused.

**K: Mis on „tunne oma klienti“ tugevused ja nõrkused?**
V: Noh, kuidas võtta, et ma arvan, et ta annab tegelikult turuosalistele ikkagi hea raamistiku kuidas aru saada, mis on nagu võimalikud riskifaktoreid. Probleem ongi see, et need nõuded on muutunud väga põhjalikuks, et neid nagu efektiivselt manuaalselt rakendada on suhteliselt raske ja tehnilised lahendused, mis turul on pigem need võib-olla alati ei ole efektiivselt võimelised toetama seda andmekogu korjeti analüüsi et pigem ma ütleks, et see on võib-olla kõige suurem väljakutse, et regulatiivsed nõuded muutuvad järjest karmimaks, aga protsesside juhtimise mõttes automaatkontrollid ei ole võib-olla nii head, kui nad võiks olla. Muus osas tugevuste, nõrkuste osas ma isegi oskaks niimoodi öelda või mingeid etteheiteid hakata välja tooma, et ta on selline normide ja reeglite kogum. Kuidas hinnata kliendiga seotud riske ja milliseid, millistele andmetele tuginedes seda teha? Et jah tugisammas riskide hindamisel

**K: Viimastel aastatel on kuulda olnud mitmest Eestis toimust rahapesuskandaalist. Milline on Eestis olev olukord rahapesuga?**
V: See on keeruline küsimus, ma arvan, et esiteks on ühtepidi Eesti asukoht kaardil on nagu väga halb, et me jääme alati lääne-idapiirile ehk et see kuritegelik raha vist nagu ida poolt üritab tulla, et see, see üritab ikkagi siseneda Euroopa pangandussüsteemide läbi nende piiririikide, et see risk on nagu alati olemas. Teistpidi Eesti on hästi läbipaistev, hästi väike keskkond, et ma arvan, et just sellised väikesed finantssüsteemid on, võib-olla rahapesijate, läheb pigem nagu ebahuvitavad, sest et rahapesu noh, pigem ikkagi eesmärk on pigem suuremaid summasid, eks ole, suurimal suuremaid summad, mis on kuritegelikul teel teenitud läbi finantssüsteemi juhtida ja, ja kui nad suurenevad, summad hakkavad liikuma läbi väikese finantssüsteemi nagu Eesti on või siis paratamatult hakkab silma ja tekitab küsimusi, et miks see nii on. Ehk et ma arvan, et välismaised kurjategijad võib-olla pigem siit et, et me ei ole nende jaoks nagunii huvitav, et paistaks oma tegevuse lihtsalt liiga palju silma, et võib-olla isegi suurem probleem on võimalik, selline siseriiklik kuritegevus, et et noh, kui sa mäletad siin viimase nädala viimase paari nädala jooksul meediast läbi käinud ka üks selline globaalne krüpto kelmuse kaasus. Kui sul silma hakkas, et seal olid Eesti kodanikud, vene nimega eraisikud Potapenko ja Turogin, et USA alustas nende osas uurimist, et väidetavalt ligi kuussada miljonit dollarit peteti välja. Et pigem nagu sellised kodumaised kriminaalide, kelmid, võib-olla on väljakutse, et mingi osa rahavoost vanad, eks ole, suunanud ära ka Eestist välja. Et kuidas nagu aru saada mida, mida sul siin kohalikud inimesed teevad, et see võib olla suurem väljakutse, et eelistaks võib-olla pigem pigem nii-öelda sisemaised ja, ja välismaised kurjategijad. Ning eestis pakutav e-residentsus ei anna võimalust välismaalastel rahapesuks, kuna Eesti pangad on selles mõttes väga konservatiivsed pangad, pangad, minu arvates eriti ükski väga hea meelega e-residentidele kontosid lahti ei tee, et pigem tehakse seda vähe. Ja põhjus ongi see, et see esialgne kontroll vida mida Eesti välis välisesindused teevad, et tegelikult see kontroll on ikka väga pinna peale, et me ei tea tegelikult nende e-residendi liiga palju ja nagu statistika näitab, et ega, ega need e residendid ei ole reaalselt, ei suutnud Eesti majandusele liiga palju lisaväärtust luua. Tegelikkuse praktika ikkagi, käärid on väga suured.

**K: Kuidas mõjutavad suuremad süüdistused panka, kas peale maineriski võib veel olla rängemaid tagajärgi?**
V: Noh, eks mingil määral mingil määral võib see kuidagimoodi mõjutada välisinvesteeringute mahtu, aga noh, ma arvan, et see on pigem niisugune teoreetiline

hüpotees, et ega ega Danske *case* ka ju kuidagimoodi ei mõjutanud seda. Ja välisinvesteeringute mahtu Jah, ma arvan, et otsene ja oluline mõju pankade jaoks ongi needsamad seotud isikud, et tippjuhtkond ja seotud otseselt isikud nende isikute personaalvastutusega ikkagi täiesti olemas ja, ja Eestis on nii, et kui, kui sinu suhtes on ikkagi algatatud juba kriminaalmenetlused, siis sa enam edaspidi kontroll funktsioonidel ja juhtivatel kohtadel finantssüsteemis töötada ei saa, et see on tuleviku jaoks välistus. Ma arvan, et need on siuksed, põhilised, mida võiks võiks välja tuua, sest et trahvid finantsinspektsioon, kes teostuda eraldatud pankade suhtes võib trahve määrata pankadele, noh, kui asi läheb kriminaaluurimiseks juba nagu Swedbanga puhul tegelikult, eks ole, finantsspektsioon oma omapoolse uurimise lõpetas, andis materjalid edasi prokuratuuri. Et sealt või teoreetiliselt võivad ka, eks ole, riigipoolsed mingisugused karistusmeetmed jõustuda noh, nii trahvide kui, kui ka võib-olla vanglakaristuse näol. Et nagu ikka, et eks me need võimalused tuginevad, tuginevad jah, mis on finantsinspektsiooni võimalused ja mis, mis on nagu lubatud karistusseadustikus tulenevalt.

**K: Kas pankade vahel võivad regulatsioonid erineda? Kui võimalik, siis tooge näite.**
V: Ja ikka, ühtepidi nõuded, kui vaatame Eestis tegutsevaid panku, nõuded põhimõtteliselt kõigile samasugused ega rahapesu tõkestamise vaatas, põhimõtteliselt ei ole vahet, kas oled kas sa oled eraldiseisev pank või sa oled filiaal siseriiklikke nõudeid pead rakendada ma ikka ühtemoodi, aga noh, see, kuidas rakendad neid, kuidas iga pank seaduse nõuetest aru saab, see on tõesti erinev ja, ja noh, see osalt tuginebki siis nagu ka riski hinnangul ja riskiisule, et kui suuri riske mingisugune pank võtta tahab, et sealt tegelikult tulenevalt kerisid sisse. Et on, on pangad, kes võib olla teenindavad natukene parema meelega Eestiga seotud, mitte Eestiga seotud isik või mitteresidente, on pangad, kes pigem nagu on suunatud ainult kohalike klientide teenindamisele. Ja sealt sealt tulevad erisused sisse.

**K: Kas pangad võivad võita ka siis tegelikult rahapesust, kui see peaks nende pankades toimuma.**
V: Danske näite kuldajal andis tegelikult ärimahtude mõttes suht väikeste mahtudega Eesti filiaal ligi kolmkümmend protsenti grupi tuludest vist, kui ma õigesti mäletan, et aga noh, see on sihuke lühiajaline benefit, et täna läheb hästi, aga kuid tegevus jõuab nagu riigiasutuste uurimisasutuste uurimisorbiiti, siis, siis see on läinud, sa kaotad tegelikult oluliselt rohkem. Sest et paar nädalat tagasi tuli uudis välja, et Danske, Taani kontsern siis eks ole on jõudnud Ameerika Ühendriikide uurimisasutustega kokkuleppele, maksavad trahviks kaks miljardit dollarit. Et see on ilmselgelt nagu oluliselt suurem, kui kunagi tegelikult nende mitteresidentide teenindamist teenis.

**K: Tänapäeval on paljud pangad hakanud aktsepteerima krüptot, kas sellel on ka ohukohti?**
V: Krüpto on hetkel jah, mõnevõrra vähem reguleeritud, eks ole, kui nii-öelda tavapärane raha maksevahendina. Aga krüptoga seonduvalt ka, et Euroopa Liit on järgmine aasta jõustamasi uut direktiivi, MiCa direktiiv, *Markets in Crypto-Assets directive*, et võiks seda ka vaadata, et sellega seonduvalt tegelikult pannakse peale krüpto vahendamisele päris karmid nõuded. Et sisuliselt noh, võib öelda seda, et selline anonüümsus kui selline järgmise pooleteise kahe aasta jooksul kaob ära, mis siiamaani andis nagu eelise rahapesijad, te olete, et hetkel selline jah, eelis on veel olemas, aga ka see pigem on nagu kadumas.

**K: Kas pangad teevad omavahel koostööd ehk näiteks kas nad jagavad omavahel klientide andmeid?**

V: Ei ole, otseselt seda ei ole ja see on alati niisugune tundlik teema olnud, et noh, meil on, eks ole, on ka selline direktiiv nagu isikuandmete kaitse direktiiv, määrus, sealt tegelikult rahapesu tõkestamisega seotud andmevahetus peaks olema välistatud, aga see on alati olnud siseriiklikult teema, mis kus pangad on pigem nagu tagasihoidlikud olnud, aga aga Eestis meil on natuke üle aasta tegutsenud selline suurepärane vahetusplatvorme, mille on arendanud välja kohalik startup, Salv äkki oled kuulnud - Salv on selline platvorm nagu *bridge*. Ja tegelikult selle alusel pangad vahetavad infot küsivadki, et palun näiteks näevad, et kontol on toimunud mingi tehing mis on tulnud mingisugust teisest pangast, tehing tekitab küsimusi, et selle platvormi asele platvormi kaudu on võimalik siis pankadel omavahel suhelda, et pank üks saab pank kahelt küsida, et, et me saime, nägime sellist tehingut, raha tuli sinu pangast, et palun selgita, mis sa selle kliendi kohta teavad, milline on nagu kogu aeg kogemus olnud, milliseid riske sa näed, et selles mõttes selline info vahel siis täitsa toimib. Ja see on üldnõuded jah, seda seadusetasudega võimaldavad see infovahetus, sellisel moel on ka nagu heakskiidu saanud finantsinspektsiooni rahapesu andmebüroo poolt. Et selles mõttes selles mõttes panga, vahetavad infot, aga sellist ühtset andmebaasi kui sellist jah, et seda ei ole, seda ei ole olemas ja seda hetkel ei ole ka võimalik tegelikult veel teha, et sel moel.
**K: Väga hästi. See on muidu minu küsimustega ühel pool. Suur aitäh küsimustele vastamise eest!**

LISA E
*Cross-case* analüüs

Tabel 2
*Cross-case analysis Eesti suurpankade kontaktisikute intervjuude põhjal*

| | Pangad | |
|---|---|---|
| Uuritav | SEB | Anonüümseks sooviv jääv pank |
| Mõju panganduse le | Negatiivne mõju panga usaldusväärsusele ning mainele<br>Negatiivne mõju majandusele | Negatiivne mõju mainele, langetab panga aktsiahinda kui tegemist on avaliku ettevõttega |
| Rahapesu kahju | Riigile suur kahju, mõjutab investeerimisotsuseid, majandust, klientide, partnerite usaldust, finantssektori mainet, maineriskist võivad suured ja olulised kokkulepped jääda sõlmimata | Mõju välisinvesteeringute mahule<br>Kahju mainele > juhtkonna väljavahetamine |
| Meeskond | Terve panga personal, suur roll kliendihalduritel<br>Tagatoaüksused | Eraldi koostatud üksused esimeses ja teises kaitseliinis<br>Suur osakaal on kliendihalduritel ning inimestel, kes suunavad kliente antud panka. |
| Automatiseeritus | Riskihindamisest klienditegevuse jälgimiseni | Tehingute jälgimine on automatiseeritud<br>Tuleviku suhtes tahetakse ka kliendiandmete kogumine ja uuendamine automatiseerida |
| Kahtlase tehingu tuvastamine | Tehingute maht<br>Riikidevahelised maksed<br>PEP (riikliku taustaga isik)<br>Tehingute jadad | Tuvastamine rahapesu andmebüroo kahtlaste tehingute tunnuste juhendi järgi<br>Finantsinspektsiooni põhi AML juhend<br>Hindama kliendi profiili > leidma ebatavapäraseid tehinguid |
| Eestis kogemus rahapesus | Mõned negatiivsed kogemused<br>Pikk protsess kindlaks rahapesuga kindlakstegemisel<br>Võimalus õppida antud juhtumitest | Eesti geograafiline asukoht soosib rahapesu, kuna on ligidal lääne-idapiirile (ida poolt tulev kuritegevuslik raha proovib liikuda Euroopa pangandussüsteemi)<br>Positiivselt vaadates on Eesti läbipaistev, kuna Eesti on väike keskkond ning siin on väikesed finantssüsteemid > suuremad summad jäävad silma.<br>E-residentsusega kodanike üldised pangad ei võta vastu |
| Regulatsioonid | Euroopa direktiivid<br>RahaPTS (Rahapesu ja terrorismi rahastamise tõkestamise seadus) | Hoolsusmeetmete riski juhtimise süsteem > Finantsinspektsiooni soovituslik juhend |

| | | |
|---|---|---|
| | Rahvusvaheliselt FATF (*Financial Action Task Force*)<br>Riigikogu seadused<br>Finantsinspektsiooni soovituslik juhend „Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks“ | Kolm kaitseliini:<br>1) Esimene kaitseliin õpib tundma klienti ning kontrollib kas on vastavuses sellega, mida klient on pangale öelnud.<br>2) Teine kaitseliin ehk vastavuskontrolli funktsioon tegeleb kaasuste uurimisega, mida esimene kaitseliin on neile edastanud. Töötab välja erinevaid metodoloogiat, kuidas hinnata rahapesuga seonduvaid riske ning kliente. Teostab kontrolli esimese kaitseliini üle.<br>Kolmas kaitseliin ehk siseaudit hindab nii esimese kui ka teise kaitseliini tegevust. |
| Regulatsioonide erinevus pankade vahel | Kindlad regulatsioonid pankade vahel<br>Turuosalisi vähe<br>Valib milliseid kliente lubab oma panka > riskiisu kõrgema riskiga klientide suhtes | Ühtepidi nõuded<br>Erinevus on selles, kuidas pank neid rakendab, osad pangad eelistavad teenindada Eestiga seotud isikuid, osad aktsepteerivad ka mitteresidente > panga riskiisu |
| Rahapesu kasulikkus pangale | Finantsmahtude pealt jah, kuid mainerisk on liiga kõrge hind, et sellega riskida. | Ärimahtudes suhtes küll, kuid see on lühiajaline kasum.<br>Jõudes riigiasutuse uurimisasutuste uurimisorbiiti, siis kahju on tunduvalt suurem kui saadad kasum |
| Karistused | Vastutatavad pangatöötajatele, panga juhtkonnale väärteomenetluse kuid ka kuriteomenetluse korras<br>Pangale kui juriidilisele isikule | Tippjuhtkond ja seotud otsesed isikud<br>Kriminaalmenetlused<br>Trahvid<br>Vanglakaristused |
| Digimaailma võimalused | Pettused (näiteks pangapettused või investeerimis petuskeemid) ning sealt saada tulu puhtaks pesemine<br>Kiired maksed<br>Uued tegevusvaldkonnad ning tööstusharud (näiteks kinnivaraarendus või *peer-lending crypto*)<br>Automatiseerimine, tehisintellekt, *machine-learning* | E-residentsus<br>Pettused (näiteks krüpto kelmused) |

| | | |
|---|---|---|
| Krüpto riskid | Toimib kiiremini kui sularahaga arveldamine<br>Sarnane sularahaga – anonüümne<br>Võimalus tuvastada tehingute jadasid, aga suures plaanis on anonüümne<br>Kontrollmehhanismide abil saab riske vähendada | Vähem reguleeritud kui tavapärane raha maksevahendina<br>Euroopa Liit on jõustamas uut MiCa direktiivi, kus krüpto vahendamisele seatakse karmid nõuded, mis teeb anonüümsuse tagamise keeruliseks<br>Praegu anna eelise rahapesijatele, aga tulevikus on see eelis kadumas |
| „Tunne oma klienti“ | Annab võimaluse teada, milliseid tehinguid klient teeb antud pangas ning miks ta valis antud panga selleks<br>Võimaldab kliendiriski adekvaatsemalt ja detailsemalt hinnata<br>Negatiivseks küljeks on kliendiandmete korjamine, mis on ebaproportsionaalselt koormav<br>Dünaamiline tunne oma klienti vs kliendi tegevusalast lähtuv tunne oma klienti<br>Klientide poolne negatiivne kogemus, osad peavad seda liigselt koormavaks | Tugisammas riskide hindamisel - annab turuosalistele hea raamistiku ning riskifaktorid<br>Efektiivselt manuaalselt rakendada on keeruline ning tehnilised lahendused ei ole alati efektiivselt toetama andmekogu analüüsi<br>Automaatkontrollid ei ole nii head nagu nad võiksid olla |
| Rahapesu kindlaks tegemise viisid | Ettevõttel omandistruktuuri kindlakstegemine, uurimine, mis füüsilised isikud teenivad antud ettevõtetega kasumit ning nende tausta uurimine (kliendiriski hindamine)<br>Äritehingute, kaubavahetuslepingute vaatamine | Kahtlaste tehingute uurimine, kliendiga ühendust võtmine ja selgituste otsimine ja vajadusel rahapesu andmebürood teavitada |
| Pankade vaheline koostöö | Otseselt puudub vastavalt andmekaitseseadusele<br>Eesti suurpangad kasutavad Salve suhtlustarkvara, kus jagatakse omavahelise info jagamiseks | Otseselt puudub, kuna isikuandmete kaitse direktiiv<br>Eestis tegutsev startup Salv, kus pangad jagavad omavahel infot |

Allikas: Autori koostatud Eesti suurpankade esindajate intervjuude põhjal

**Summary**

PREVENTION OF MONEY LAUNDERING AND FINANCING TERRORISM BY THE EXAMPLE OF MAJOR ESTONIAN BANKS

Enrik Lillemaa

Preventing money laundering and terrorist financing is one of the biggest challenges in banking, which financial institutions must actively and effectively monitor and implement due diligence measures.

In the theoretical work, the author introduced which regulations and laws banks follow to ensure the prevention of money laundering and terrorism. More precisely, banks use the guidelines and recommendations created by Estonian legislation, the Financial Supervision Authority, and the Estonian Financial Intelligence Unit. Ineffective prevention leads to a bad reputation for the state and the bank, which can have an impact on foreign investments, which in turn leads to wider economic losses.

As part of the empirical work, in-depth interviews were conducted with contact persons of various large Estonian banks, who explained how they regulate the prevention of money laundering and terrorist financing, what risks it involves, how it affects the bank and the country, and future opportunities to prevent money laundering and terrorist financing. From the information obtained from both interviews, the author made a cross-case analysis, from which it became clear that the prevention of money laundering and terrorist financing is very important from the financial institution's point of view. Failure to prevent money laundering and terrorist financing can have very severe penalties, including financial fines, loss of license, and even prison terms. Even more, it can have a strong impact on the bank's share price if it is a listed company. One of the most notorious examples of this is the Danske Bank case, where Danske Bank must pay $2 billion in fines. Banks do not have a direct database of customers, which makes it more difficult to identify money laundering, but the Estonian company Salv has found a solution to this, offering the opportunity for banks to contact one-on-one about suspicious transactions and to learn more about the person who made the suspicious transaction.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Enrik Lillemaa,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose „Rahapesu ja terrorismi rahastamise tõkestamine Eesti suurpankade näitel“ mille juhendaja on Maire Nurmet, 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.

*Enrik Lillemaa*

***15.01.2024***