TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Karistusõiguse osakond

Kaido Ivan

RAHAPESU VIRTUAALVÄÄRINGUTEGA JA SELLE TÕKESTAMISE MEETMED

Magistritöö

Juhendaja
Mag iur Indrek Tibar
Kaasjuhendaja
PhD Andreas Kangur

Tartu
2022

Sisukord

Sissejuhatus

Rahapesu all mõistetakse traditsioonilise käsitluse järgi ebaseaduslikult saadud tulu legaliseerimist läbi finantssüsteemi, muundades, paigutades vara ümber, kasutades selleks erinevaid varjamistegevusi või aidates kuritegelikus tegevuses osalejat ja püüdes kriminaaltulu suunata seaduslikku majanduskäibesse. Sel viisil legaliseeritud tulu aga kahjustab majanduse normaalset toimimist. Kui rahapesu protsess on edukalt läbitud, saab kurjategija või organiseeritud kuritegelik ühendus, nt märkimisväärseid summasid sularahas teeninud narkogrupeering või majandusalaseid süütegusid toimepanevad ettevõtjad oma ebaseadusliku tegevuse vilju nautida.

Viimastel aastatel Eestis laiemat kõlapinda ja negatiivset rahvusvahelist tähelepanu pälvinud suurtes mahtudes rahapesujuhtumid on seotud ülaltoodud viisil finantssüsteemi kuritarvitamisega. Nimetagem siin Danske Bank A/S Eesti filiaalis aastatel 2007-2015 toimunut[1], samuti teistele Eestis tegutsevatele pankadele järelevalveorganite määratud trahve rahapesu ja ettekirjutusi terrorismi rahastamise vastu võitlemise süsteemides tuvastatud vajakajäämiste eest.[2] Loomulikult kasutatakse rahapesu toimepanemiseks paljusid meetodeid ehk tüpoloogiaid, näiteks võib olla tegemist lihtsalt kuritegelikul teel saadud vara päritolu varjamise või füüsilise peitmisega. Rahapesu koosseis sisustatakse karistusseadustiku[3] (edaspidi KarS) § 394 kaudu viitega rahapesu ja terrorismi rahastamise tõkestamise seaduse[4] (edaspidi RahaPTS) § 4 lg-s 1 sätestatud tegudele.

Karistusõiguslikult rahapesu koosseisust rääkimiseks peab kasutatav vara pärinema kuritegelikust tegevusest ehk eelkuriteost. Eelkuritegu on rahapesu koosseisuline tunnus KarS § 394 lg-s 1 sätestatud kuriteokoosseisu mõttes. Eesti õiguses ei ole eelkuritegude loetelu piiratud ehk omaks on võetud kuritegude nn avatud kataloog (ingl *all crime approach*). Teoreetiliselt võib

[1] Väidetavalt liigutasid panga mitteresidentidest kliendid läbi filiaali rahapesukahtlusega 200 miljardit eurot. Riigiprokuratuur. Aastaraamat 2018. – https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2018/2018-riigiprokuratuuri-suudistusosakonnas (14.12.2021).
[2] Finantsinspektsioon, uudised. (2020) – https://fi.ee/et/uudised/swedbank-saab-trahvi-ja-ettekirjutuse-rahapesu-vastu-voitlemise-reeglite-rikkumise-eest (06.02.2022).
[3] Karistusseadustik. – RT I, 21.05.2021, 9.
[4] Rahapesu ja terrorismi rahastamise tõkestamise seadus. – RT I, 12.03.2022, 19.

seega eelkuriteoks olla mistahes karistusseadustikus sätestatud kuritegu, mille tulemusel on saadud rahapesu objekt.[5] Rahapesuna mõistetakse RahaPTS § 4 lg 1 kohaselt tegusid, millega suunatakse legaalsesse majandus- või rahakäibesse kuritegelikke vahendeid selliselt, et need kahjustavad riigi rahandus- ja majandussüsteemi korrapärast toimimist.

Rahapesu ja terrorismi rahastamise riske hinnatakse erinevatel tasanditel, nagu Euroopa Liidu, liikmesriigi ja RahaPTS järgi kohustatud isikute tasandil. Vabariigi Valitsuse rahapesu tõkestamise alane komisjon kinnitas 2021. aastal Eesti teise rahapesu ja terrorismi rahastamise alase siseriikliku riskihinnangu (NRA) tulemused. Riskihinnangu koostamise aluseks olid andmed aastatest 2017-2019 ning selle erianalüüsi osa puudutab perioodi 2020-2021. Riskihinnangu kohaselt on registreeritud rahapesukuritegusid ning seotud kohtulahendeid võrreldes muude kuritegude ning kohtulahenditega suhteliselt vähe. Keskmiselt on jõustunud 9-12 kohtuotsust aastas. Kohtus tõendatud juhtumite põhjal pannakse rahapesu eelkuriteod enamasti toime väljaspool Eestit ning sageli jäävad eelkuritegude toimepanijad kriminaalmenetluse käigus tuvastamata. Muude ohtude seas on suuremad ohud Eesti finantssektori jaoks seotud vahendite liigutamisega Eesti virtuaalvääringute teenusepakkujate kaudu.[6]

Rahapesu protsess koosneb traditsiooniliselt kolmest etapist või staadiumist. Ebaseadusliku tulu finantssüsteemi kandmine ehk paigutamine on esimene etapp, sellele järgneb laotamine ehk kihitamine, milles raha kantakse erinevate kontode vahel või teostatakse muid varjamistegevusi. Kolmas etapp on integreerimine, milles vara suunatakse legaalsesse majandusse, investeerides selle omakorda teistesse varadesse. Kirjelduse kohaselt lihtne protsess nõuab aga vähemalt algstaadiumis eriteadmisi[7] ja mingilgi määral toimepanijate organiseerituse taset. Seda läbiviivad isikud peavad tundma finantssüsteemi, järelevalve- ja uurimisasutuste töömeetodeid, et vältida nende poolset tähelepanu ja kuriteo avastamist.

[5] RKKK 3-1-1-34-05, p 21.

[6] Rahandusministeerium. Eesti rahapesu ja terrorismi rahastamise siseriiklik riskihinnang 2020. – https://www.fin.ee/finantspoliitika-valissuhted/rahapesu-ja-terrorismi-rahastamise-tokestamine/riskihinnangud (06.02.2022).

[7] Egmont Group Bulletin, Professional Money Laundering Facilitators, 2019 - https://egmontgroup.org/wp-content/uploads/2021/09/2019_Egmont_Group_Bulletin_Professional_Money_Laundering_Facilitators.pdf (12.04.2022).

Eriteadmistega spetsialiste on ka järjest laiemalt kasutusele võetavas finantstehnoloogia (ingl *fintech*)[8] valdkonnas, nagu ka krüptorahade[9], virtuaalvääringu rahakotiteenust[10] ja virtuaalvääringu vahetamise teenust pakkuvates ettevõtetes. Virtuaalvääringute kasutamine rahapesu protsessis lisab anonüümsust ja tehingute läbipaistmatus annab kurjategijatele võimaluse oma raha legaliseerimiseks. Kuigi virtuaalvääringute tehingute aluseks oleva plokiahela ja hajusraamatu tehnoloogia (*blockchain technology* ja *distributed ledger technology* -DLT)[11] kasutamisele on tehingud iseenesest avalikud, siis ülekannete peitmiseks saab kasutada erinevaid meetodeid, mis raskendab oluliselt varade liikumise jälgimist ja algse omaniku tuvastamist. Seetõttu kujutavad virtuaalvääringud (mh kõige paremini tuntud *bitcoin*) endast nende vahendamise ja kasutamise anonüümsuse, järjest laiema leviku ning kontrollimeetmete rakendamise keerukuse tõttu üha mastaapsemat ohtu finantssüsteemide usaldusväärsusele ja laiemalt kogu julgeolekule nii riikide tasemel kui globaalselt. FATF[12] ehk rahapesuvastane töökond on 2014. aastal maininud, et virtuaalvääringud on maksesüsteemide tulevik, kuid pakuvad kurjategijatele raha liigutamisel mõjusa vahendi kuritegude toimepanemiseks.[13]

Eesti on üks esimesi riike maailmas, kus asuti reguleerima alternatiivsete maksevahendite (praegu kasutatav mõiste on virtuaalvääring - VV) pakkujate tegevust. Kuna leiti, et infotehnoloogilised arengud võimaldavad regulatsioonidele mittealluvaid praktikaid rahapesuks, allutati 2008. aastal teenuse pakkujad RahaPTS regulatsioonile.[14] Virtuaalvääringute mõiste on avatud RahaPTS § 3 p-s 9, mille kohaselt on VV digitaalsel kujul esitatud väärtus, mis on digitaalselt ülekantav, säilitatav või kaubeldav ja mida füüsilised või juriidilised isikud aktsepteerivad maksevahendina, kuid mis ei ole ühegi riigi seaduslik maksevahend ega rahaline vahend. VV-d pakuvad õiguspärasel kasutamisel mitmeid eeliseid, nagu makse toimumise kiirus ja väiksemad tehingukulud. Potentsiaalselt kõrge rahapesuriskiga virtuaalvarad on osa tehnoloogilisest arengust ja nende aluseks olevat plokiahela süsteemi kasutavad teised teenusepakkujad ja arendajad,

[8] Mõiste kohta vt Euroopa Keskpank. - https://www.bankingsupervision.europa.eu/about/ssmexplained/html/fintech.et.html (14.12.2021).
[9] Autor kasutab töös mõisteid virtuaalvääring/virtuaalvara, krüptoraha/krüptovara ja *token* samas tähenduses.
[10] Vt mõiste kohta pt 1.3.
[11] DLT – ingl *distributed ledger technology* ehk hajusraamatu tehnoloogia on tehnoloogia liik, mis toetab krüpteeritud andmete hajutatud hoiustamist.
[12] FATF (*Financial Action Task Force*), prantsuse keeles *Group d'Action Financiere sur le Blanchment de Capitaux*, lühend GAFI ehk rahapesuvastane toimkond on 1989. aastal G7 valitsusjuhtide asutatud valitsustevaheline organ, mis kehtestab rahapesu ja terrorikuritegude rahastamise vastaseks võitluseks rahvusvahelisi standardeid.
[13] FATF Report. (2014). - https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (06.02.2022).
[14] Rahapesu andmebüroo (RAB 2020), Virtuaalvääringu teenuse pakkuja uuring. - https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b (22.11.2021).

kelle tegevuse käigus vahetavad VV-d samuti omanikku, nt tasu võtmine teenuse eest, e-kaubandus.

Samas, innovatiivsete tehnoloogiliste lahenduste arendajad, rääkimata krüptoäride pidajatest juhivad tähelepanu kõrge riski tõttu kehtestatud rahapesu tõrjumise meetmete liigsele tungimisele tehnoloogiamaastikule ja seeläbi kliendi jaoks lihtsamate ning mugavamate finantsteenuste suunas arengu pärssimisele.[15] Rahapesu ja selle eelkuritegude avastamine ning tõendamine muutub kuritegude rahvusvahelise mõõtme ja VV-de kasutuselevõtu tõttu järjest kompleksemaks ja tehnoloogiliselt keerukamaks. Seda suuremaid väljakutseid esitab selline areng valdkonda reguleerivatele organisatsioonidele ja riikide seadusandjatele, kes peavad esile kerkinud rahapesuriske kiiresti maandama. Sätestatud rahapesu tõkestamise meetmete riigisisene kehtestamine ja rangemate nõuete järgimine on vältimatu, sest sellest sõltub suuremas plaanis riigi maine ja majanduse toimimine. 2022. aasta kevadel hindab Eesti regulatsioonide tehnilist kooskõla FATF-i standarditega ning rahapesu tõkestamise süsteemide efektiivsust FATF-i regionaalne ekspertkomitee MONEYVAL.[16] Hindamise tulemusel võidakse riiki kohustada raporteerima hindajate antud soovituste täitmisest FATF-ile, millega kaasneb rahvusvahelise üldsuse negatiivne tähelepanu ning halduskoormus. Järgneva kordushindamise ebarahuldavate tulemuste korral nimetatakse riik kõrge rahapesu riskiga jurisdiktsiooniks ning see mõjutab kogu selle riigi era- ja juriidiliste isikute majandustegevust. Oluliste puuduste korral, näiteks krüptovääringute valdkonnas on võimalik risk Eesti lisamine nn halli nimekirja. See halvendaks siin tegutsevate pankade ja teiste ettevõtete võimalusi finantsturgudelt raha kaasata, takistaks välismaksete teostamist ning rahvusvaheliste tehingute läbiviimist.[17]

Rahapesu tõkestamiseks kehtestatud regulatsioonide alusel peavad RahaPTS § 2 mõistes juriidilised ja füüsilised kohustatud isikud rakendama hoolsusmeetmeid (ingl *customer due diligence*). Hoolsusmeetmete rakendamine tähendab VV ettevõtja jaoks tegelikkuses väga suuri investeeringuid tehnoloogilistesse lahendustesse ja süsteemidesse ning kvalifitseeritud tööjõu palkamiseks ja nende väljaõppeks. Viimastel aastatel VV valdkonnas järjest karmistatud nõuete

[15] Vedler, S. „Eesti finantssüsteemi ähvardab halli nimekirja kukkumine. Oht tuleb krüptoärist". — Eesti Ekspress 09.02.2022.
[16] 1997. aastal Euroopa Nõukogu ministrite komitee asutatud rahapesu ja terrorismi rahastamise vastase võitlusega tegelev ekspertkomitee, ingl *Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism*.
[17] Eesti Pank, Finantsstabiilsuse ülevaade, 2/2021, lk 4. https://www.eestipank.ee/publikatsioonid/finantsstabiilsuse-ulevaade/2021/finantsstabiilsuse-ulevaade-22021 (02.07.2022).

valguses, nagu VV teenusepakkujale tegevusloa taotlemisel RahaPTS-s kehtestatud tingimused, on kohane analüüsida rahapesu tõkestamisel avalik-õiguslikele ja eraõiguslikele isikutele pandud kohustuste vahekorra üle. VV on selles kontekstis aktuaalne näide kiiresti arenevast tehnoloogilisest ja õiguslikust maastikust, mille muutused hõlmavad enamikke meie eluvaldkondi ja pälvivad laia avalikkuse tähelepanu.

Eeltoodust tulenevalt on autor seisukohal, et Eesti Vabariigi kehtiv regulatsioon ei ole piisavalt tõhus virtuaalvääringutega teostatava rahapesu tõkestamiseks ja tuvastamiseks. Seetõttu on raskendatud kriminaalmenetluses eelkuritegude tõendamiseks andmete kogumine. Autor seab eesmärgiks probleemi analüüsida ja välja selgitada, kas kehtiv õigus pakub ajakohaseid võimalusi VV-de abil toime pandava rahapesu tuvastamiseks ja tõkestamiseks ning milline oleks sellega seoses tasakaal avaliku sektori ja eraõiguslikele isikutele pandud kohustuste vahel selles valdkonnas.

Töö uurimisküsimused on:

1) Millised on virtuaalvääringute käibega seotud suurimad rahapesuriskid ja kas käesoleval ajal rakendatavate tõkestusmeetmetega on võimalik neid riske maandada?

2) Milliseid meetmeid oleks võimalik rakendada efektiivseks võitluseks virtuaalvääringute abil toimepandava rahapesuga?

Küsimustele vastamiseks on autor kasutanud kvalitatiivset uurimismetoodikat, et allikates toodud seisukohti sisuliselt läbi töötada ning nendest tulenevalt oma järeldusteni jõuda. Autor analüüsib Eesti rahapesuvastase tõkestamise süsteemi ja seda valdkonda reguleerivat seadusandlust ning püüab leida võimalusi efektiivseks lahenduseks, milles on ühendatud nii eraõiguslikud kui avalik-õiguslikud preventiivsed ja sanktsioneerivad kriminaalõiguslikud meetmed. Uurimisküsimustele vastamisel võrdleb autor mõnede välisriikide õigusaktides sätestatud ajakohaseid nõudeid ja järeldused teeb autor deduktiivse meetodi abil.

Käesolev töö on jaotatud kolme peatükki. Esimeses peatükis käsitleb autor rahapesu olemust, kujunemislugu ja rahvusvaheliselt sätestatud nõudeid rahapesu tõkestamisel, pidades silmas alternatiivsete maksevahendite ja tehnoloogilise arenguga seotud aspekte. Laiem ajalooline ja rahvusvaheliste õigusallikate käsitlus on vajalik rahapesu ja VV-ga seotud probleemide spetsiifika tõttu. Nimelt on rahapesu tõkestamisel võimalik edu saavutada rahvusvahelises koostöös, sellest saadud kogemustest ning järelevalveasutuste ja turuosaliste vahel kokku lepitud meet-

meid rakendades. Seonduvates alapeatükkides annab autor ülevaate rahapesuvastaste meetmetega seotud arengutest Eestis ning kirjeldab taustsüsteemi loomiseks VV-d ning analüüsib nende õiguslikku staatust. Teises peatükis kirjeldab autor rahapesu protsessi ebaseaduslikes tegevustes VV-tega, võrreldes neid rahapesuga seni tuvastatud traditsioonilisematel viisidel ja käsitleb järgnevas alapeatükis VV-tega seotud olulisemaid riske, mida on tuvastatud rahvusvaheliste organisatsioonide uuringutes, samuti teised riigid ja Eesti oma riskihinnangutes. Riskidena käsitleb autor VV käivet konkreetsetest ebaseaduslikest tegevustest, mis analüüside kohaselt ja autori hinnangul võivad realiseerumisel kõige enam riigi rahandus- ja majandussüsteemi kahjustada. Kolmandas peatükis pakub autor töös tuvastatud riskide ja regulatsioonide puudujääkide põhjal võimalikke lahendusi rahapesu tõkestamiseks arenevas VV tehnoloogilises valdkonnas ning vastab püstitatud uurimisküsimustele.

Krüptovääringute ja rahapesu seoste kohta on Tartu Ülikoolis 2016. aastal kaitsnud magistritöö teemal „Rahapesu *bitcoin´*idega“ T. Morel, kes analüüsis, milline võiks olla *bitcoin´*ide õiguslik käsitlus rahapesu regulatsioonis ja leidis oma järelduses, et tollal kehtinud RahaPTS-i regulatsioon hõlmab krüptorahasid ja on piisav, et takistada raha pesemist *bitcoin´*idega. 2021. aastal on T. Pilberg oma töös „Krüptovaluuta karistusõiguses“ käsitlenud krüptovaluutadega seonduvate kuritegude koosseise ja nende läbi kahjustatud isikute õiguste kaitset.

Allikatena kasutab autor eesti- kui inglisekeelseid materjale, rahvusvahelisi, Euroopa Liidu (konventsioonid, AMLD I-V) ja Eesti õigusakte, õigusalast kirjandust, teadusartikleid, teiste Euroopa riikide ja Eesti riskihinnanguid (2021. aastal), organisatsioonide uuringuid (RAB, FATF 2021. aastal) hinnanguid ja juhiseid, hoiatusi ja arvamusi (ESMA, EBA, Rahandusministeerium, Finantsinspektsioon), Europoli riskianalüüse. Kasutatud on ka Eesti ja välisriikide uudisartikleid ning virtuaalvara teemadel internetis avaldatud ajakohast teavet ja statistikat, paljud allikaid on vaid veebis avaldatud ning veebipõhiselt kättesaadavad.

Magistritöö märksõnad Eesti märksõnastikust on: rahapesu, virtuaalvääringud, süüteod.

1. Rahapesu tõkestamise nõuete kujunemine ja virtuaalvääringute kasutamine rahapesus

1.1 Rahapesu olemus, rahapesu tõkestamise regulatsioon rahvusvaheliselt

Rahapesu võib traditsiooniliselt kirjeldada protsessina, milles eelkuritegudest saadud vara kantakse selle päritolu varjates finantssüsteemi ja legaliseeritakse see majanduskäibes muu varana. Rahapesu võib olla suhteliselt lihtne tegevus kohalikul ja riiklikul tasemel või keerukas protsess, mis hõlmab paljusid isikuid, jurisdiktsioone, rahvusvahelisi vahendajaid ja finantsasutusi.

Rahapesu tulemuslikuks uurimiseks tuleb läbida traditsiooniline kriminaalmenetlus eelkuriteo toimepanemise tõendamiseks ja n-ö finantsmenetlus, mille eesmärk on välja selgitada kriminaaltulu ning selle võimalik legaliseerimine ehk rahapesu.[18]

Autor peab vajalikuks kirjeldada rahapesu tõkestamiseks kehtestatud meetmeid nende ajaloolise kujunemise kaudu, mis võimaldab paremini mõista tänapäeval VV seotud probleeme, pidades silmas nende riikide ülest mõõdet nii võimalikul ebaseaduslikul kasutamisel kui vältimatult ühtsete rahvusvaheliste regulatsioonide kehtestamisel. Selles käsitluses selguvad põhimõtted, mille alusel kehtestatakse rahapesu tõkestamise kriminaalõiguslikud ja preventiivsed meetmed.

Esimesed konkreetsed meetmed rahapesu tõkestamiseks sätestati 1970. aastal Ameerika Ühendriikide pangasaladuse seaduses (ingl *The Bank Secrecy Act*). Seadus nägi ette, et pank peab säilitama teatud andmeid oma klientide tehingute kohta ning teavitama Ameerika Ühendriikide rahandusministeeriumit (ingl *US Treasury Secretary*) tehingutest suuremate summadega. Selles seaduses sätestati tänapäevases mõistes tehingu andmete säilitamise kohustus ja teatamiskohustus.[19]

Euroopa tasandil valmis 1980. aastal Euroopa Nõukogu valikkomitee soovitus, milles anti juhised pankadele, kuidas takistada tundmatute isikute anonüümsete kontode avamist ning juhiti

[18] Feldmanis, L., Ploom, T. Rahapesu kriminaliseerimine: kelle suhtes ja millise põhjendusega. – Juridica 2007/3, lk 180 - https://www.juridica.ee/article_full.php?uri=2007_3_rahapesu_kriminaliseerimine_kelle_suhtes_ja_millise_p_hjendusega_&pdf=1 (05.02.2022).

[19] Financial Crimes Enforcement Network (FinCEN). – https://www.fincen.gov/history-anti-money-laundering-laws (07.09.2021).

tähelepanu pankadevahelise rahvusvahelise koostöö ja teabevahetuse parandamise vajadusele.[20] Rahapesu mõistet kasutati esmakordselt karistusõiguses 1982. aastal Ameerika Ühendriikides Floridas tehtud kohtuotsuses[21], mis käsitles Kolumbia narkokaubanduse ebaseadusliku tulu konfiskeerimist.

Rahapesu tõkestamise süsteemi toimimiseks on oluline rahapesu kriminaliseerimine, võimaldamaks karistusmeetmete rakendamist. Kuriteo toimepanija karistamisega mõjutatakse teda hoiduma uute kuritegude toimepanemisest ning teisalt välditakse ebaseadusliku vara seaduslikku majanduskäibesse kandumist. Nii tõkestusmeetmete rakendamiseks kui kriminaal- ja kohtumenetluseks peavad olema loodud vajalikud seaduslikud eeldused ja antud võimalused.

1986. aastal võeti vastu Ameerika Ühendriikide rahapesuseadus (ingl *Money Laundering Control Act*). Senine pangasaladuse seadus ei osutunud rahapesu tõkestamiseks tõhusaks, uue rahapesuseadusega kriminaliseeriti rahapesu föderaalkuriteona. Pangasaladuse seaduse kohaldamisel ilmnenud rahapesu meetod *smurfing* ehk *structuring* muudeti kuriteoks. *Smurfing* on sisuliselt suuremate rahasummade väiksemate summadega tehinguteks jagamine, et mitte ärata pangaülekandeid tehes tähelepanu ehk iga üksik tehing jääks alla piirsumma, mida ületades tekib pangal pangasaladuse kohaselt teatamiskohustus.[22]

Rahvusvahelisel tasandil võeti 1988. aastal Viinis vastu Ühinenud Rahvaste Organisatsiooni narkootikumide salakaubaveo vastu võitlemise konventsioon[23], mis esimese rahvusvahelise konventsioonina määratles rahapesu kuriteona.

1990. aastal võeti vastu Euroopa Nõukogu rahapesu ning kriminaaltulu avastamise, arestimise ja konfiskeerimise nn Strasbourg´i konventsioon.[24] Konventsiooni eesmärk oli luua kurjategijatelt nende tegevuseks vajalike vahendite ja selle tulemusena saadud tulu konfiskeerimiseks tõhus rahvusvahelise koostöö mehhanism. Konventsioonist on tänaseks koostatud uus versioon

---

[20] Council of Europe. Recommendation No (80) 10 of the Commitee of Ministers to Member States on Measures Against the Transfer and the Safekeeping of Funds of Criminal Origin, 1980. – http://www.coe.int/t/dghl/monitoring/moneyval/Instruments/Rec%2880%2910_en.pdf (04.08.2021).

[21] United States District Court for the Southern District of Florida (1982), "United States of America v. Four million two hundred and fifty-five thousand, six hundred and twenty-five dollars and thirty-nine cents" – https://law.justia.com/cases/federal/district-courts/FSupp/551/314/2366254/ (15.02.2022).

[22] Brown, C. Dividing Your Deposits Is a Federal Crime. Tennessee Bar Journal (2011). Vol. 47, No. 10, https://www.tba.org/?pg=Articles&blAction=showEntry&blogEntry=9664 (17.02.2022).

[23] Narkootiliste ja psühhotroopsete ainete ebaseadusliku ringluse vastane Ühinenud Rahvaste Organisatsiooni konventsioon. 10.10.2000. – RT II 2000 15, 92.

[24] Euroopa Nõukogu rahapesu ning kriminaaltulu avastamise, arestimise ja konfiskeerimise konventsiooni ratifitseerimise seadus. 01.06.2002. – RT II 2000, 7, 41.

- rahapesu ning kriminaaltulu avastamise, arestimise ja konfiskeerimise ja terrorismi rahastamise konventsioon, ehk nn Varssavi 2005. aasta konventsioon.[25]

1989. aastal otsustasid seitsme suure tööstusriigi ehk G7 (Ameerika Ühendriigid, Kanada, Jaapani, Saksamaa, Prantsusmaa, Suurbritannia ja Itaalia) valitsusjuhid ning Euroopa Komisjon luua rahapesu vastu võitlev rahapesuvastase töökonna *Financial Action Task Force* ehk FATF-i. Töökonna eesmärgiks seati rahapesu meetodite ja selle ulatuse väljaselgitamine ning rahvusvahelise koostöö edendamine rahapesuvastases võitluses. 1990. aastal esitas FATF nelikümmend soovitust rahapesuga võitlemiseks.[26] Soovitusi on hiljem üle vaadatud ja uuendatud, et kajastada muutusi rahapesu tehnikates ja meetodites.[27] FATF-i soovitused põhinesid 1988. aastal Baseli pangandusjärelevalve komitee (*The Basel Committee on Banking Supervision* - BCBS) regulatsioonil[28], milles soovitati muuhulgas ebaseaduslike tehingute vältimiseks kohaldada protseduure pangatoiminguid teostavate isikute identifitseerimiseks. Baseli komitee juhistega kasutusele võetud printsiibid on tänapäeval jätkuvalt kasutusel, neid tuntakse kliendi tuvastamisel ja äritegevuse seirel hoolsuskohustuse täitmise (ingl *Customer Due Diligence* ehk CDD) ja tunne oma klienti põhimõtetena (ingl *Know Your Customer* ehk KYC). Baseli pangajärelevalve komitee asutasid G-10 riikide (Belgia, Kanada, Prantsusmaa, Saksamaa, Itaalia, Jaapan, Luksemburg, Madalmaad, Hispaania, Rootsi, Šveits, Ühendkuningriik, Ameerika Ühendriigid ning Euroopa Komisjon ja Euroopa Keskpank on vaatleja staatuses)[29] keskpankade presidendid ja komiteesse kuuluvad pankade usaldatavusnormatiivide täitmise eest vastutavate asutuste esindajad.

Paljuski FATF-i 1990. aasta soovitustest ja põhimõtetest lähtudes võttis Euroopa Ühenduste Nõukogu 1991. aastal vastu esimese rahapesuvastase direktiivi 91/308/EMÜ[30] (*Anti-Money Laundering Directive* - AMLD I). Direktiiv oli suunatud krediidi- ja finantsasutustele, kohustades neid rakendama preventiivseid meetmeid rahapesu tuvastamiseks. Selles määratleti

[25] Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198). – https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/198 (15.01.2022).
[26] FATF Recommendations (2012). Mitteametlik tõlge eesti keelde: Rahapesu ning terrorismi ja massihävitusrelvade leviku rahastamise vastu võitlemise rahvusvahelised standardid. FATF-i soovitused (2012). – http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Estonian.pdf (15.01.2022).
[27] Egmont Group. Money Laundering and the Financing of Terrorism. – https://egmontgroup.org/en/content/money-laundering-and-financing-terrorism (14.02.2022).
[28] Prevention of criminal use of the banking system for the purpose of money laundering. - http://www.bis.org/publ/bcbsc137.pdf (03.02.2022).
[29] International Monetary Fund. – https://www.imf.org/en/About/Factsheets/A-Guide-to-Committees-Groups-and-Clubs#G10 (08.02.2022).
[30] Euroopa Nõukogu direktiiv, 10. juuni 1991, rahandussüsteemi rahapesu eesmärgil kasutamise vältimise kohta (91/308/EMÜ). – EÜT L 166, 28.06.1991, lk 77–83.

mõiste „rahapesu" uimastikuritegude kaudu ja kehtestati kohustused ainult rahandussektorile. Võrreldes 1988. aasta Viini konventsiooni ja 1990. aastal Strasbourg'i konventsiooni eelkõige rahvusvahelise narkokuritegevuse ohjamiseks kujundatud repressiivsele lähenemisele oli selle direktiivi eesmärgiks luua võimalused tuvastada rahapesu enne kriminaalmenetluse (ingl *criminal investigation*) alustamist ehk kasutada preventiivseid vahendeid. Direktiivi preambulas selgitatakse, et kuigi rahapesu tuleb tõkestada peamiselt kriminaalõigusmeetmete kaudu ning kohtute ja õiguskaitseasutuste rahvusvahelise koostöö raames, ei peaks kriminaalõiguslik lähenemine olema ainus viis rahapesu tõkestamiseks. Ennetavad meetmed saab juba varem kasutusele võtta, tõhustades kontrolli finantssüsteemis. Rahandussüsteemi rahapesuks kasutamise vältimine on ülesanne, mida selle eest vastutavad asutused ei saa täita, tegemata koostööd krediidi- ja finantseerimisasutuste ja nende järelevalveasutustega.[31] Nagu direktiivi nimest nähtub, et see oli suunatud finantsasutustele – direktiiv pidi olema mehhanismiks rahapesu vältimiseks krediidi- ja finantseerimisasutuste kaudu teostatavate tehingute ning teatud kutsealade jälgimise teel.

2000. aastal võttis ÜRO Peaassamblee vastu rahvusvahelise organiseeritud kuritegevuse vastu võitlemise konventsiooni (nn Palermo konventsioon[32]). Konventsiooniga kohustati osalisriike kehtestama regulatsioonid ja järelevalve kord rahapesuriskiga finantsasutuste ja muude asutuste tegevuse üle. Konventsiooni reguleerimisala hõlmab raskeid kuritegusid ja selle artiklis 6 määratleti rahapesukuriteod. Lisaks reguleeriti osalisriikide vastastikust õigusabi kuritegude uurimisel, kuriteo toimepanija karistamisel ja kohtumenetluse korraldamisel ning õiguskaitseasutuste koostööd.

2001. aastal võtsid Euroopa Parlament ja Nõukogu vastu direktiivi 2001/97/EÜ[33] (AMLD II), mis laiendas kohustatud isikute ringi väljapool finantssektorit, nt notarid, advokaadid ja raamatupidajad, kellele seati samuti kohustus tuvastada oma kliente, säilitada andmeid tehingute kohta ja teha koostööd rahapesu tõkestamise eest vastutavate asutustega. FATF avaldas 2003. aastal rahapesu tõkestamiseks uuendatud 40 soovitust, mis laiendas samuti kohustatud isikute ringi, kasutades mõistet mittefinantsteenuseid pakkuvad määratud ettevõtjad ja kutsetöötajad (ingl *designated non-financial businesses and professions*, lühend DNFBP).[34]

[31] *Ibid.,* lk 77.
[32] Rahvusvahelise organiseeritud kuritegevuse vastu võitlemise Ühinenud Rahvaste Organisatsiooni konventsioon - RT II 2003, 1, 1.
[33] Euroopa Parlamendi ja nõukogu direktiiv 2001/97/EÜ, millega muudetakse nõukogu direktiivi 91/308/EMÜ rahandussüsteemi rahapesu eesmärgil kasutamise vältimise kohta. – EÜT L 344, 28.12.2001, lk 76–82.
[34] FATFi soovitused (2012), lk 19-20.

2005. aastal võeti vastu kolmas rahapesualane direktiiv 2005/60/EÜ[35] (AMLD III), mis pidi muuhulgas tagama FATF-i 2003. aastal uuendatud soovituste ühetaolise liikmesriikide ülese rakendamise. Direktiiv võttis kasutusele rahapesu tõkestamise põhimõttena riskipõhise lähenemise. Sätestati, et kuna keerulistes rahapesu operatsioonides osalevad sageli juriidilised isikud, tuleb karistusi rakendada ka juriidiliste isikute tegevuse suhtes. Samuti märgiti preambulas, et direktiiv peaks kohalduma sellega hõlmatud asutuste ja isikute Interneti-keskkonnas toimuvale tegevusele.[36] Euroopa Nõukogu avas 2005. aastal allkirjastamiseks rahapesu ning kriminaaltulu avastamist, arestimist ja konfiskeerimist ning terrorismi rahastamist käsitleva Varssavi konventsiooni.[37] Konventsioon seadis osalisriikidele ülesandeks tagada õiguslik raamistik ja kohaldada meetmeid, mis võimaldaks tuvastada ja kontrollida klientide isikusamasust, täita ärisuhetes hoolsusnõudeid ja kasutada riskide tuvastamise meetodeid, täita rahapesu teavitamiskohustust, dokumenteerida andmeid ja tehinguid, pakkuda töötajatele väljaõpet. Konventsiooni artiklis 9 vähendati eelkuritegude tõendamise nõudeid, mille kohaselt eelnev või samaaegne süüdimõistmine eelkuriteo eest ei ole rahapesus süüdimõistmise eeldus. Kui varem oli kohustus näidata konkreetse eelkuriteo seost rahapesuga, siis konventsiooni kohaselt on võimalik isik rahapesus süüdi tunnistada juhul, kui on tõendatud vara pärinemine mistahes kuriteost.

Reageerimaks vajadusele ühtlustada karistusi raskete piiriüleste kuritegude eest, avardati Lissaboni leppega[38] märgatavalt Euroopa Liidu karistusõiguslikku pädevust ja pärast seda on liidu karistusõiguse mõju aina kasvanud. Euroopa Liidu toimimise lepingu (ELTL)[39] artikli 83 lõike 1 järgi võivad Euroopa Parlament ja Nõukogu direktiivide abil kehtestada miinimumeeskirju kuritegude ja karistuste määratlemiseks eriti ohtlike piiriülese mõõtmega kuriteoliikide puhul, milleks on ka rahapesu. Lisaks saab Euroopa Liit ELTL artikli 83 lõike 2 kohaselt kuritegude ja karistuste määratlemise miinimumeeskirju kehtestada ka juhul, kui õigusnormide lähendamine osutub möödapääsmatuks, et tagada liidu poliitika valdkonnas, kus ühtlustamismeetmeid

[35] Euroopa Parlamendi ja nõukogu direktiiv 2005/60/EÜ, 26. oktoober 2005, rahandussüsteemi rahapesu ja terrorismi rahastamise eesmärgil kasutamise vältimise kohta. – ELT L 309, 25.11.2005, lk 15–36.
[36] *Ibid.*, lk 5.
[37] 2022. a aprilli seisuga ei ole Eesti Varssavi konventsiooni ratifitseerinud - https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=198 (13.04.2022). Vabariigi Valitsuse menetluses on Rahapesu ning kriminaaltulu avastamise, arestimise ja konfiskeerimise ning terrorismi rahastamist käsitleva Euroopa Nõukogu konventsiooni ratifitseerimise seadus 583 SE - https://www.riigikogu.ee/tegevus/eelnoud/eelnou/9fd047bc-3e4e-4782-9e14-a9759eae254f (14.04.2022).
[38] Lissaboni leping, millega muudetakse Euroopa Liidu lepingut ja Euroopa Ühenduse asutamislepingut. - ELT C 306, 17.12.2007.
[39] Euroopa Liidu toimimise leping (konsolideeritud versioon). – ELT C 326, 26.10.2012.

on rakendatud.[40] Euroopa Liidu pädevus kriminaalõiguslike meetmete vastuvõtmiseks on suurenenud ning liikmesriigid peavad vastuvõetud meetmetega arvestama ka siseriikliku kriminaalpoliitika kujundamisel. Üksnes võimalikult ühetaoline EL-i sisene rahapesuvastane regulatsioon aitab tagada meetmete efektiivsuse ja seatud eesmärkide saavutamise.[41]
2012. aastal andis FATF välja uued, riskipõhised rahapesu ja terrorismi rahastamist tõkestavad soovitused. Kõrge riskiga valdkondades karmistati nõudeid ja soovitusi laiendatud uute ohtude vastu võitlemiseks ja riskide maandamiseks. Riskipõhine lähenemisviis annab finants- ja krediidiasutustele ning teistele kohustatud isikutele võimaluse maandada enda tuvastatud riske kõige enam tähelepanu vajavates sektorites.[42] Täpsemalt kirjeldab autor VV osa puudutavaid FATF-i muudatusi edasises käsitluses.

2015. aastal vastu võetud Euroopa Liidu rahapesu direktiivi 2015/849[43] (AMLD IV) eesmärk on kaitsta finantssüsteemi rahapesu ja terrorismi rahastamise tõkestamise, avastamise ja uurimise abil. Sellega suunati riike reeglipõhiselt regulatsioonilt üle minema riskipõhistele lähenemisviisidele ja seiremeetmetele, lisaks anti erasektorile senisest suurem vastutus rahapesu tõkestusmeetmete kasutuselevõtuks ja laiendati rahapesu eelkuriteo mõistet. Võimalikult laiast eelkuritegude ringi määratlusest soovitab lähtuda ka FATF. Riikidel on võimalik valida eelkuritegude määratlemisel erinevate lähenemisviiside vahel, nt hõlmata kõik õigusrikkumised, valida eelkuritegude loetelu. Olenemata valitud lähenemisviisist peaksid eelkuriteod hõlmama õigusrikkumisi igast FATF-i soovitustes välja toodud õigusrikkumiste kategooriast. Kuritegude täpsem definitsioon ja konkreetsed tõsised rikkumised on antud riikidele siseriiklikuks otsustamiseks. Samuti soovitab FATF kohaldada rahapesu igat liiki vara suhtes, mis kujutab endast kuritegevusest saadud tulu, sõltumata selle väärtusest.[44]

---

[40] Truu, M. Pilk karistusõiguse lähtele: määratletuse põhimõttest süüteokoosseisu sõnastamisel ja tõlgendamisel. – Juridica 2019/9, lk 676 - https://www.juridica.ee/article_full.php?uri=2019_9_pilk_karistus_iguse_l_htele_m_ratletuse_p_him_ttest_s_teokoosseisu_s_nastamisel_ja_t_lgendami&pdf=1 (02.02.2022); vt ka Rosin, K. Euroopa Liidu kriminaalõiguse areng Lissaboni leppe jõustumise järel. – Juridica 2015/IX: lk 659 - https://www.juridica.ee/article_full.php?uri=2015_9_euroopa_liidu_kriminaal_iguse_areng_lissaboni_leppe_j_ustumise_j_rel&pdf=1 (02.02.2022).
[41] Sootak J. Karistusõigus. Üldosa. Kirjastus Juura, Tallinn, 2018, lk 657 - https://karistusseadustik.juuraveeb.ee/ (04.02.2022).
[42] FATFi soovitused (2012) lk 9 - 12.
[43] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/849, 20. mai 2015, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist ning millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 648/2012 ja tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2005/60/EÜ ja komisjoni direktiiv 2006/70/EÜ. – ELT L 141, 05.06.2015, lk 73-117.
[44] FATF Recommendations, Interpretative note to recommendation 3; Glossary pp 119-120. – https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (07.01.2022).

Euroopa Parlamendi ja nõukogu rahapesu ja terrorismi tõkestamise viies direktiiv 2018/843[45] (AMLD V) võeti vastu 2018. aastal. Selles direktiivis on osutatud vajadusele ennetada virtuaalrahaga seotud riske, samuti antakse juhised finantstehinguteks kõrge riskiga kolmandate riikidega ning rõhutakse tegeliku kasusaajate registreerimise ja sellekohase rahvusvahelise infovahetuse vajadusele. Direktiivi kohaselt pidid liikmesriigid looma hiljemalt 2020. aastaks automatiseeritud kesksed mehhanismid, et võimaldada panga- ja maksekontode ning hoiulaegaste omanike tuvastamist. Viimati nimetatud nõude täitmiseks sätestab RahaPTS § 81 lg 1 krediidi- ja finantseerimisasutuste kohustuse tagada info kättesaadavus elektroonilise arestimissüsteemi kaudu kliendi maksekonto kohta, millele on väljastatud IBAN-kood või hoiulaeka üürinud kliendi kohta.

Käesoleva töö seisukohast VV puudutavad asjakohaseimad sätted on AMLD V artiklites 8-11, millest lähtudes on tehtud muudatused RahaPTS regulatsiooni. Kuna VV ja ametlike vääringute (st *fiat*-raha ehk riigi seaduslikuks maksevahendiks määratud müntide ja pangatähtede ning e-raha, mida tunnistatakse käibele lasknud riigis vahetusvahendina) vahetamise teenuse pakkujad, samuti rahakotiteenuse pakkujad ei olnud kohustatud kahtlast tegevust tuvastama, oli oluline laiendada direktiivi kohaldamisala selliselt, et see hõlmaks VV ja ametlike vääringute vahetamise teenuse pakkujaid ja rahakotiteenuse pakkujaid.

VV ja ametlike vääringute vahetamise teenuse pakkujate ning rahakotiteenuse pakkujate hõlmamine ei lahenda VV tehingutega seotud anonüümsuse probleemi lõplikult, kuna suur osa VV keskkonnast jääb endiselt anonüümseks, sest kasutajad saavad tehinguid teha ka ilma selliste pakkujateta. Anonüümsusega seotud riskidega võitlemiseks peaksid riiklikud rahapesu andmebürood olema suutelised hankima teavet, mis võimaldab seostada VV aadresse VV omaniku isikuga.[46]

Osutamaks VV kasutusvaldkondadele ja seadmaks raamistiku osalisriikides siseriiklikult kehtestatavatele õigusaktidele, lisati direktiivi (EL) 2015/849 artiklisse 3 punktid 18 ja 19, mille kohaselt on VV digitaalsel kujul esitatud väärtus, mida ei ole välja andnud ega taganud keskpank ega avaliku sektori asutus, mis ei pruugi olla seotud ametliku vääringuga ja millel ei ole vääringu või raha õiguslikku staatust, kuid mida füüsilised või juriidilised isikud aktsepteerivad vahetusvahendina ning mida on võimalik elektrooniliselt üle kanda ja säilitada ning millega on võimalik elektrooniliselt kaubelda. Tulenevalt laienenud regulatsioonist kohustatud isikute osas

[45] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2018/843, 30. mai 2018, millega muudetakse direktiivi (EL) 2015/849, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist, ning millega muudetakse direktiive 2009/138/EÜ ja 2013/36/EL. – ELT L 156, 19.06.2018, lk 43–74.
[46] Direktiiv (EL) 2018/843, lk 45, preambuli 10.

selgitatakse ka, et rahakotiteenuse pakkuja on isik, kes osutab oma klientide nimel krüptograafiliste privaatvõtmete kaitse teenuseid, et VV hoida, säilitada ja üle kanda. AMLD V eesmärk on hõlmata VV kõikvõimalikke kasutusviise, samas ei peaks käsitama VV kohalikke ehk täiendavaid vääringuid, mida kasutatakse väga piiratud võrgustikus ja mille kasutajaskond on väike.[47]

Kuna rahapesu ning sellega seotud terrorismi ja organiseeritud kuritegevuse rahastamine on jätkuvalt suureks probleemiks, mis kahjustavad finantssektori usaldusväärsust, stabiilsust ja mainet ning ohustavad Euroopa Liidu siseturgu ja sisejulgeolekut, võeti 2018. aastal vastu Euroopa Parlamendi ja nõukogu direktiiv 2018/1673[48], mille eesmärk on võidelda rahapesu vastu kriminaalõiguse abil, võimaldades pädevatel asutustel teha piiriülest koostööd tõhusamalt ja kiiremini. Direktiivis rõhutatakse, et rahapesu vastu võitlemisel tuleb arvestada, et VV kasutamisega kaasnevad uued riskid ja probleemid. Märkimisväärsete muudatustena ei sätestata põhimõtteid ega lisatingimusi, mis piiraksid laia rahapesukoosseisu kohaldamist ja ei sea rahapesu mõistet sõltuvusse sellest, kas rahapesuga ka reaalselt majanduskäibe usaldusväärsust kahjustati. Rahapesukuriteo koosseis ei sõltu pestud vara väärtusest ega näe ette erandeid väheoluliste ja väikesemahuliste tehingute suhtes.[49]

Direktiivis tähistatakse eelkuritegu terminiga „kuritegelik tegevus“, mis ei tähenda üksnes eelkuriteo täideviimist, vaid igasugust kuritegelikku osalemist süüteo toimepanemises. Eelkuriteo mõiste on seotud teo eeldatava raskusastmega (ingl *threshold approach*). Eelkuritegude regulatsiooniga läheb direktiiv kaugemale Varssavi konventsioonist ja FATF-i soovitustest, sest viimased ei kohusta riike tingimata kuriteo raskust karistusmäärade järgi hindama ning võimaldavad eelkuritegude nimekirja kindlaks määrata ka teistel viisidel.[50]

VV seonduvate ohtude osas korrigeeris FATF veel mitmel korral oma standardeid, kohustades riike hindama ja maandama vastavaid riske. Näiteks tuleb riikidel VV teenusepakkujaid litsentseerida või registreerida. Riigid peaksid tagama, et teenusepakkujad kasutavad kõiki võimalikke rahapesu ja terrorismi rahastamist ennetavaid meetmeid, nagu kliendi kohta käivad hoolsusmeetmed, klientide ning tehingute kohta andmete kogumine ja säilitamine, kahtlastest tehingutest teavitamine. Samuti tuleks teenusepakkujaid monitoorida ning vajadusel ka karistada,

[47] Direktiiv 2018/843, lk 54.
[48] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2018/1673, 23.oktoober.2018, rahapesu vastu võitlemise kohta kriminaalõiguse abil. – ELT L 284, 12.11.2018, lk 22-30.
[49] Kärner, M. Direktiiv (EL) 2018/1673 rahapesu vastu võitlemise kohta kriminaalõiguse abil. – Juridica 2019/7, lk 520 - https://www.juridica.ee/article_full.php?uri=2019_7_direktiiv_el_2018_1673_rahapesu_vastu_v_itlemise_kohta_kriminaal_iguse_abil&pdf=1
[50] *Ibid.*, lk 524.

kui teenusepakkujad lähevad vastuollu rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmetega. FATF-i soovitusi järgides peaks VV käsitlema kui vara, tulu või muud analoogset rahalist väärtuseühikut.[51] Rahapesu tõkestamine ei ole enam ammu rahapesu tõkestamine selle juriidilises tähenduses. Paradigma on selliselt muutunud, et isegi standardiseadja FATF ise peab rahapesu tõkestamise all silmas laiemat kuritegevuse vastu võitlemist. Meedias ja avalikus ruumis peetakse täna rahapesu tõkestamise all silmas juba võitlust igasuguse kahtlase tehingu ja tegevuse vastu.[52]

Regulatsioone VV ja laiemalt tehnoloogiliste uuenduste valdkonnas muudetakse kõrget riskitaset arvestades sageli, püüdes tuvastatud riske maandada eeldusel, et õiguslik raamistik, sealhulgas karistusmeetmed on ühetaoliselt rakendatavad. Euroopa tasandil peetakse silmas aga ka võimalusi kasutada arenguid järelevalvemenetluses ja kontrollimehhanismide väljatöötamisel. Näiteks Euroopa Pangandusjärelevalve[53] keskendub finantsinnovatsiooni jälgimisele, teadmiste jagamise ja tehnoloogilise neutraalsuse edendamisele regulatiivsetes ja järelevalvealastes lähenemisviisides ja otsib võimalusi finantssektoris regulatiivtehnoloogia (RegTech) kasutuselevõtuks.[54]

Järjest globaliseeruva majandus- ja finantstegevuse ning sellega paratamatult kaasneva rahvusvahelise organiseeritud kuritegevusega on muutunud üha keerukamaks ka meetodid, kuidas kuritegelikul teel teenitud raha seadustatakse. Seetõttu laiendatakse rahapesuvastaseid meetmeid üha enam erasektorile, kohustatud isikutele, et tuvastada erinevates majandusharudes ja valdkondades kasutatavaid rahapesu tüpoloogiaid, seda eriti läbi kübermaailma.

---

[51] Virtuaalvääringute teenusepakkujate uuring, RAB 2020, lk 17 - https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b) (15.01.2022).

[52] Mäeker, M., Nõmm, A. (2020). Pangasaladuse hoidjast politseinikuks: valikud rahapesu tõkestamisel. Juridica, 8, lk 664 - https://www.juridica.ee/article_full.php?uri=2020_8_pangasaladuse_hoidjast_politseinikuks_valikud_rahapesu_t_kestamisel&pdf=1 (02.02.2022).

[53] Euroopa Pangandusjärelevalve (EBA) on Euroopa Liidu sõltumatu asutus, mille ülesanne on tagada kogu Euroopa pangandussektoris tõhus ja ühtne usaldatavusnormatiivide kehtestamine ja nende täitmise järelevalve. Euroopa Pangandusjärelevalve üldeesmärgid on säilitada Euroopa Liidus finantsstabiilsus ja pangandussektori terviklikkus ning tagada nende tõhus ja korrapärane toimimine, vt - https://www.eba.europa.eu/languages/home_et (04.02.2022).

[54] EBA analysis of RegTech in the EU financial sector (2021) - https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1015484/EBA%20analysis%20of%20RegTech%20in%20the%20EU%20financial%20sector.pdf (04.02.2022). Vt mõistet ka Komisjoni teatis Euroopa Parlamendile, Nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide komiteele. Regulatiivtehnoloogia: finantstehnoloogia alaliik, mis keskendub tehnoloogiale, mis võib hõlbustada regulatiivsete nõuete täitmist tõhusamalt ja tulemuslikumalt kui seda võimaldab olemasolev suutlikkus. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2020:0591:FIN:ET:PDF (23.02.2022).

1.2 Rahapesuvastaste meetmete kujunemine Eestis

1.2.1 Rahapesu tõkestamise süsteem

Rahapesu tõkestamise mehhanism ja selleks kasutatavad meetodid koosnevad suures plaanis kahest sambast, milleks on preventsioon ehk ennetamine ning repressioon ehk keelatud tegevusele reageerimine. Ennetamise eesmärk on takistada kurjategijatel kuritegevuse tulemusel saadud raha kasutamist. Kui ennetusmeetmed ei ole tõhusaks osutunud, tuleb karistuslike vahenditega kurjategijaid vastutusele võtta, kui neil on õnnestunud kriminaaltulu majanduskäibesse siiski integreerida.

Ühelt poolt on rahapesu tõkestamine tegevus, mille eesmärgiks on rahapesu ära hoida ehk efektiivsete meetmete kaudu ennetada. Teisalt seisneb tõkestamine kuriteo kriminaliseerimises, mille alusel on kuriteo toimepanijat võimalik vastutusele võtta ning saadud vahendeid konfiskeerida. Preventiivsete meetmete kohaldamise roll avalik-õigusliku kohustusena on pandud erasektorile ning riigi roll on võtta kriminaalõiguslike meetmetega teo toimepanijaid koosseisu täitumisel vastutusele.[55]

Kuna traditsioonilise rahapesu puhul on ajalooliselt suur osa olnud finantsasutustel, on rahapesu tõkestamise meetmed töötatud välja pankades hoolsusmeetmete rakendamiseks. Sel viisil pannakse finantsasutustele vastutus oma teenuste osutamisel ka riigi majandussüsteemi toimimise ja finantsstabiilsuse tagamise eest. Rahapesu tõkestamisel on oluline takistada kriminaaltulu majanduskäibes kasutamist aga samal ajal ei tohiks rahapesu tõkestamise meetmed olla võimalikke riske arvestades liigselt ettevõtlust piiravad.

Rahapesu tõkestamise regulatsioonid püüavad selles vastandlikus olukorras leida tasakaalu avalik-õiguslike ning eraõiguslike huvide vahel. Ka eraõiguslikes sektorites lähtutakse riskipõhisest lähenemisest, hinnates kõige enam tähelepanu vajavaid rahapesu trende ja tegeledes nende riskide maandamisega.

Krediidi- ja finantseerimisasutuste puhul on rahapesu riskifaktor oluliselt kõrgem, kuna krediidi- ja finantseerimisasutustele on omased väga suured rahavood.[56]

Rahapesu ja terrorismi rahastamise õigusaktide normid on riskide vähendamise meetmed, olles sellisena riskide teadmise tulemuseks. Näiteks anonüümsust majanduskäibes on põhjendatult

[55] Mäeker, M., Nõmm, A. (2020), lk 664.

[56] Rahapesu andmebüroo. Aastaraamat. Tallinn 2006. Ülevaade rahapesu tõkestamisest Eestis 1999-2005, lk 12. (Eesti seaduste järgi on teatamiskohustus kahtlusepõhine, mis tähendab, et seaduse subjekt saadab teate RABile siis, kui tal tekib kahtlus, et tegemist on rahapesu või terrorismi rahastamisega. Rahapesu andmebüroo aastaraamatute kohaselt laekub igal aastal ligikaudu 75% kuni 95% kahtlaste tehingute teatistest krediidi- ja finantseerimisasutustelt).

peetud rahapesu, aga ka terrorismi rahastamist soosivaks. Seetõttu, vähendamaks anonüümsuse ärakasutamise võimalusi, seisnebki rahapesu ja terrorismi rahastamise tõkestamise üks alustalasid hoolsuskohustuses, mis rahapesu ja terrorismi rahastamise kontekstis hõlmab identifitseerimiskohustust, aga ka anonüümsust pakkuvate toodete ja varistruktuuride kasutamise piiranguid.[57]

Käsitledes eraldi krediidiasutusi, panku, siis need peavad tegutsema paradoksaalses ettevõtluskeskkonnas. Ühelt poolt sunnivad pidevalt muutuvad ja karmistuvad regulatsioonid finantsasutusi oma ärimudeleid muutma, et vähendada oma riske ja tegutseda ühiskonna kaitsjana. Teisest küljest peavad pangad turutingimustel tegutsedes suurendama kasumlikkust ja head klienditeenindust. Pangandussektor peab pidama sammu kiire tehnoloogilise arengu ja ühiskondlike muutustega. Pankade roll rahapesuvastases võitluses (AML) illustreerib seda paradoksi väga hästi.[58] RahaPTS § 20 lg 1 p 4 kohaselt peab kohustatud isik aru saama kliendi ärisuhtest ja koguma selle kohta täiendavat teavet. Muu hulgas tuleb kindlaks teha kliendi püsiv asukoht, tegevus- või elukoht, kutse- või tegevusala, olulisemad tehingupartnerid ning maksetavad. Nagu kõigi teiste hoolsusmeetmete puhul, lähtub kohustatud isik ärisuhte eesmärgi ja olemuse tuvastamisel riskipõhisest lähenemisest. Seejuures, mida suurem on kliendiga kaasnev risk, seda rohkem peab kohustatud isik meetmeid võtma, et kliendist ja tema riskiprofiilist aru saada.

Oma artiklis rahapesu kujunemisloost ja olemusest[59] on I. Tibar nimetanud neli rahapesule sageli iseloomulikku joont. Esiteks on rahapesu seotud sularahaga. Seetõttu on muudetud võimalikult keeruliseks sularaha finantsinstitutsioonidesse paigutamine. Samas tuleb märkida, et seotus sularaha hakkab kaduma, sest kuritegevus siirdub elektroonilisse vormi ja tähelepanu tuleb pöörata nendele uudsetele võimalustele. Rahapesu teine iseloomulik joon on rahvusvahelisus ja seda võib võrrelda legaalse majandustegevusega, milles äriettevõttele jääb ühe riigi turg kitsaks ja oma tegevust tuleb üle riigipiiride laiendada. Rahvusvahelistumise põhjuseks on spetsialiseerumine ja jälitamise keerukus. Mida rohkem riike raha läbib, seda keerukam ja aeganõudvam on kuritegude lahendamine ja väiksem oht saada karistatud. Kolmandaks rahapesu iseloomustavaks asjaoluks on seotud pangandus- ja finantssüsteemiga, kuna pangakontodel on

---

[57] Tibar, I. Tähelepanekuid uue rahapesu ja terrorismi rahastamise tõkestamise seaduse jõustumisega seoses. – Juridica 2018/1, lk 38 - https://www.juridica.ee/article_full.php?uri=2018_1_t_helepanekuid_uue_rahapesu_ja_terrorismi_rahastamise_t_kestamise_seaduse_j_ustumisega_seoses&pdf=1 (12.02.2021).

[58] Juntunen, J. and Teittinen, H. (2022), "Accountability in anti-money laundering – findings from the banking sector in Finland", Journal of Money Laundering Control, Vol. ahead-of-print No. ahead-of-print. - https://doi.org/10.1108/JMLC-12-2021-0140 (22.02.2022).

[59] Tibar, I. Rahapesu kujunemisloost ja olemusest. – Juridica 2007/7, lk 579-580. - https://www.juridica.ee/article_full.php?uri=2007_8_rahapesu_kujunemisloost_ja_olemusest&pdf=1 (07.11.2021).

lihtsam ja kiirem rahasid kasutada ning rahapesuoperatsioone sooritada. See on ka rahapesuvastase võitluse eesrinne. Neljandaks rahapesu tunnuseks on ohvri puudumine, kuid ulatuslik rahapesu mõjutab finants- ja rahandussüsteemi. Kaasajal on kerkinud tõsiselt päevakorda anonüümseid makseid võimaldavate rahasiirdamissüsteemide kasutuselevõtt.

Eelnev käsitlus on aastast 2007, kuid kõik need jooned on asjakohased ka tänasel päeval omas kontekstis nii seoses pangandussüsteemi, anonüümsete VV, organiseeritud kuritegevuse ja rahvusvahelisusega.

R. Durrieu kirjeldab rahapesu tõkestamise meetmete karistusliku lähenemise (*punitive-criminal approach*) kõrval rahapesu ja terrorismi rahastamise tõkestamisele rahvusvaheliselt loodud ja täiendatud nn ennetav-regulatiivset lähenemist või õigussüsteemi (*preventive/regulatory AML-CFT approach*). See süsteem koosneb põhiliselt haldus-, tsiviilõiguslikest ja pangandusseadustest ning regulatsioonidest. Mõnedes riikides sisaldavad ennetav-regulatiivsed AML-CFT süsteemid ka karistusõiguslikke sätteid ja karistusi. Rahvusvaheliste õigusaktidega loodud ennetav-regulatiivne rahapesu tõkestamise süsteem toetub viiele sambale, milleks on:

1) kohustatud isikud;

2) tunne-oma-klienti kohustused (*know your client* - KYC);

3) kahtlaste tehingute raportid (*suspicious activity report* -SAR);

4) rahapesu andmebürood (*Financial Intelligence Unit* - FIU) ja

5) varade käsutamise piiramise meetodid (arest/konfiskeerimine) ning kahtlaste isikute ja gruppide nimekiri.[60]

Ennetamise ja karistamise põhimõtted on sätestatud rahvusvahelistes normides, mis on üle võetud siseriiklikku regulatsiooni – seadustesse, määrustesse ja juhenditesse. Rahapesu tõkestamise mehhanismi toimimine sõltub regulatsioonide ühtsest toimimisest rahvusvahelisel tasemel, nende samasugusest tõlgendamisest ja nendes sätestatud nõuete järgimisest.

Autori hinnangul lisanduvad VV-ga toimepandava rahapesu puhul väljatöötatud tõkestussüsteemidele ja koostöövõrkudele spetsiifilised analüüsivahendid ning tehingutest tervikpildi saamiseks andmebaasidele ristkasutatavus ja juurdepääsude loomine.

---

[60] Durrieu, R. Rethinking Money Laundering & Financing of Terrorism in International Law: Towards a New Global Legal Order. Leiden, Boston, 2013. ProQuest Ebook Central, pp 155-167. - https://books.google.ee/books?id=4xVs_PGt3ocC&pg=PA2&lpg=PA2&dq=Rethinking+Money+Laundering+%26+Financing+of+Terrorism+in+International+Law:+Towards+a+New+Global+Legal+Order&source=bl&ots=2BNnzZVliu&sig=ACfU3U1sKsmv7O-3T3ypqfgI4Fq1TLFlGg&hl=et&sa=X&ved=2ahUKEwj50omoqKz3AhWDrosKHd0IBJE4ChDoAXoECBUQAw#v=onepage&q=Rethinking%20Money%20Laundering%20%26%20Financing%20of%20Terrorism%20in%20International%20Law%3A%20Towards%20a%20New%20Global%20Legal%20Order&f=false (22.01.2022).

1.2.2 Rahapesu tõkestusmeetmete kujunemine Eestis

Eesti seadusandja on kujundanud kehtiva õiguse FATF-i soovituste kohaselt, mis seavad nõude tugineda NarkPsAKonv-le[61] ning OrgKuriTKonv-le[62]. Lisaks on seadusandja tuginenud õigusliku alusena RahaPKonv-le, rahapesudirektiividele (AMLD IV ja V) ning direktiivile rahapesu vastu võitlemise kohta kriminaalõiguse abil. Samuti on ÜRO 2003. aasta korruptsioonivastases konventsioonis[63] seda valdkonda sisuliselt reguleerivad sätted.[64]

Rahapesu mõistet kasutati Eesti seadustes esmakordselt 1994. aastal krediidiasutuste seaduses (KAS)[65], mis sisaldas peatükki rahapesu tõkestamisest. Seaduse kohaselt pidid krediidiasutused hakkama tuvastama klientide isikusamasust, kes tegid tehinguid üle kindlaksmääratud piirsummade ning seda infot tuli säilitada. Kriminaalkoodeksis[66] kriminaliseeriti rahapesu ja rahapesu tõkestamise seaduse nõuete eiramine 1999. aastal. Seaduses kohustatud subjektidele, krediidi- ja finantseerimisasutustele ning teistele ettevõtjatele pandi kohustus tuvastada oma klientide isikusamasus ning rahapesukahtluse korral koostada rahapesu andmebüroole (RAB) tehingu kohta teade.

2004. aastast kehtib rahapesu ja terrorismi rahastamise tõkestamise seadus (RahaPTS), milles sätestati, et rahapesus kasutatud vara peab olema saadud kuriteo tulemusena. 2017. aastal jõustus RahaPTS-i redaktsioon, millega võeti üle AMLD IV direktiiv, viidi sisse mõningad muudatused seoses järgnenud AMLD V direktiiviga, rakendati rahvusvaheliste hindamiste käigus Eestile tehtud soovitusi ja laiendati seaduse kohaldamisala. RahaPTS selle redaktsiooniga võeti omaks FATF-i 2012. aasta soovituste kohane riskipõhine lähenemisviis Eesti õiguses.

Rahapesuriske hinnatakse kolme kihi vaates: Euroopa Liidus, liikmesriigi ja kohustatud subjekti tasandil. Riskide analüüsimise käigus tuleb määratleda ka riskiisu, mis on kohustatud isiku võime ja soov võtta oma majandustegevuses riske. Võetavate riskide kogum peaks olema kohustatud isiku poolt hallatav ja maandatav, seda ka RahaPTS-ist tulenevate kohustuste rakendamisel.[67]

---

[61] Narkootiliste ja psühhotroopsete ainete ebaseadusliku ringluse vastane Ühinenud Rahvaste Organisatsiooni Konventsioon, viide 22.
[62] Rahvusvahelise organiseeritud kuritegevuse vastu võitlemise Ühinenud Rahvaste Organisatsiooni Konventsioon, viide 31.
[63] Ühinenud Rahvaste Organisatsiooni korruptsioonivastane konventsioon. – RT II 2010, 4, 10.
[64] Tibar I. KarS § 394/1.5 – Karistusseadustik. Komm vlj. 5. vlj. Tallinn: Juura 2021. - https://karistusseadustik.juuraveeb.ee/ (07.02.2022).
[65] Krediidiasutuste seadus - RT I, 07.12.2021, 13.
[66] Kriminaalkoodeks - RT 1992, 20, 288.
[67] Rahandusministeerium, 2018, lk 35. Rahapesu ja terrorismi rahastamise tõkestamise valitsuskomisjoni analüüs ja ettepanekud. -

Alates 2021. aastast kujundati Rahapesu Andmebüroo Rahandusministeeriumi valitsemisala iseseisvaks valitsusasutuseks. RAB on keskne riigisisene üksus, mis vastutab võimaliku rahapesu või terrorismi rahastamisega seonduva teabe vastuvõtmise, analüüsi ja selle edastamise eest uurimisorganitele, teostab järelevalvet kohustatud subjektide tegevuse üle. RABi igapäevapraktika jaoks on väga olulisel kohal Egmont Group'i[68] väljatöötatud teabevahetamise põhimõtted ning teabekanalite Egmont Secure Web-i ja FIU.NET-i kasutamine.

Eelkuriteo sisustamisel võeti Eesti õigusesse üle (RahaPTS § 4 lg 5) Varssavi konventsiooni, direktiivi 2018/1673 ja FATF-i standardite tõlgendussäte, et rahapesuga on tegemist ka siis, kui kuritegeliku tegevuse üksikasjad, mille tulemusel saadi rahapesus kasutatav vara, ei ole kindlaks tehtud. See tähendab, et rahapesus süüdimõistmist ei välista asjaolu, et rahapesu objektiks oleva vara allikaks olnud konkreetse eelkuriteo asjaolud ei ole lõpuni välja selgitatud.

Eelkuriteo ja rahapesu kuriteo seose osas on Riigikohus leidnud, et rahapesuasja menetluses ei pea kohus eelkuriteosündmuse fakti tuvastamisel lahendama eelkuriteo toimepanijate süüküsimust. Rahapesu süüdistuses ei tehta automaatselt isikule karistusõiguslikku etteheidet eelkuriteo toimepanemises, kuid see ei välista eelkuriteo toimepanija vastutust rahapesu eest.[69]

Jätkuvalt tuvastati aga kõrget rahapesuriski eelkõige VV teenusepakkujate sektoris ja vajadusest kiiresti reageerida muutuvale olukorrale, sealhulgas VV valdkonnas, jõustus näiteks 2020. aastal Eestis viis RahaPTSi redaktsiooni, millega võeti üle AMLD V nõuded, laiendati ja täpsustati kohustatud isikute ringi, koondati VV teenuse pakkujad ühendmõiste alla (RahaPTS § 10) ja muudeti rahapesu mõistet (RahaPTS § 4).

1.3 Virtuaalvääringute olemus ja nende regulatsioon Eestis

VV on RahaPTS § 3 p 9 definitsiooni kohaselt digitaalsel kujul esitatud väärtus, mis on digitaalselt ülekantav, säilitatav või kaubeldav ja mida füüsilised või juriidilised isikud aktsepteerivad maksevahendina, kuid mis ei ole ühegi riigi seaduslik maksevahend ega rahaline vahend ega makseinstrument või maksetehing. Ühisrahastuse ja muude investeerimisinstrumentide

https://www.rahandusministeerium.ee/sites/default/files/rahapesu_tokestamise_valitsuskomisjoni_analuus_ja_ettepanekud.pdf (06.02.2022).

[68] Vt Finantsinspektsioon. Rahapesu tõkestamise valdkonnas on rahapesu andmebüroodel üleilmne koostöövõrgustik, mida kutsutakse Egmont Group. See ühendab 159 rahapesu andmebürood ja grupi liikmeks on ka Eesti rahapesu andmebüroo. Antud töövormi kaudu vahetavad andmebürood rahapesu tõkestamiseks vajalikku teavet. Finantsjärelevalveasutused Egmont Groupi ei kuulu. https://fi.ee/et/uudised/finantsinspektsiooni-praktika-rahvusvahelise-rahapesu-asjades (19.04.2022).

[69] RKKKm 1-17-5176, p 21.

ning virtuaalvääringute seaduse (ÜMIVS) eelnõus[70] on VV sätestatud samamoodi kui RahaPTS-s. Maksevahendina kasutamine või VV maksevahendina tunnustamine ei pea olema VV loomise või (esma)pakkumise ajal kindlaks määratud, vaid VV võib ajapikku areneda maksevahendiks, mida tunnustavad füüsilised ja juriidilised isikud.

Järgnevalt VV ja krüptovarade mõisteid, toimimisviise ja kasutusvaldkondi avades toetub autor ÜVIMS-s, Eesti 2020. aasta rahapesu ja terrorismi rahastamise siseriiklikus riskihinnangus[71], Rahapesu ja terrorismi rahastamise tõkestamise seaduse ja teiste seaduste muutmise seaduse eelnõu 507 SE[72] seletuskirjas ja Rahapesu andmebüroo 2022. aasta jaanuaris välja antud uuringus Virtuaalvääringu teenuse pakkujatega seonduvad riskid Eestis[73] kasutatavatele tähendustele ja selgitustele.

Laiemas tähenduses kasutatakse sageli mõistet krüptovarad, kuid krüptovarade alla võib tinglikult liigitada kõiki instrumente, mis on esitatud krüptograafilisel kujul. Krüptovarasid on nende peamisest funktsioonist ja kasutusotstarbest lähtuvalt võimalik jagada kolmeks. Nendeks on makse*token*id ehk VV, investeerimislaadsed *token*id ja kasutus*token*id. VV-d on eeskätt maksete tegemiseks või väärtuse ülekandmiseks kasutatavad krüptovarad, millega tavaliselt ei kaasne õigusi *token*i väljastaja enda või tema poolt pakutava toote või teenuse suhtes (erinevalt investeerimis- või kasutus*token*'itest). Teisisõnu kasutatakse VV pigem vahetusvääringuna või investeerimise eesmärgil läbi *token*i enda väärtuse, nt on selline vääring *bitcoin*. Uuem makseviis on „varaga tagatud *token*", mis on tagatud teatud varaga (riiklik valuuta, kaup või toore, teine krüptovara).[74] Enamik VV-sid kasutab plokiahela tehnoloogiat. VV alustalaks olev plokiahel kujutab endast jagatud digitaalset andmebaasi, mis salvestab tehinguid ning mida ei ole võimalik muuta, tehes andmed võltsimiskindlaks ja püsivaks. Tehingute detailid on avalikud ja lõpuni jälgitavad. Plokiahela puhul on tegemist koodiga ning avaliku registriga, millesse kantakse muutmata kujul tehtud tehingud, mis kokku moodustavad plokid ehk koodi osad ja need seotakse omavahel krüpteerimisfunktsiooniga.

---

[70] Ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu - https://eelnoud.valitsus.ee/main/mount/docList/a41d0022-7752-4009-9a08-1b97fc44be64#JqPC82Xu, (22.02.2022).
[71] Rahandusministeerium. NRA 2020.
[72] Rahapesu ja terrorismi rahastamise tõkestamise seaduse ja teiste seaduste muutmise seaduse eelnõu 507 SE - https://www.riigikogu.ee/tegevus/eelnoud/eelnou/ffe848a6-7b78-43cf-b106-720915882205/Rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20seaduse%20ja%20teiste%20seaduste%20muutmise%20seaduse%20eeln%C3%B5u%20(507%20SE%20I) (22.02.2022).
[73] Rahapesu andmebüroo. 2022 - https://www.fiu.ee/aastaraamatud-ja-uuringud/uuringud (08.02.2022).
[74] Seletuskiri ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu juurde, lk 11. - https://eelnoud.valitsus.ee/main/mount/docList/a41d0022-7752-4009-9a08-1b97fc44be64#4NwfcK7w (08.02.2022).

VV-ga seoses on kasutusele võetud ka koondnimetusi vastavalt kasutusvaldkonnale, nagu näiteks „plokiahela tehnoloogial põhinevad instrumendid“ (PTP-instrumendid), mis omavad tavaliselt füüsilise substantsita mitterahalist vormi, kujutades teatud väärtuse digitaalset esitust.[75]

VV ostmise, vahetamise ja müümise vahendiks on nn rahakott (ingl *wallet*), mis võib olla rakendus, programm arvutis või VASP-i hallatav rahakott, mis hoiab endas kahte võtit – avalikku ja privaatset ja mida on vaja VV turvaliseks hoiustamiseks ja tehinguteabe kaitsmiseks ning kinnitamiseks. VV-l ei ole füüsilist vastet: nad eksisteerivad ainult digitaalsete kannetena ühises raamatus. VV omandi üleandmine vajab kinnitamist krüptograafiliselt allkirjastatud sõnumiga. Privaatvõtme abil antav allkiri annab kasutaja nõusoleku hajusraamatu süsteemile küsida digitaalse raamatu väljavõte, mis kinnitab omandi muutumist. Kehtiv allkiri kinnitab hajusraamatu süsteemis, et tehingu algatajal on volitus teha vastav raamatu kanne ja VV seostakse kasutaja avaliku võtmega. Sellises kontekstis on privaatvõtit võimalik võrrelda parooliga, mis avab kasutajakonto ja seostatav avalik võti kujutab endast kasutaja pangakonto numbrit.[76] Uusi krüptoühikuid luuakse protsessis, mida nimetatakse "kaevandamiseks" (ingl *mining*). Selles protsessis kasutatakse arvutiressurssi keeruliste matemaatiliste võrrandite lahendamiseks ehk teiste osapoolte tehingute kinnitamiseks enne andmeblokkidesse lisamist. See protsess nõuab palju energiat ja arvutustehnikat. Tasuks ressursi kulutamise eest jaotatakse uusi VV-sid. Eristatakse tsentraliseerituid ja detsentraliseerituid VV-sid. Tsentraliseeritud VV-l on keskne administraator, kes VV väljastab, nende kasutamist haldab ja käibest kõrvaldab. Sageli leiab neid veebikeskkondadest, mis pakuvad alternatiivseid maksevõrgustikke või *online*-mänge. Detsentraliseeritud VV-l, nt *bitcoin*, selline keskne administraator puudub. Kitsamalt saab VV all eristada krüptograafilistel alustel üles ehitatud rahasüsteemi, mis on tavaliselt detsentraliseeritud ja isereguleeruv.

Krüptorahade kategooriasse kuulub enamik tuntumaid VV nagu *bitcoin* ja *ethereum*. VV alla liigituvad ka nn stabiilsed mündid (*stablecoins*), mille hind seotakse mingi konkreetse vara väärtusega, tavaliselt USA dollariga (nt *Tether, USD Coin, Paxos*). Need nn globaalsed stabiilsusrahad (GSCs) võivad tugevate AML/CTF meetmeteta muutuda järgmiseks suureks ohuks

[75] Raamatupidamise Toimkond võttis krüptoraha ühise nimetusena kasutusele neutraalse termini PTP - https://www.rmp.ee/raamatupidamine/raamatupidamine-yldiselt/plokiahela-tehnoloogial-pohinevate-instrumentide-kajastamine-2018-09-11 (22.02.2022).

[76] Rahandusministeerium. Krüptovarade reguleerimise väljatöötamiskavatus (sic!). *Sine loco*, november 2019. – https://www.rahandusministeerium.ee/sites/default/files/news-relatedfiles/kruptovarade_reguleerimise_vtk.pdf. (12.10.2021). Väljatöötamiskavatsus on osa Vabariigi Valitsuse 2019- 2023.a tegevusprogrammist, millega anti Rahandusministeeriumile ülesandeks analüüsida krüptovarade reguleerimise vajadust. *Sine loco*, kinnitatud 30. mail 2019, lk 33. – https://www.valitsus.ee/valitsuse-eesmargid-ja-tegevused/valitsemise-alused/tegevusprogramm (12.10.2021).

finantssüsteemi terviklikkusele.[77] Eesti on üks esimesi riike maailmas, kus asuti reguleerima VASP-ide tegevust. Regulatsioonides on aja jooksul toimunud olulisi muudatusi. VASP-idega seonduvalt nähti kõrgendatud rahapesu riski Eestis juba 2006. aastal, kui leiti, et infotehnoloogilised arengud võimaldavad uusi, regulatsioonidele mittealluvaid praktikaid rahapesuks. Seetõttu allutati n-ö mittetraditsiooniliste maksevahendite pakkujad 2008. aastal jõustunud RahaPTS-is alternatiivsete maksevahendite teenuse pakkuja mõiste all RahaPTS regulatsioonile, mis kohustas alternatiivsete makselahenduste pakkujaid end majandustegevuse registris registreerima. 2010. aastal jõustus makseasutuste ja e-raha asutuste seadus (MERAS)[78], mis sätestas e-raha asutusena aktsiaseltsid, mille peamine ja püsiv teenus on enda nimel e-raha väljastamine.

Euroopa tasemel rõhutati AMLD V-s, et VV ei tohiks ajada segamini e-raha ega rahaliste vahendite laiema mõistega ega liikmesriikide lokaalsetele makseinstrumentidega, samuti mitte mänguvääringuga, mida saab kasutada ainult konkreetses mängukeskkonnas.[79]
2014. aastal jõustus majandustegevuse seadustiku üldosa seaduse ning korrakaitseseaduse muutmise ja rakendamise seaduse muutmise seadus[80], mille §-s 52 sätestati loakohustus alternatiivsete maksevahendite teenuse osutamisele ja tegevusloa andmise otsustas rahapesu andmebüroo.
2016. aastal tegi Riigikohus otsuse kohtuasjas nr 3-3-1-75-15[81] (de Voogd), mis kujunes üheks ajendiks õigusliku regulatsiooni loomisele. Kohus leidis, et alternatiivsete maksevahendite teenuse pakkuja mõiste võib hõlmata virtuaalvaluuta vahetusteenuse pakkujaid ning seadus vajab alternatiivsete maksevahendite teenuse osutamise valdkonnas selgemat lahendust. Kohtu seisukoht oli, et krüptorahaga, sh *bitcoin*'idega majandustegevusena kauplemine vastab alternatiivsete maksevahendite teenuse pakkumise mõistele ning on sellisena allutatud rahapesuvastasele regulatsioonile ning riiklikule järelevalvele.

[77] IMF Notes 2021/002. Schwarz, N., Chen. K., Poh. K., Jackson, G., Kao. K., Fernando. F., Markevych, M. Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1) Some Legal and Practical Considerations - https://www.imf.org/en/Publications/fintech-notes/Issues/2021/10/14/Virtual-Assets-and-Anti-Money-Laundering-and-Combating-the-Financing-of-Terrorism-1-463654 (21.02.2022).
[78] Makseasutuste ja e-raha asutuste seadus - RT I, 10.07.2020, 21.
[79] Direktiiv (EL) 2018/843, lk 4.
[80] Majandustegevuse seadustiku üldosa seaduse ning korrakaitseseaduse muutmise ja rakendamise seaduse muutmise seadus - RT I, 29.06.2014, 1.
[81] RKHKo 3-3-1-75-15.

1.4 Virtuaalvääringute kasutamine rahapesu protsessis

Rahapesu objektiks on kuritegelikul teel saadud vara ehk kriminaaltulu, mis suunatakse legaalsesse majandus- ja finantskäibesse. Rahapesu kuritegu ei saa toimuda ilma eelkuriteota, mille tulemusel teenitakse kriminaaltulu. Aastakümneid tagasi olid rahapesu eelkuritegudeks eelkõige narkootikumidega seotud kuriteod, millel on kuriteo iseloomu tõttu tihe seos organiseeritud kuritegevusega. Eelkuritegudena on lisandunud järjest suuremat kahju tekitavad ja raskesti tõendatavad küberkuriteod. Autor märkis sissejuhatuses, et nn klassikaline rahapesu koosneb kolmest peamisest etapist ja kirjeldab seda protsessi täpsemalt ning võrdleb seda VV abil teostatava rahapesu mudeliga. Olulised erinevused nendes tegevustes tulenevad eelkõige infotehnoloogilistest eripäradest, mille abil VV tehinguid teostada saab.

Rahapesu protsessi on võimalik jagada järgmisteks etappideks:
1) kriminaaltulu muundamine ja paigutamine (ingl *placement*)
2) kriminaaltulu päritolu varjamine, laotamine, kihitamine (ingl *layering*) ning
3) kriminaaltulu lõimimine, integreerimine, omandamine (ingl *integration*).[82]
RahaPTS § 4 lg 1 kohaselt on rahapesu kuritegelikust tegevusest saadud vara või selle asemel saadud vara: 1) muundamine või üleandmine eesmärgiga varjata vara ebaseaduslikku päritolu või abistada kuritegelikus tegevuses osalenud isikut, et ta saaks hoiduda oma tegude õiguslikest tagajärgedest (nn moondamistegevused); 2) omandamine, valdamine või kasutamine, kui selle saamisel on teada, et see on saadud kuritegelikust tegevusest või selles osalemisest (nn kolmanda isiku teod) ja 3) tõelise olemuse, päritolu, asukoha, käsutamisviisi, ümberpaigutamise või omandiõiguse varjamine või varaga seotud muude õiguste varjamine (nn varjamistegevused).[83]

Paigutamine on nn klassikalise rahapesu esimene etapp ning selles staadiumis suunatakse kuritegelikust tegevusest saadud tulu finantssüsteemi. Kogu rahapesu protsessis on selles etapis rahapesijatel vahelejäämise oht kõige suurem, sest selles staadiumis peavad kohustatud isikud (nt finantsasutused) järgima hoolsusmeetmeid ja süsteemi kantava vara päritolu tuvastama. Seetõttu püüavad kurjategijad näiteks kanda raha pangakontodele alla finantsasutusele kohustusliku tuvastamis- ja järelevalveasutustele teavitamispiiri. Ebaseadusliku vara ülekandmise etapis

[82] Stessens, G. Money laundering: a new international law enforcement model. Cambridge: University Press 2000, pp 114–115 - https://ebookcentral-proquest-com.ezproxy.utlib.ut.ee/lib/tartu-ebooks/detail.action?docID=144722 (12.03.2022).
[83] Tibar I. KarS § 394/2.4 – Karistusseadustik. Komm vlj. 5 vlj. Tallinn: Juura 2021. - https://juuraveeb.ee/kommenteeritudvaljaanded (02.02.2022).

finantssüsteemi saavad uurimisasutused esitada kahtlustuse rahapesu toimepanemises. Paraku muudab varjamismeetodite kasutamine ülekantava vara kuritegeliku päritolu tõendamise väga keeruliseks. Paigutamise etapis kasutatakse erinevaid meetodeid vara pangandussüsteemi suunamiseks, näiteks variisikute ja -ettevõtete (ka *offshore*-äride ehk erandliku maksusüsteemiga piirkondade ettevõtete) kasutamine jm. Siin saab võrdluse tuua tehingutes VV-ga, milles *fiat*-raha saab anonüümselt vahetada VV-ks virtuaalvara teenuse pakkuja (*virtual asset provider* ehk VASP) juures, mis ei järgi piisava hoolsusega rahapesuvastaseid nõudeid. Kuna erinevatel VV kauplemisplatvormidel on finantstehingute kontrollimiseks erinevad, st leebemad või ebapiisavad nõuded[84], on võimalik VV-sid omavahel vahetada ja viimaks näiteks *fiat*-rahas välja võtta või teostada VV makseid. Paigutamise faasis võidakse mistahes kuritegelikul teel (küberkuritegevusega, pettuse või kelmuse teel) saadud *fiat*-raha kanda vahenduseta otse VV-sse.

Rahapesu protsessi järgmise etapi, kihitamise, eesmärk on muuta vara päritolu tuvastamine keerulisemaks, sooritades näilikke ja fiktiivseid tehinguid kaupade ja teenustega, laenudega. Paigutatud kriminaalset päritolu raha muudetakse nii, et järelevalve- ja õiguskaitseasutustel oleks keerulisem rahapesu tunnuseid tuvastada. See etapp võib sisaldada rahvusvahelisi pangaülekandeid erinevate isikute erinevate kontode vahel, varem käesolevas töös nimetatud *smurfing´*ut, mis on sisuliselt suuremate rahasummade väiksemate summadega tehinguteks jagamine. Kontodele kantud raha võidakse sularahana välja võtta ja taas teistes valuutades sisse maksta. VV rahapesu vaates on kõige olulisem säilitada anonüümsus, kuna alati jääb võimalus, et läbi plokiahela suudetakse digitaalset jälge vara omanikuga seostada. Selles etapis on kurjategijate seas levinud tumeveebi (*darkweb*) kasutamine, et kaotada jäljed vara omaniku ja ülekannete vahel. Põhilisteks vahenditeks VV ebaseadusliku päritolu varjamine rahapesus kasutamiseks on segamis- või trummelteenus (*mixing* või *tumbling service*) ja VASP-ide kasutamine. Kuna VV-d põhinevad plokiahelal, avalikul hajusraamatul, on kõik nende ülekanded avalikult jälgitavad. Kurjategijad saavad aga tegutseda teatud anonüümsuse tasemel (teostada tehinguid pseudonüümselt), kuna vääringute aadresse ei registreerita isikute nimele, vaid neile on juurdepääs rahakoti paroole teadval isikul. Seega on ülekannete taga ebaseaduslikku tegevust kahtlustades väga raske tuvastada konkreetset isikut.

[84] 2020 Geographic Risk Report: VASP KYC by Jurisdiction - https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/ (16.04.2022). CipherTrace´i uuringu kohaselt oli 2020. a 56%-l maailma VASP-idest nõrk tunne-oma-klienti protsess, mis tähendab, et rahapesijad said nende kaudu minimaalsete kontrollimeetmete tõttu ebaseaduslikku tuluga tehinguid teha. Samuti on nende VASP-ide puhul oht, et tehinguid tehakse alla kehtestatud piiramäärade, kasutatakse kihitamist.

Tavapärases VV, nt *bitcoin*i ülekandes, mis kehtib ka rahapesu tegevuste korral, osaleb viis osapoolt: 1) *bitcoin*i saatja, kes alustab tehingu veebis, rahapesu puhul „musta rahaga“, 2) *bitcoin*i vastuvõtja, antud juhul rahapesija, kes aitab saatjal „musta raha“ päritolu ähmastada, 3) *bitcoin*i kaevandajad, kes tõestavad ülekannet ja töötlevad andmeplokke, mõnikord teenustasu eest, 4) *bitcoin*i arendusmeeskond, kes uuendab vajadusel *bitcoin*i koodistikku, 5) *bitcoin*i vahetusteenuse pakkujad, mis vahendavad *bitcoin*ide vahetamist teistesse valuutadesse ja vastupidi.[85] Lahendusi rahapesuvastaste meetmete rakendamiseks VV reguleerimisel tuleb otsida nende osapoole seast, kellelt tuleks andmeid koguda ja kellele tuleks teisalt pakkuda vahendeid kahtlaste tehingute tuvastamiseks.

Järgnevad ülevaated *bitcoin*i segamisteenuste toimimise kohta pärinevad 2018. aasta uuringust ja läbiviidud eksperimendist segamisteenuse pakkujate seas, mille eesmärgiks seati segamisteenuse kättesaadavuse ja usaldusväärsuse ning seeläbi sellise teenuse võimaliku rahapesuriski hindamine.

Kui *bitcoin*i *f*iat-rahaks tegemise ülekanne aitab kurjategija tuvastada, võib selle omakorda seostada ebaseadusliku tegevusega. Segamisteenus aitab kurjategijatel kuritegeliku tulu päritolu varjata, võimaldades raha vabalt välja võtta. *Bitcoin*i segamisteenus pakub tavaliselt kliendile sissemakseks äsja loodud *bitcoin*i aadressi. *Bitcoin*i segamisteenus maksab pärast segamistasu mahaarvamist teised *bitcoin*id oma varudest kliendi pakutud *bitcoin*i aadressidele. Maksete/tasude sagedust ja koguseid muudetakse, et tekitada mulje legitiimsusest. Plokiahel võimaldab küberkurjategijatel segamisprotsessi järel tuvastada sissekantud ja saadud *bitcoin*ide seose protsenti, mida nimetatakse „määrdumiseks“. Kui *bitcoin*ide segamine on korralikult teostatud, siis seos puudub („määrdumine“ on null protsenti). Mõned *bitcoin*i segamisteenused suudavad tagada, et naasvad kliendid (st sagedased rahapesijad), kes on saanud varem määrdunud *bitcoin*i, ei saa tulevastes ülekannetes sama *bitcoin*i. Uuringus tehti eksperiment, milles katsetati erinevate *bitcoin*i segajate ja VASP-ide platvorme, et saada selgust, kuidas vastavad teenused toimivad. Tulemuseks oli, segamisteenused tumeveebis osutusid osaliselt pettusteks ja osaliselt toimivateks, nimelt viiest kolm teenuspakkujat osutusid pettuseks (*bitcoin*e küll võeti vastu, aga vastu ei antud midagi), kaks teenust toimisid. Üks vahetusteenus seostas väärингud otse pangakontoga, mis sellisel viisil paljastaks kurjategijad õiguskaitseasutustele. Anonüümsuse suurendamiseks eelistavad kurjategijad kasutada väljundplatvorme nagu PayPal, mis

[85] Bryans, D. (2014). Bitcoin and Money Laundering: Mining for an Effective Solution. Indiana Law Journal. Vol. 89:441 p 447. - https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=11100&context=ilj (15.01.2022).

võimaldab neil saada raha minimaalsete registreerimisnõuetega. Uuring tuvastas, et segamis- ja VASP-ide kaudu teostatava rahapesu tasu on alla 15% kriminaaltulust, teiste rahapesumeetodite tasud võivad ulatuda kuni 50%-ni.[86]

Mõnedel andmetel maksab VV segamisteenus 0,29 kuni 3% segatavast summast. Segamisteenus iseenesest ei ole ebaseaduslik ja VV mineviku kustutamine ja turvalisuse suurendamine ei ole keelatud, kui VV ei ole saadud kuritegelikul teel. Seda teenust kasutatakse aga kuritegelikel eesmärkidel ja see on sageli viisiks krüptoraha tehingutelt makstavate maksude vältimiseks.[87]

Plokiahela tehnoloogiat on edasi arendatud ja see pakub nüüd mõnede VV puhul veelgi suuremat anonüümsust, näiteks ei ole nende avalik register tegelikult avalik. Anonüümsuse seisukohast on *fiat*-raha ja VV sarnase riskiga aga VV kuritegeliku kasutamise ohtu süvendab tehingute tehnoloogiline kiirus ja mobiilsus.

See kehtib näiteks selliste valuutade osas nagu *bytecoin* või selle järglane Monero, mis põhinevad CryptoNote'i tehnoloogial. See on krüptograafiline protsess, mis põhineb nn "*ring signature*"-tehnoloogial ja erineb *bitcoin*i ja *ethereum*i omast. See tehnoloogia võimaldab kasutajaid grupeerida. Kui üks kasutaja teeb ülekande, on võimatu teada, milline grupi liige seda tegi. Lisaks saab CryptoNote'i algoritmiga tehingute ajalugu täielikult peita, erinevalt *bitcoin*i plokiahelast, kus iga kasutaja saab vaadata kogu tehingute ahelat. CryptoNote võimaldab jagada tehingus kolmandate osapoolte kontode kaudu ülekantud summad, mille tulemusena muutub tegelik kogusumma tehingute jadas jälitamatuks. Erinevalt *fiat*-rahast saab krüptovaluuta summasid mõne sekundi jooksul ühelt elektrooniliselt kontolt teisele kanda, teadmata, kes tehinguid teostab. Seega saab summad teha peaaegu kohe kättesaadavaks anonüümsetele kasutajatele kõikjal maailmas. Lisaks saab virtuaalrahakoti omanik privaatvõtme vabatahtlikult edasi anda, andes seeläbi kolmandale osapoolele täiesti anonüümse juurdepääsu oma elektroonilisele rahakotile. Ka seda võib võrrelda sularaha käest kätte andmisega, kuid kuna VV-sid saab interneti kaudu anonüümselt edasi anda, siis sellega seotud risk suureneb.[88]

Rahapesu integreerimise etapis suunatakse vara legaalsesse majanduskäibesse, investeerides kinnisvarasse, aktsiatesse ja muudesse varaklassidesse. VV puhul võib kuritegelik grupp luua

[86] Wegberg, R., Oerlemans, J.-J., Deventer, O. (2018). Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. Journal of Financial Crime - https://www.emerald.com/insight/content/doi/10.1108/JFC-11-2016-0067/full/html (22.02.2022).
[87] Freeman Law. - https://freemanlaw.com/what-is-a-tumbler-and-is-cryptocurrency-tumbling-safe/ (27.02.2022).
[88] Swiss National Risk Assessment (NRA): Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding pp 19-20, - https://www.sif.admin.ch (23.02.2022).

näiteks äriühingu, mis võtab vastu *bitcoin*i makseid, et muuta ebaseaduslik virtuaalvara seaduslikuks. Samuti tehakse VV makseid tumeveebis ebaseaduslike kaupade eest tasumiseks kas kurjategijate endi või teiste tumeveebi kasutajate vahel. Samuti kasutatakse võimalust osta VV kaevandamise seadmeid, et luua omakorda uusi VV-sid, võimendada ebaseaduslikku tulu ja osta nende eest *fiat*-raha.

Autori seisukoht on, et segamisteenuse ja muid hägustamisviise läbinud aadressid ehk VV-d tuleb plokiahela analüüsivahenditega tuvastada ja VASP-id peavad nendega tehingute tegemisest keelduma. Lisaks tuleb vastavalt riskihinnangutele ja aadresside tuvastatud seostele kriminaalsete võrkudega täita automaatselt teavitamiskohustust, et reaalajas oleks võimalik tõkestada järgnevad tehingud kahtlaste VV-ga. Kuna VV tehingud on teiste teenuse kasutajate suhtes nagunii anonüümsed, siis viitab segamisteenuste kasutamine otseselt soovile vältida tuvastamist, mida võib selgitada vaid ebaseadusliku tegevusega (küberkuritegevuse, pettuste kõrval näiteks ka VV tehingutelt maksude tasumise vältimine).[89]

2. Virtuaalvääringutega seotud rahapesuriskid

2.1 Virtuaalvääringu teenuse pakkujate ja virtuaalvääringute käibega seotud riskid

Järgnevalt käsitleb autor rahapesuriskide kontekstis eraldi VASP-idega ja tõusetunud probleeme ja nende lahendamiseks kasutusele võetud meetmeid.

Rahapesuvastase võitluse meetmed on muutunud märkimisväärselt seoses finantssektoris toimunud tehnoloogiliste arengutega, eriti seoses VV-dega, mille kasutamist ja rahandussüsteemi lülitamist tuleb ajakohaselt ja kiiresti reguleerida. Erinevate riikide riskihinnangutes on kasvava rahapesu ohu tõttu seoses VV kasutamisega tõstetud ka riskitasemeid ja võetud kasutusele tõkestusmeetmed. Eestis reguleeriti esmakordselt tegevusloa taotlemise kohustus VV raha vastu vahetamise teenuse pakkumisel ning VV rahakotiteenuse pakkumisel 2017. aastal vastu võetud RahaPTS §-s 70. VV teenuse pakkujad on RahaPTS mõistes kohustatud subjektid, st nad peavad järgima RahaPTSi nõudeid, taotlema VV teenuse pakkumiseks RABilt tegevusluba ning nende tegevus on allutatud RABi järelevalvele. RABile saabunud info kohaselt on VV teenuseid üritatud Eestis korduvalt pakkuda ka ilma tegevusloata, seda teavet on kinnitanud RABi

[89] Virtuaalvääringuid käsitletakse tulumaksuseaduse § 15 lõike 1 kohaselt varana ning nendest saadud tulu maksustatakse, vt Tulumaksuseadus - RT I, 05.04.2022, 5.

läbi viidud väärteomenetlused. RAB on oma 2017. ja 2018. aasta aastaraamatutes[90] märkinud, et varem väljastatud tegevuslubasid võidi kasutada petlikult ettevõtte usaldusväärsuse suurendamiseks teises jurisdiktsioonis finantsteenuste pakkumiseks.

Tagantjärgi tuleb tõdeda, et VASP-idele väljastati tegevuslube ebapiisavate nõuete alusel, mille tõttu ei hakanud ettevõtted Eestis tegutsema, nende juhtimine toimus mujal ja siin puudusid ka kliendid. RAB juhtis seonduvatele riskidele tähelepanu ning seoses olukorraga rõhutati pettuste ja vara omastamise riski, rahapesu ja terrorismi rahastamise riski ning hoolsusmeetmete mittepiisava kohaldamise riski. Samuti toodi välja, et RABi pädevus pole piisav nende riskide maandamiseks. 2020. aastal jõustunud RahaPTS muudatusega kehtestati mitmed täiendavad nõuded, näiteks peavad VV ettevõtte registrijärgne asukoht, tegelik äritegevus ja juhatuse asukoht asuma Eestis. Tõsteti oluliselt riigilõivu ning regulatsiooni laiendati krüptoraha vahetamisele teise krüptoraha vastu.

Eesti NRA tulemusel selgus, et VASP-idega seonduvalt on vaja teha riske maandavaid tegevusi. Virtuaalvääringu teenuse pakkujate arvukus oli 2021. aastal kasvutrendis, nt 01.09.2021 seisuga oli menetluses 259 tegevuslubadega seotud taotlust. Samaaegselt ei ole langenud VASP-idega seotud välispäringute arv, mis viitab sellele, et hoolimata reeglite karmistamisest jätkuvad kahtlased ja välisriikide õiguskaitseasutuste tähelepanu pälvivad tehingud. Finantssektorile laiemalt on kõige suuremad ohud seotud vahendite liigutamisega VV teenusepakkujate kaudu ning mitteresidentide või e-residentide Eestis registreeritud äriühingute tegevusega, kellele pakutakse müüdud riiulifirmade nn postkastiteenust (ingl *letterbox*). Tõdetakse, et kuni 2019. aastani oli regulatsioon liialt leebe.[91]

Siiani Eestis VV loamenetluse regulatsiooni puudujääke ja seeläbi järelevalveasutuste võimetust rikkumistele reageerida ilmestab tegelikkuses mastaap, millega Eesti on pidanud VV sektoris silmitsi seisma. Seetõttu on mõistetav, et RahaPTS muudatused on 2017. aastast suunatud reageerimisele rahapesuvastases võitluses kriitiliseks osutunud probleemidele.

2021. aasta lõpu seisuga oli väljastatud 381 Eesti tegevusluba virtuaalvääringu teenuse pakkumiseks, mis mitteametliku statistika kohaselt on 55% kõikidest maailma litsentsidest.[92]

Kuid ka teiste riikide rahapesuvastased seadused, mille sätete kohaselt peab riik VASP-e kontrollima, ei ole piisavad kõikide VV kaasnevate erisuste ja võimaluste reguleerimiseks. VV on

[90] Rahapesu andmebüroo, https://fiu.ee/aastaraamatud-ja-uuringud/aastaraamatud#item-4 (02.03.2022).
[91] Rahandusministeerium, NRA 2020, 7. sektor, lk 9.
[92] Rahapesu Andmebüroo väliskoostöö ülevaade 2021, lk 4 - https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#virtuaalvringu-tee (23.04.2022).

detsentraliseeritud ja seega on VASP-id tehingute ja andmebaaside osas detsentraliseeritud, kuid regulaatoritele kaasneb kohustus kõikide nende tehingute jälgimiseks ja arvestuse pidamiseks. VV seaduslik kasutamine on muutunud riikide jaoks keeruliseks ülesandeks ja on panku, mis on keeldunud VV vahetuse aktsepteerimisest, et vältida rahapesu tõkestavate seaduste regulatsiooni alla sattumist.[93]

Baseli Instituudi 2021. aasta rahapesu ohuhinnangu kohaselt on virtuaalvarade sektoris oht, et teenusepakkujad otsivad tegevuskoha registreerimiseks leebema regulatsiooniga jurisdiktsioone (ingl *regulator shopping*). Seda riski süvendab virtuaalsete varade globaalne olemus. Kooskõlas toimiva ülemaailmse tegevustiku puudumine võib seega viia selleni, et mõned jurisdiktsioonid muutuvad virtuaalvarasid kasutava ebaseadusliku tegevuse peidupaikadeks. Probleemi on tunnistatud Euroopa Komisjoni 2021. aasta ettepanekute paketis rahapesu ja terrorismi rahastamise vastu võitlemiseks, mis sisaldab ambitsioonikat kava ühtlustada VASP-idega seotud AML/CFT õigusakte kõigis ELi jurisdiktsioonides. See on positiivne samm, kuid ilma teiste jurisdiktsioonide ja piirkondlike asutuste sarnaste jõupingutusteta on tõenäoline, et ebaseaduslik tegevus liigub lihtsalt kohtadesse, kus kontrolle on vähem või need puuduvad üldse. Samuti leitakse instituudi uuringus, et erinevad jurisdiktsioonid ei saa virtuaalvaradega seotud rahapesuohtudega hakkama.[94]

Eestis on menetluses ÜMIVS eelnõu, millega viiakse VV teenuse pakkujate tegevusloa andmise ülesanne ja järelevalve Finantsinspektsiooni pädevusse ning kehtestatakse täiendavaid nõudeid, eelkõige vajadusest tagada senisest suurem investorite kaitse. Finantsinspektsioonilt tegevusloa taotlemise võimalus tekib VV vahendajatel 2023. aasta alguses.

15.03.2022 võeti vastu RahaPTS VV-ga seotud muudatused, mille eesmärk on valdkonnas läbipaistvuse ja usaldusväärsuse suurendamine. Seadusesse lisati VV ülekandeteenus ning selle väljastamine, pakkumine, müügi korraldamine või sellega seotud finantsteenuse osutamine. Muudatused hõlmavad seaduse §-s 25 hoolsusmeetmete erisuste rakendamise osas FATFi nn „*travel rule*-i“ nõuet. See tähendab, et VV ettevõtjad peavad krüptoülekandes saatma vastaspooltele samasuguse teabe, mida edastavad pangad ja maksevahendajad rahaliste vahendite ülekandmisel. Teave hõlmab lisaks isikuandmetele tehingu kordumatut tunnust, maksekonto või

[93] Preller, F. 2008, Comparing AML legislation of the UK, Switzerland and Germany, Journal of Money Laundering Control, Vol. 11 No. 3, pp. 241 - https://www.emerald.com/insight/content/doi/10.1108/13685200810889380/full/html (14.02.2022).
[94] Basel Institute on Governance. Basel AML Index 10th public edition 2021, p 9.- https://baselgovernance.org/basel-aml-index (22.01.2022).

virtuaalvääringu rahakoti identifikaatorit. RahaPTS §-d 70-72[5] sätestavad põhjaliku dokumentatsiooni esitamise kohustuse VV tegevusloa taotlemisel, mis hõlmab äriplaani, nõudeid omavahenditele, andmeid kavandatavate teenuste osutamiseks vajalike infotehnoloogiliste süsteemide ning muude tehnoloogiliste vahendite ja süsteemide kohta, kõrgendatud nõuded virtuaalvääringu teenuse pakkuja asukohale, tegevuskohale, juhatuse liikmetele ja kontaktisikule. VASP peab omama omavahendeid kas algkapitali ehk 100 000 või 250 000 euro ulatuses või sõltuvalt pakutavast teenusest üldkulude või tehingute mahu meetodil arvutatud suuruse ulatuses.

Autori hinnangul seisnevad seaduse muudatuste põhilised probleemid viidatud tehniliste lahenduste (infotehnoloogilised süsteemid ning muud tehnoloogilised vahendid ja süsteemid) puudumises. Seaduses nõutav VASP-i kavandatavate teenuste osutamisel kasutatavad tehnoloogilised vahendid peavad hõlmama vahendeid, mille abil täidab ettevõtja RahaPTS §-s 25 sätestatud hoolsusmeetmeid. Regulatsiooni uudsuse tõttu puudub teave, kuidas selline infovahetus tehingute osapoolte ja järelevalveasutuste vahel välja hakkab nägema. Eesti on liikunud VV teenusepakkujate aruandluse leebe regulatsiooni poolelt oluliselt karmimate nõuete kehtestamise suunas. Valdkonnas tuvastatud riske arvestades oli see vajalik, kuid kuna sellised nõuded (mh „*travel rule*“) ei ole Euroopa Liidu riikides ühtselt kehtestatud, rääkimata maailma mastaabist, siis kerkivad esile uued probleemid. Teistes riikides sarnaste registreerimisnõuete ja tehinguandmete kogumiseta on tõenäoline, et ebaseaduslik tegevus (VASP-ide asutamine ja nende kaudu rahapesu teostamine) liigub leebema regulatsiooniga jurisdiktsioonidesse.

Spetsiifilise riski tõstva faktorina on RAB märkinud VASP-ide puhul pesastatud teenuste (*nested services*) pakkumise, mille puhul võib ühe kliendi konto taga peituda suurel arvul teisi kliente, kelle tehingute seiret ei suudeta tagada.[95]
VV tehingute ja tehingupoolte kohta teabe kogumise peamine eesmärk peab olema kriminaalses tegevuses kasutatud VV aadresside tuvastamine, mille suhtes saaks meetmeid kasutusele võtta. Aadresside taga füüsiliste ja juriidiliste isikute tuvastamine on tõkestusmeetmete kontekstis edasise menetluse ülesanne, mis iseenesest ei ole tehingute jälgimisel ajakriitiline.
Eesti Pank on 2018. aastal esimeses finantsstabiilsuse ülevaates leidnud, et VV-dega seotud riskid võib jagada kolme kategooriasse: 1) tarbijate ja investorite riskid, mis on tingitud selgete reeglite puudumisest ning sellest tulenevast pettusohust, 2) tavapärast finantssüsteemi ohusta-

[95] Rahapesu andmebüroo, 2022, lk 5.

vad riskid, mis võivad väljenduda näiteks pankade ja kindlustusseltside seotuses krüptovaradega, 3) rahapesu ja terrorismi rahastamisega seotud riskid, mis tulenevad sellest, et virtuaalvarad võivad võimaldada väärtust üle kanda osapooli identifitseerimata.[96] Seejuures puudutavad tavatarbijat enim just eri liiki pettused, mis võivad hõlmata nii investeeringuid püramiidskeemidesse kui ka kiire rikastumise lootuses investeeringuid VV-sse, mida tegelikult ei ole olemas.[97]

Käesoleva töö eesmärki silmas pidades on autor koondanud järgnevalt ka erinevate rahvusvaheliste organisatsioonide ja siseriiklike asutuste ajakohased hinnanguid seoses VV kasutamisega rahapesu eelkuritegude toimepanemisel ja finantssüsteemi integreerimisel. Autor on kasutanud ülevaateid Suurbritannia, Saksamaa ja Šveitsi rahapesuvastastest regulatsioonidest ja riiklikke riskihinnanguid seoses VV kasutamisega rahapesu meetodites. Nimetatud riikide näited osutavad ehk kõige olulisemale probleemile seoses VV-ga, nimelt ühtse rahvusvahelise ja regulatsiooni kehtestamise keerukusele selles valdkonnas.

Näiteks Šveitsis asub nn krüptoorg (Crypto Valley)[98] ja riik soodustab VV käivet ettevõtetes, Saksamaal kehtivaid sätteid peetakse selles osas pigem piiravateks. Suurbritannia seadused on selles osas kõige karmimad, mille kohaselt jälgitakse laialdaselt rahapesu tegevusi ja digitaalvaluuta kasutamist. Leitakse, et ebaselgust on palju, aga informatsiooni ja juhiseid seadusliku ning ebaseadusliku tegevuse kohta VV ja rahapesuga seoses on vähe.[99]

Maailma riikidest keelas Hiina hiljuti VASP-id ja nende veebipõhised maksekanalid. Keelatud teenused hõlmavad nimetatud ettevõtete registreerimist, küptovaluutaga kauplemist, tasaarvestust ja arveldust. Eraisikud võivad siiski omada digitaalset valuutat.[100] Samuti tegi Venemaa keskpank 2022. aasta jaanuaris ettepaneku keelata krüptovaluutade kasutamine ja kaevandamine Venemaa territooriumil, viidates ohtudele riigi finantsstabiilsusele, kodanike heaolule ja

[96] Finantsstabiilsuse ülevaade 1/2018. Tallinn: Eesti Pank 2018, lk 21, - https://www.eestipank.ee/publikatsioon/finantsstabiilsuse-ulevaade/2018/fi nantsstabiilsuse-ulevaade-12018 (23.02.2022).

[97] Oengo, O. F. Virtuaalvääringu teenuse regulatiivsed eripärad, senine areng ja perspektiiv. – Juridica 2020/8, lk 653. - https://www.juridica.ee/article_full.php?uri=2020_8_virtuaalv_ringu_teenuse_regulatiivsed_erip_rad_senine_areng_ja_perspektiiv&pdf=1 (02.02.2022).

[98]SWI swissinfo. „Swiss ‘Crypto Valley’ boasts 14 'unicorns'“ (2022) - https://www.swissinfo.ch/eng/swiss--crypto-valley--boasts-14--unicorns-/47291870, (15.02.2022).

[99] Wronka, C. (2021) - Anti-money laundering regimes: a comparison between Germany, Switzerland and the UK with a focus on the crypto business - https://doi.org/10.1108/JMLC-06-2021-0060 (19.02.2022).

[100] Reuters (2021), “China bans financial, payment institutions from cryptocurrency business” - https://www.reuters.com/technology/chinese-financial-payment-bodies-barred-cryptocurrency-business-2021-05-18/ (19.02.2022).

rahapoliitika sõltumatusele. See on viimane samm ülemaailmses krüptovaluutade survestamises, kuna valitsused Aasiast Ameerika Ühendriikideni on mures, et eraomandi juhitavad ja väga volatiilsed digitaalsed valuutad võivad kahjustada nende kontrolli finants- ja rahandussüsteemide üle. Venemaa keskpanga sõnul tehakse koostööd järelevalveasutustega riikides, kus VASP-id on registreeritud, et koguda teavet Venemaa klientide tegevuse kohta. Viidati sammudele, mida on astutud näiteks Hiinas krüptoraha aktiivsuse piiramiseks. Venemaa on *bitcoi-n*ide kaevandamise mahult maailma suuruselt kolmas riik Ameerika Ühendriikide ja Kasahstani järel. Venemaa keskpank teatas, et krüptokaevandamine tekitab probleeme energiatarbimises. *Bitcoin*i ja teisi krüptovaluutasid "kaevandavad" võimsad arvutid, mis konkureerivad globaalses võrgus keeruliste matemaatiliste mõistatuste lahendamisel teistega. Protsess neelab elektrit ja seda toidavad sageli fossiilkütused.[101]

Keelustamise tee valimine on üks võimalik viis krüptoraha probleemi piiramiseks, kuid see võib põhjustada laiemat ebaseaduslikku vahendustegevust isikult-isikule, tumeveebi jm võimaluste kaudu, vähendades veelgi ülevaadet VV teostatavatest tehingutest. Venemaa VV kaevandamismahtu silmas pidades on ebatõenäoline, et kaevandamise keeldu tegelikkuses kontrollida suudetaks.

2017. aasta lõpus juhtis *bitcoin*i vahetuskursi erakordne tõus avalikkuse ja meedia tähelepanu krüptovaradele ning juba varajases staadiumis olid riigid sunnitud *bitcoin*i üle kontrolli puudumise ja selle anonüümsuse tõttu tegelema seonduvate võimalike pettuste, rahapesu ja terrorismi rahastamisega seotud riskidega.[102] Suurbritannia on oma 2020. aasta riskihinnangus hinnanud VV-te rahapesuks kasutamise riski keskmiseks. Aastast 2017 on kurjategijad järjest enam hakanud kasutama VV ja ühendanud neid oma rahapesu meetoditesse.[103] Suurbritannia on alates 2020. aasta jaanuarist allutanud VASP-id rahapesu regulatsioonidele (*Money Laundering Regulations*), mis aitavad vähendada nende tegevusega seotud haavatavusi õigeaegselt. Enne seda ei pidanud näiteks VASP-id täitma kliendi hoolsuskohustust (CDD) ega tuvastama kliendi raha päritolu.[104]

---

[101] Reuters (2022), „Russia proposes ban on use and mining of cryptocurrencies," - https://www.reuters.com/business/finance/russian-cbank-proposes-banning-cryptocurrencies-crypto-mining-2022-01-20/ (23.02.2022).
[102] Swiss National Risk Assessment (NRA), p 7.
[103] UK. National risk assessment of money laundering and terrorist financing 2020, p 7 - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf (19.02.2022).
[104] *Ibid.*, p 70.

Suurbritannia AML/CTF reeglistik ulatub kaugemale AMLD V nõuetest, järgides FATF-i standardeid (välja arvatud 16. soovitus, "*travel rule*"). Reegli rakendamine annab järelevalveasutustele ja õiguskaitseorganitele enam teavet krüptovara ülekande osapoolte kohta, parandades õiguskaitseasutuste võimet "vara jälgida". Leitakse, et VV maaklerid (*over the counter* – OTC teenusepakkujad) võivad olla seotud vahetusteenustega, kuid tegutsevad iseseisvalt, spetsialiseerudes kurjategijatele rahapesuteenuste osutamisele. Rahapesijad võivad kasutada isikult-isikule (P2P, *peer-to-peer*) vahetusplatvorme ning on väga tõenäoline, et organiseeritud kuritegelikud rühmitused kuritarvitavad neid. Kui P2P-vahetusplatvorm vahetab või korraldab krüptovarade vahetamist äritegevuse raames, peab see arvestama rahapesu maandamise riske, vähendades kuritarvitamiste ohtu. Siiski võivad P2P-platvormid viia kasutajad omavahel otsekontakti interneti kaudu või füüsiliselt kokku, andes võimaluse krüptovarade üleandmiseks. Detsentraliseeritud P2P-vahetuste (DEX-id) areng loob selles sektoris samuti võimalikke uusi haavatavusi. DEX-id võimaldavad P2P-vahetussüsteemi otse digitaalsel plokiahelal, suurendades veelgi vahetustehingute anonüümsust kurjategijate vahel ja pakkudes veel ühte tavalise füüsilise kontaktita vahetusviisi. Kriminaalmenetluste statistika kohaselt on krüptovarade abil toimepandava rahapesuga seotud uurimiste ja süüdistuste arv endiselt väike, kuid see on tõusuteel.[105]

Šveitsi riskihinnangu kohaselt tuleneb krüptovarade oht tehingute anonüümsusest ning asjaolust, et suur osa neist tehingutest sooritatakse otse, ilma finantsvahendajata. Enamikul juhtudel ei võimalda krüptovarade aluseks olev tehnoloogia omaniku identiteeti kindlaks teha. Ainult siis, kui krüptovaluutasid ostetakse või müüakse *fiat*-raha eest, saab kindlaks teha vastavate varade tegeliku kasusaaja. Lisaks on äärmiselt raske tõestada krüptotehinguga seotud varade kuritegelikku päritolu. VV uus tehnoloogia on suur väljakutse ka prokuratuuridele. Krüptovarade tegelike kasusaajate tuvastamine ja selliste varadega seotud tehingu kriminaalse tausta tuvastamine ei ole mitte ainult raske, vaid ka tehniliselt on võimatu konfiskeerida rahakotti hoiustatud vara ilma vastava privaatvõtmeta. Lisaks, kuna VV tehingud on tavaliselt piiriülesed, on sellega seotud kuritegude eest vastutusele võtmiseks vaja rahvusvahelist õiguskaitseasutuste koostööd.[106]

Analüüsidest ilmneb läbiv probleem, et rahapesukuriteo tõendamise kõige keerulisem osa on eelkuriteo väljaselgitamine, kuna VV-ga seotud kuritegude puhul tehakse tehingud viivitamata ja tehingu osapooled ning vahendusteenuse pakkujad asuvad erinevates jurisdiktsioonides. Silmas tuleb pidada, et eelkuritegude tõendamisstandardi ulatuse ja kuritegudega seotud vara

[105] *Ibid.*, p 74.
[106] Swiss National Risk Assessment (NRA), p 4.

mõiste määratleb direktiiv rahapesu vastu võitlemise kohta kriminaalõiguse abil[107], mille kohaselt piisab süüdimõistmiseks, kui on tehtud kindlaks, et vara saadi kuritegelikust tegevusest, ilma et oleks vajalik teha kindlaks kõik kuritegeliku tegevusega seotud tegelikud üksikasjad ja asjaolud, sealhulgas süüteo toimepanija isik.

FATF tuvastas oma 2021. aasta standardite kohaldamisel riikides põhiliste probleemkohtadena:

1) "*Travel rule*"-i ehk ülekande info nõude ebapiisav rakendamine, mis tähendab, et teavet krüptovaluuta tehingute algatajate ja kasusaajate kohta ei koguta ega tehta kättesaadavaks pädevatele asutustele.
2) AML/CFT kohustuste aeglane rakendamine virtuaalvarade sektoris, koos harvade kontrollide ja sanktsioonidega.
3) Üldiselt järelevalveasutustes teadmiste ja oskuste puudumine virtuaalvarade valdkonnas, mis vähendab nende võimet VASPe kontrollida ja juhendada.[108]

Hiljuti esile kerkinud suhteliselt uus VV-te alaliik nn stabiilsed krüptovarad (*stablecoins)* pälvis nii üldsuse kui ka regulatiivasutuste tähelepanu kõikjal maailmas. Kuigi VV turg on suuruselt tagasihoidlik ega kujuta endast veel ohtu finantsstabiilsusele, võib olukord muutuda, kui tekivad nn ülemaailmsed stabiilsed krüptovarad. Nende varade puhul püütakse saavutada laialdasemat kasutuselevõttu selle abil, et neile lisatakse väärtust stabiliseerivaid elemente ja kasutatakse ära neid varasid propageerivatest äriühingutest tulenevat võrguefekti. Kuna krüptovarad on plokiahela tehnoloogiate peamine rakendus, toetatakse terviklikku lähenemisviisi plokiahelale ja DLT-le, eesmärgiga seada Euroopa plokiahela innovatsiooni ja kasutuselevõtu esirinda. Selles valdkonnas tehtud poliitiline töö hõlmab muuseas usaldusväärsete plokiahelarakenduste rahvusvahelise ühendusega kavandatud avaliku ja erasektori partnerlusi.[109]

USA Rahandusministeeriumi finantskuritegevuse vastase võitluse büroo, ehk USA rahapesu andmebüroo - *Financial Crimes Enforcement Network* (FinCEN)[110] märgib, et kujutades endast küll märkimisväärset finantsinnovatsiooni, on VV osakaal samaaegselt mitmesugustes internetis toimuvates ebaseaduslikes tegevustes kasvuteel.

VV aktuaalsemate riskidena ja riiklike haavatavustena käsitleb autor järgnevas alapeatükis küberkuritegevust ja küberpesu, mille abil jõuab kuritegelikku tulu kõige rohkem finantssüsteemi

[107] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2018/1673.
[108] FATF (2021), Second 12-month Review Virtual Assets and VASPs, FATF, Paris, France - https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf (21.03.2022).
[109] Euroopa Komisjon. (2020) Ettepanek: Euroopa Parlamendi ja Nõukogu määrus, mis käsitleb krüptovaraturge ja millega muudetakse direktiivi (EL) 2019/193, COM(2020) 593 final
[110] Vt https://www.fincen.gov/ (13.04.2022).

ja mida kasutatakse muuhulgas võõrriikide mõjutustegevuses. Nimetatud ohte silmas pidades selgub konkreetsem reguleerimisvaldkond ja spetsiifilised meetmed, mida tuleks riskide vähendamiseks vastavalt kasutusele võtta.

2.2 Küberkuritegevusega ja tuvastamata päritoluga virtuaalvääringutega seotud riskid

Mõistet "küberkuritegevus" kasutatakse sageli koos mõistega "arvutikuritegevus". Küberkuritegevus tähendab aga kuritegu, mis on seotud nii arvutite kasutamisega kui ka infotehnoloogia ja globaalsete võrkude kasutamisega. Mõiste "arvutikuritegu" viitab ainult arvutite või arvutiandmete vastu toime pandud kuritegudele. Interneti vahendusel toimepandavat rahapesu võib laias laastus seostada kahe probleemiga: 1) interneti kasutamine eelkuritegude (küberkuritegevus) toimepanemiseks ja 2) interneti kasutamist kuritegelikul teel saadud tulu pesemiseks (küberpesu). Seetõttu peab rahapesu tõkestamine käima käsikäes küberkuritegevuse vastase võitlusega.[111]

Küberkuritegevuse eeluurimisel on oluline saada kiiresti teavet sellest, kas sellega võib olla seotud rahapesu kahtlus, see tähendab VV puhul nende aadresside analüüsi, et tuvastada teadaolevad kriminaalses tegevuses varem kasutatud aadressid ja muud andmed, mis viitavad riskidele. Kuna rahapesu kuritegu on erinevalt arvutikuritegudest eelkuritegudena riikides ühtlasemalt ja rangemate karistusmääradega kriminaliseeritud, on ka riikidevaheline kriminaalkoostöö tõsisema kahtluse korral tõhusam.

Riigiprokuratuur tõdeb, et ilma varem kogutud taustainfota ehk sihtmärgipõhise uurimiseta antakse näiteks küberrünnakute puhul menetluse algusfaasis pigem tagasihoidlik karistusõiguslik hinnang, piirdudes tihti arvutikuriteo ettevalmistamise kahtlusega või mõne küberkuriteo toimepanemise katsega ja digitaalsete tõendite kogumine vahetult pärast kuriteo toimepanemisest teadasaamist on olnud problemaatiline.[112]

Justiitsministeeriumi kuritegude statistikast nähtub, et 2019. aastal oli Eestis registreeritud 10 657 kuritegu, millest saadud kuritegelik tulu võib olla hüpoteetiliseks rahapesu allikaks. Sellis-

[111] Nizovtsev, Y.Y., Parfylo, O.A., Barabash, O.O., Kyrenko, S.G. and Smetanina, N.V. (2021), p 4 - "Mechanisms of money laundering obtained from cybercrime: the legal aspect", Journal of Money Laundering Control - https://doi.org/10.1108/JMLC-02-2021-0015 (03.02.2022).

[112] Prokuratuuri aastaraamat 2021. Rahvusvahelise küberkuritegevuse tõkestamise väljakutsetest tõendite kogumisel (2022) - https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2021/rahvusvahelise-kuberkuritegevuse-tokestamise-valjakutsetest (12.04.2022).

teks kuritegudeks on korruptsioon ja altkäemaks, väljapressimine, pettus, maksukuriteod, küberkuriteod, võltsimised, vargused, ebaseaduslik kauplemine narkootiliste ja psühhotroopsete ainetega jne. Nende kuritegudega seoses arestiti 2019. aastal vara 7,86 mln euro väärtuses.[113]

RAB-i uuringu kohaselt toimub suur osa n-ö kuritegeliku keskkonna arveldamistest virtuaalvääringutes ning neid kasutatakse ka kuritegude ettevalmistamise faasis. Küberkuritegude vaates kasutatakse virtuaalvääringuid peaaegu kõikide kuriteoliikide puhul, väga levinud on näiteks igasuguse kuritegevuslikuks otstarbeks kasutatava taristu või kuritegelike teenuste eest tasumine krüptorahaga, aga ka lunaraha nõudmine krüptorahas.[114]

Küberkuritegevusega on 2021. aasta lõpu seisuga põhjustatud maailma mastaabis hinnanguliselt 6 trln USA dollari ulatuses kahju, mida võib võrrelda USA ja Hiina järel suuruselt kolmanda majandusega. Küberkuritegevuse kahjude hulka arvatakse näiteks ebaseaduslikult omandatud raha, isikuandmed, finantsandmed, intellektuaalomand, andmete kahjustamine ja hävitamine ning mainekahju. See on ajaloos kõige märkimisväärsem rikkuse ülekandmine, mis organiseeritud kuritegelike jõukude häkkimistegevuse ja terrorirühmituste toetamise järsu kasvu tõttu mõjutab ka innovatsiooni ja investeeringuid kogu maailma finantssektoris. Krüptovaluutade abil toimepandud rahapesu maht oli 2020. aastal hinnanguliselt 10 mld dollarit.[115;116]

Küberturbe ettevõtted hindavad, et rahvusvahelise küberkuritegevuse tekitatav kahju kasvab järgmise viie aasta jooksul 15% aastas, jõudes 3 trln USD-lt 2015. aastal 10,5 trln USD-ni aastal 2025. Hinnates kuritegelikelt aadressidelt teenusepakkujate aadressidele saadetud krüptovaluuta kogust, pesid küberkurjategijad 2021. aastal 8,6 mld dollari väärtuses krüptoraha. See tähendab 2020. aasta võrdluses rahapesutegevuse 30% kasvu. Arvestatud on summasid ainult nn krüptovaluutal põhinevast kuritegevusest, näiteks müügist tumeveebis või lunavara rünnakutest, mille tulu saadakse peaaegu alati krüptovaluutas, mitte fiat-rahas. Raskem on arvestada välja seda, kui palju vahetatakse rahapesuks näiteks traditsioonilisest uimastikaubandusest pärinevat fiat-raha ümber krüptovaluutaks.[117]

---

[113] *Ibid*., NRA 2020. – pt 5.3.1., 5.4.1.1.
[114] Virtuaalvääringute teenusepakkujate uuring, RAB 2020, lk 19.
[115] Grauer, K. Updegrave, H. (2021), "The 2021 crypto crime report" - https://go.chainalysis.com/2021-Crypto-Crime-Report.html (15.01.2021).
[116] Wronka, C. (2021), ""Cyber-laundering": the change of money laundering in the digital age", Journal of Money Laundering Control, p 2 - https://doi.org/10.1108/JMLC-04-2021-0035 (19.04.2022).
[117] Morgan, S. (2021), "Cybercrime to cost the world $10.5 trillion annually by 2025" - https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (12.02.2022).

Rahapesu andmebüroole 2020.a esitatud välispäringud olid enamuses seoses kelmusejuhtumitega.[118] Sama trendi näitab 2021. aasta statistika, mille kohaselt on oletatavateks eelkuritegudeks välispäringutes ja spontaansetes infoedastustes kelmused (65%), mille osakaal oli 2020. aastal 50%. Kelmused olid välisriigi päringutes levinuim oletatav eelkuritegu, 32% juhtudest polnud eelkuritegu teada. Oletatavalt kelmustest teenitud tulu pesemisel liikus läbi Eesti tegevusloaga virtuaalvääringu teenuse pakkujate kaudu 140 miljonit eurot. Politsei- ja Piirivalveametile (PPA) saadetud õigusabitaotlustest on 74% samuti seotud kelmustega. PPA-s perioodil 2015–2021 menetluses olnud rahapesu kriminaalasjades olid 92% juhtudest eelkuriteoks kelmused, enamasti arvutikelmused.[119]

Tüüpjuhtumina edastati teistes riikides kelmustega saadud raha Eesti pangakontodele, mille on avanud teises riigis registreeritud makseteenuse pakkujad või VASP-id. Kontodel konverteeriti kuritegelik tulu kas samal või järgmisel päeval virtuaalvaluutaks. Uue mõistena kerkis 2020. a Rahapesu andmebüroo töös esile VIBAN-pangakonto, mis on n-ö tehniline konto makseteenuse pakkujale. Tänu toimivale koostööle Eesti pankade ja piiriüleste makseteenuse pakkujate vahel õnnestub kelmusega saadud ja Eesti VIBAN-kontodele edastatud raha sageli blokeerida juba enne, kui see suunatakse VV rahakottidesse.[120]

VV ülekannete analüüsimisel on pikaajalise kogemusega USA ettevõte Chainalysis[121], mille läbiviidud analüüsi tulemuses torkab silma erinevus krüptovaluutal põhinevate kuritegude erinevus kasutatud rahapesu meetodites. Ebaseaduslikult saadud varadega seotud aadressidelt saadeti alla poole varast DeFi[122] platvormidele. Eriti palju kasutasid seda viisi Põhja-Korea seostega häkkerid. Samas saadi just DeFi protokollidest ebaseaduslikult kätte rohkem krüptovaluutat kui teistelt platvormi tüüpidelt. Ebaseaduslikult teistelt kontodelt ülekantud varade pesemisel kasutatakse ka märkimisväärselt sageli segamisteenust. Petturid seevastu saadavad enamiku varadest tsentraliseeritud VASP-ide platvormidele. See võib viidata petturite suhteliselt piiratud oskuste pagasile. Krüptovaluuta platvormile häkkimine sealt vara ülekandmiseks nõuab paremaid tehnilisi oskuseid kui pettuste toimepanemine. Seega on arusaadav, et need küberkurjategijad kasutavad keerukamat rahapesu strateegiat. Analüüsi raskendab asjaolu, et mõned kurjategijad kasutavad krüptovarasid tavakuritegevusest (*offline*), nt narkokuritegevusest teenitud

[118] Rahapesu andmebüroo (RAB 2020), Aastaraamat, lk 21.
[119] Rahapesu Andmebüroo väliskoostöö ülevaade 2021, lk 3-5.
[120] Rahapesu andmebüroo (RAB 2020), Aastaraamat, lk 21.
[121] Chainalysis on plokiahela andmete platvorm, mis arendab plokiahela analüüsivahendeid. - https://www.chainalysis.com/company/ (05.02.2022).
[122] DeFi ehk detsentraliseeritud rahandus on üks kiiremini kasvavaid sektoreid. DeFi rakendused on ehitatud *smart contract*'e ehk nn nutikaid lepinguid toetavale plokiahelale. Vt https://krupto.ee/kruptoraha/defi-ehk-detsentraliseeritud-rahandus-tousev-trend/ (17.02.2022).

kuritegeliku tulu pesemiseks, samuti ei ole tuvastatud paljud kuritegelikud aadressid. Kuid paremini peidetud rahapesujuhtumeid on võimalik leida mustrite järgi, milles kliendid püüavad vältida vastavusnõuete kohast nn skriiningut - reaalajas ülekannete jälgimist. Näiteks peavad VV teenusepakkujad erinevate regulatsioonide alusel tegema ülekannete teostamisel üle 1000 USD väärtuses täiendavaid tuvastus- jm toiminguid, ehk täitma *travel rule*-i nõuet. Nagu arvata võib, tehakse illegaalsetelt aadressidelt VASP-idele selle vältimiseks ebaproportsionaalselt palju ülekandeid alla lävendi.[123] Tähelepanuta ei saa jätta samas ka väga madala riskiga VV valdkonna väliseid ettevõtteid, mille varjus võib toimuda rahapesu. Seda tuleb arvestada ja arendada ka mittetraditsioonilisi monitooringumeetodeid ja uurimisviise.[124]

Kuna tugevdatud hoolsusmeetmete rakendamine vaid tehingu piirmäära järgi ei täida oma eesmärki, peaks VASP-id sarnaselt *fiat*-raha *smurfing*u tehingutele kohaldama VV tehingute monitoorimisel vastavaid stsenaariumeid, mis tuvastaks samadelt VV aadressidelt väiksemates osades ülekandeid.

Järgnevalt käsitleb autor VV-ga teostatavat rahapesu, mida võivad toetada ebasõbralikud riigid (võõrriigi mahitatud rahapesu) ja millega seotud eelkuriteod võivad olla toimepandud jurisdiktsioonides, millega koostöö kriminaalmenetluses suure tõenäosusega vilja ei kanna.

VV-sid on kasutanud kõrge ohuhinnanguga riigid oma ebaseadusliku tegevuse ja tuumarelvaambitsioonide edendamiseks. Näiteks on Põhja-Koreaga seotud küberkurjategijad alates 2019. aastast tõenäoliselt varastanud küberrünnakutega teenusepakkujate vastu sadade miljonite dollarite eest VV-sid. Ebaseaduslikult saadud VV-d on pestud teiste teenusepakkujate ja rahakottide kaudu ning saadud tulu on kasutatud massihävitusrelvade ja ballistiliste rakettide programmide rahastamiseks. Kahjukannatajad ja varastatud raha pesemiseks kasutatud asutused asuvad mitmes riigis, rõhutades taas VV-ga seotud finantskuritegude ülemaailmset olemust.[125]

Seaduseelnõu 771 SE seletuskirja kohaselt on Eestis üheks rahapesu tõkestamise probleemsituatsiooniks olnud krediidi- ja makseasutuste kontodele kantavad teadmata päritoluga rahad ja raha päritolu ei ole tuvastatav, sest rahvusvahelistele õigusabipalvetele vastuste saamisega on

[123] The Chainalysis 2022 Crypto Crime Report, p 13 - https://go.chainalysis.com/2022-crypto-crime-report.html (02.03.2022).

[124] Frechtling, D. (2017), "Recognising and thwarting transaction and payment laundering", Journal of Payments Strategy and Systems, Vol. 11 (2), p. 119. - https://hstalks.com/article/2159/recognising-and-thwarting-transaction-and-payment-/ (08.01.2022).

[125] Financial Crimes Enforcement Network U.S. Department of the Treasury. Anti-Money Laundering and Countering the Financing of Terrorism National Priorities June 30, 2021, pp 4-5 - https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf (12.02.2022).

suured probleemid. Seega puudub tihti võimalus algatada skeemis osalejate suhtes kriminaalmenetlust rahapesu kuriteo tunnustel. Lisaks rahapesujuhtumitele ning kriminaaltulu transiidile on Eestit läbivaid tuvastamata päritoluga rahavooge võimalik kasutada riiklikus mõjutustegevuses. Praktikas on tuvastatud juhtumeid, kus läbi Eesti finantssüsteemi toimusid lääne institutsioonide vastu suunatud riiklikud mõjutustegevused. Mööndakse üha selgemalt, et esineb olukordi, kus rahapesu võib olla mahitatud või korraldatud meile mittesõbralike kolmandate riikide asutuste poolt ja rahapesuks kasutatakse uudseid digitehnoloogilisi kanaleid.[126] Ka RAB on pangatehingute analüüsimisel jõudnud infoni, et näiteks läbi Danske Bank Eesti filiaali tehtud tehingute on teostatud riiklikku mõjutustegevust.[127]

Idasuunalistele rahavoogudele traditsioonilise rahapesu kuritegevusega seoses viitab autor seetõttu, et RAB-i analüüsitulemused näitasid selgelt, et ka märkimisväärsel osal ettevõtetest, mis omasid VV teenuse osutamiseks Eesti tegevusluba veel 2020. aastal, oli tegelik äritegevus välismaal ning seos Eestiga puudus. Peamiselt ilmnes analüüsi käigus nende ettevõtete Venemaa, Läti või muu Ida-Euroopa riigi taust.[128] Samas tunnistas RAB 2020. aastal kehtetuks 1784 ja 2021. aastal 329 virtuaalvääringu teenuse pakkumise tegevusluba.[129]

V. Veebel osundab oma arvustuses tähelepanu vahenditele, millega Venemaa Läänemere regioonis pingeid ja survet kasvatab. Nimelt on kasutusele võetud hübriid- või asümmeetrilise konflikti vahendid ja seoses sellega tuleb tavapärase (klassikalise) tsiviilkäibes rahapesu kõrval silmas pidada võõrriigi mahitatud või korraldatud rahapesu. Sedalaadi rahapesu tuleb lugeda hübriidohtude üheks vormiks. Nii võiks võõrriigi mahitatud või korraldatud rahapesu olla näiteks üheks osaks vabade valimiste mõjutamisest või küberrünnakust.[130]
Võõrriikide mahitatud või korraldatud rahapesu korral tsiviilkäibes rahapesu tõkestamiseks mõeldud meetmed ei toimi asjaolu tõttu, et rahapesu definitsioon ei ole sellistes skeemides asjakohane. Võõrriigi mahitatud või korraldatud rahapesu juures klassikalisele rahapesu mudelile

[126] Riigikogu. Seletuskiri audiitortegevuse seaduse, finantskriisi ennetamise ja lahendamise seaduse ning teiste seaduste muutmise seaduse (finantsvaldkonna väärteokaristuste reform, EL-i õigusest tulenevad karistused, vara legaalse päritolu pööratud tõendamiskoormus) eelnõu juurde (771 SE seletuskiri. 2018) lk 18-20. - https://www.riigikogu.ee/tegevus/eelnoud/eelnou/789782cb-80df-4e9e-9bcb-a09b5b318755/Audiitortegevuse%20seaduse,%20finantskriisi%20ennetamise%20ja%20lahendamise%20seaduse%20ning%20teiste%20seaduste%20muutmise%20seadus%20(finantsvaldkonna%20v%C3%A4%C3%A4rteokaristuste%20reform,%20EL-i%20%C3%B5igusest%20tulenevad%20karistused,%20vara%20legaalse%20p%C3%A4ritolu%20p%C3%B6%C3%B6ratud%20t%C3%B5endamiskoormus) (12.04.2022).
[127] Valitsuskomisjoni analüüs ja ettepanekud 2018, lk 12.
[128] Virtuaalvääringute teenusepakkujate uuring, RAB 2020, lk 13-14.
[129] Rahapesu andmebüroo. 2022, lk 26.
[130] Veebel, V. „Kas Läänemere-äärne rahu on saavutatav regionaalsete pingutustega?“ Diplomaatia. 2018. https://diplomaatia.ee/kas-laanemere-aarne-rahu-on-saavutatav-regionaalsete-pingutustega (12.01.2022).

omaseid aspekte ei leidu. Suure tõenäosusega on tegu lähteriigi mõistes legaalsest allikast pärit varaga ning omaniku ja eesmärgi varjamine leiavad aset enne tegevusi, mida meie regulatsioonid sanktsioneerivad. Järelikult tuleks uudse rahapesu tüübi vastu võitlemiseks vaadata esmalt üle rahapesu mõiste ja olemus.[131]

Rahapesu tõkestamise valitsuskomisjoni hinnangul ei ole valdaval osal idapoolsete kahtlaste rahavoogudega seotud analüüsitud juhtumitest kriminaalmenetluse alustamiseks olnud piisavalt viiteid eelkuritegudele. Alustatud menetlused on suures osas kohtueelses staadiumis lõpetatud. Põhjuseks on seni Eesti kohtupraktika seisukoht, et ilma vara konkreetsest kuriteosündmusest pärinemist tuvastamata ei ole võimalik käsitleda juhtumit rahapesuna. Näiteks tuuakse nn Ateka kaasus[132], mil ka variisikute kasutamine ning fiktiivsete dokumentide esitamine tehingute kohta pole rahapesu tõendamiseks piisav, kuna ei ole tõendatud raha päritolu konkreetsest kuriteosündmusest. Kriminaalõiguslikud vahendid ei ole rahvusvahelise kahtlaste rahavoogude transiidi tõendamisel töötanud ning see on olnud kindlasti üheks asjaoluks, mis on soodustanud pikaajaliselt ja suures mahus kahtlaste rahavoogude transiiti läbi Eesti finantssüsteemi. Seetõttu ei ole Eesti ka võimeline hindama, millistest osadest kahtlane rahavoog koosneb ning milline on selles legaalse ja illegaalse raha osakaal.[133]

VV kasutamisel ebaseaduslikes tehingutes ja võimalikus seoses riigivõimuga on kindlasti kohane osutada tähelepanu korruptsiooni ilmingutele, mis muutub VV kasutamise korral samuti raskemini tuvastatavaks. Korruptsiooni toimimismehhanism ei ole aja jooksul muutunud, kuid vahendid, mille abil seda teostatakse, peegeldavad muutusi tehnoloogias ja ühiskonnas. Näiteks kasutatakse järjest rohkem VV-sid korrumpeerunud ametnikele maksmiseks. Krüptovaluutade kasutamine ja anonüümsust tõstvate tehnikate, sealhulgas krüpteerimise levimine kasvab jätkuvalt. Küberkuritegevus hõlmab mitmeid erinevaid rünnakutehnikaid ja *modi operandi*sid, mis arenevad varem tundmatuid haavatavusi ära kasutades pidevalt.[134]

Chainalysis on uurinud krüptovaluuta kasutamist erinevates kriminaalsetes tegevustes ja rahapesu seostes. Venemaal on krüptovaluuta kasutamine levinud, kuid seal asuvad ka isikud ja rühmitused, kes panevad globaalses mastaabis toime ebaproportsionaalselt suure osa krüptovaluutaga seotud kuritegevusest. Venemaal on maailma kõige oskuslikumad häkkerid, kuna riigis

[131] Valitsuskomisjoni analüüs ja ettepanekud 2018, lk 46-47.
[132] TlnRnKo, 1-12-12477/74, lahend AS Ateka Resource jt. asjas, milles kohus leidis, et rahapesule eelnevat kuriteosündmust pole tuvastatud ning dokumentide võltsimine ja nende kasutamine on hõlmatud rahapesu koosseisulisest varjamistegevusest.
[133] Valitsuskomisjoni analüüs ja ettepanekud 2018, lk 49.
[134] SOCTA 2021 - https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf , pp 26, 40 (21.02.202).

pakutakse suurepärast arvutiteaduste haridust, mille kasutamiseks on aga oskajatel vähe majanduslikke väljavaateid. Seega pole imestada, et Venemaa on lunavararünnakute valdkonnas teerajaja ja sealse päritoluga lunavara seoste ulatus on ülisuur. Chainalysis seostab lunavararünnakuid Venemaaga eelkõige kolmel alusel: 1) Evil Corp – Venemaal asuv küberkurjategijate ühendus, mis arvatakse olevat seotud Vene valitsusega, 2) Sõltumatute Riikide Ühenduse (SRÜ) osalisriikide vältimine, mille puhul kood ei krüpteeri faile, kui tuvastab ohvri nendes riikides või antakse ohvrile dekrüpteerimiskoodid, 3) muud seosed – keel, sidusettevõtete asukoht vm. Sellisel alusel tehtud analüüsi tulemusel on selgunud, et umbes 74% lunavaranõudega saadud summadest, üle 400 mln dollari eest krüptorahasid, on seotud mingil viisil Venemaaga. Samuti on näha, et enamik väljapressitud varadest pestakse eelkõige Vene päritolu teenuseosutajate kaudu ning sealt oluline osa saadetakse samuti Venemaal asuvatele kasutajatele. Pealinna finantskeskuses Moscow City tegutseb mitu tosinat krüptoteenuse osutajat, mis teostavad märkimisväärses mahus rahapesu. Kolmeaastase perioodi (2019-2021) jooksul on need ärid saanud 700 mln dollari eest krüptorahasid aadressidelt, mis on eranditult seotud ebaseadusliku tegevusega. Enamiku raha päritoluks on pettused, tumeveebi turud ja lunavara nõuded. Suurimate rahapesu kahtlusega mahtudega ettevõtted on nende seas Garantex, Eggchange, Bitzlato, Suex jt. Jaanuaris 2022 pidas Vene politsei kinni 14 teenusepakkujat REvil-i nimelisest lunavaraorganisatsioonist.[135] See on väidetavalt ainus kord, kui kohalikud võimud lunavararünnaku vastu meetmeid rakendavad. Viimati kirjeldatud Venemaaga seotud rahapesujuhtumid ja VV käibed ei saaks toimida sellisel viisil ja kohas sealse riigivõimu toetuseta või teadmiseta. OFAC[136] on lisanud oma sanktsioonide nimekirja Vene krüptoteenuse osutaja Garantex 2022. aasta aprillis[137] ja lunavaranõuetest saadud varasid vahendanud VASP-i Suex 2021. aasta septembris.[138] Eestis tunnistas RAB kehtetuks Garantex Europe OÜ tegevusloa, mille tegevuses esines süsteemseid ja süstemaatilisi puuduseid. Selle äriühingu tehingute mahud olid aastas üle 5 mld euro (tegevusluba kehtis 27.11.2020 kuni 24.02.2022) ning suur osa ärist ja klientidest oli seotud Venemaaga ning teiste kõrge riskiga riikidega. RAB tuvastas, et äriühingus rikuti isikusamasuse tuvastamise kohustust üle 90% klientide puhul ning äriühingu kaudu liikunud vara oli

[135] The Chainalysis 2022 Crypto Crime Report, pp 14-17.
[136] The Office of Foreign Assets Control ("OFAC") - https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information (02.03.2022).
[137] OFAC Sanctions Hydra Following Law Enforcement Shutdown of the Darknet Market, As Well As Russian Exchange Garantex - https://blog.chainalysis.com/reports/hydra-garantex-ofac-sanctions-russia/ (15.04.2022).
[138] Crypto Crackdown: OFAC Sanctions SUEX Cryptocurrency Exchange, 2021 - https://www.jdsupra.com/legalnews/crypto-crackdown-ofac-sanctions-suex-3337719/ (18.04.2022).

seotud kuritegevusega või rahakottidega, mida kurjategijad olid kasutanud ebaseaduslikel eesmärkidel.[139]

Sarnaselt varasemalt analüüsides tuvastatud idasuunaliste kahtlaste rahavoogudega toimub ka VV sektoris üldiselt sarnane varade liikumine võimalikus rahapesu protsessis selle kihitamise etapis, kuigi teadaolevad eelkuritegude liigid on muutunud.

RAB-i töödeldud välispäringute ja PPA-le saadetud õigusabitaotluste andmed viitavad sellele, et Eestit kasutatakse rahapesu protsessis välisriikidest saadetud varade kihistamise etapis, milles varjatakse kuritegelikul teel saadud vahendite päritolu ja edasine integratsioonifaas toimub taas välisriigis. 90% analüüsitud välissuhtluse kaasustest kinnitab, et Eesti on rahapesukahtlusega vahendite liikumisel transiitriik. Võrreldes teiste riikidega on suuremad Lätist ja Venemaalt laekunud rahasummad. RAB märgib, et jätkuvalt on märgata Eesti äriühinguteenuse pakkujate idasuunalise äri mõjusid, kes on suunanud oma tegevuse idapoolsetele (Venemaa, Ukraina, Valgevene) klientidele. Samuti on märgata Venemaa suunalt suuremat Eesti tegevusloaga virtuaalvääringu teenuse pakkujate kasutamist illegaalsete vahendite liigutamisel.[140]

3. Meetmed rahapesu tõkestamiseks ja tuvastamiseks virtuaalvääringute tehingutes

3.1 Tehnoloogiate edendamine ja rakendamine

Autor viitas töös (vt pt 1.1), et regulatsioone VV ja laiemalt tehnoloogiliste uuenduste valdkonnas muudetakse kõrget riskitaset arvestades sageli, püüdes tuvastatud riske maandada eeldusel, et õiguslik raamistik, sealhulgas karistusmeetmed on ühetaoliselt rakendatavad. Keskendutakse finantsinnovatsiooni jälgimisele, teadmiste jagamise ja tehnoloogilise neutraalsuse edendamisele regulatiivsetes ja järelevalvealastes lähenemisviisides.

Konkreetsetest meetmest on arendatud finantstehnoloogiat (FinTech), mis viitab tehnoloogiapõhistele finantsteenustele ja regulatiivtehnoloogiat (RegTech), mis tähendab uute tehnoloogiate kasutuselevõttu, et hõlbustada regulatiivsete nõuete täitmist.[141]

---

[139] Rahapesu Andmebüroo. (2022). Garantex Europe OÜ kaotas õiguse pakkuda virtuaalvääringutega seotud teenuseid. - https://fiu.ee/uudised/garantex-europe-ou-kaotas-oiguse-pakkuda-virtuaalvaaringutega-seotud-teenuseid (22.04.2022).

[140] Rahapesu Andmebüroo väliskoostöö ülevaade 2021, lk 17.

[141] Euroopa Komisjon. Komisjoni aruanne Euroopa Parlamendile ja Nõukogule siseturgu mõjutavate ja piiriülese tegevusega seotud rahapesu ja terrorismi rahastamise riskide hindamise kohta. (2019). lk 3. - https://m.riigikogu.ee/tegevus/dokumendiregister/dokument/febd712d-1712-461f-b716-7ec8660a3dda/ (19.02.2022).

Euroopa Pangandusjärelevalve (EBA) analüüsi[142] kohaselt erineb finantssektor teistest sektoritest oma suure andmehulga ja kõrge reguleeritusse poolest. Seetõttu kujunevad RegTechi ja SupTechi (tehnoloogiate kasutamine järelevalve eesmärgil) lahendused paratamatult finantsturu osaliste ja järelevalveasutuste jaoks tõhusa, turvalise ja jätkusuutliku turu tagamise võtmeks. RegTech hõlmab suhtlemist finantsasutustega, andmete kogumist ja nende haldamise esimesi etappe. RegTechi lahenduste pakkumise-nõudluse turul on kõige aktiivsem just AML/CFT valdkond. EBA on Euroopa tasandil püüdnud luua üldisemat arusaama efektiivsest innovatsioonist AML/CFT vastavusnõuete täitmiseks krediidi- ja finantsinstitutsioonides. EBA andis 2021. aasta direktiivi (EL) 2015/849 alusel välja suunised, milles soovitas võtta ELi õiguses kasutusele meetmeid, et hõlbustada koostalitluslikke piiriüleseid lahendusi digitaalseks kliendisuhte loomiseks, finantsinstitutsioonide tuginemist kolmandate isikute (sealhulgas teiste pädevate asutuste) klientide digitaalsele tuvastatud identiteedile ning andmete taaskasutamist/ülekantavust. EBA väljendas seisukohta, et tunnuseid nagu juriidilise isiku identifikaator (*Legal Entity Identifier* - LEI), unikaalne tehingutunnus (*Unique Transaction Identifier* - UTI) ja unikaalne tootetunnus (*Unique Product Identifier* - UPI) peaks kasutama kohustuslikult, et hõlbustada finantsteenuste digitaalseid ja/või automatiseeritud protsesse. Eelnimetatud EBA analüüsi ja uuringute hinnangul võib AML/CFT RegTechi lahenduste kasutuselevõtt anda lisaväärtust traditsioonilisematele vastavuslahendustele (*compliance solutions*), olenemata ettevõtte sektorist, suurusest või arenguetapist. Peamine lisandväärtus AML/CFT nõuetele vastavusega seotud tegevuste puhul on a) protsessi tõhususe kasv, b) protsessi efektiivsus ja c) andmekvaliteedi kasv.[143]

Käsitledes järgnevalt VV teostatava rahapesu kuritegude eeluurimist, nähakse näiteks Šveitsi siseriiklikus riskihinnangus tehnoloogia arengus, analüüsivahendites (*chain analysis tools*) praegu piiratud võimalusi uurijate abistamiseks krüptovaluutadega teostatava rahapesu eeluurimisel. Kuid see võib kiiresti muutuda. Mitmed uurimisprojektid annavad lootust, et selles valdkonnas tehakse lähitulevikus märkimisväärseid edusamme. Näiteks töötavad mitmed ettevõtted praegu välja IT-vahendeid segamisteenust (*mixer service*) läbinud krüptotehingute jälgede rekonstrueerimiseks. Rahvusvahelisel tasandil osales Šveits TITANIUM-projektis (*Tools for the Investigation of Transactions in Underground Markets*, projekt on lõpetatud 2020. aas-

[142] EBA analysis of RegTech in the EU financial sector (2021), pp 42-45.
[143] European Banking Authority, Guidelines ML TF Risk Factors (2021)- https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20ML-TF%20risk%20factors%20%28revised%29%202021-02/Translations/1016926/Guidelines%20ML%20TF%20Risk%20Factors_ET.pdf (20.02.2022).

tal), milles Interpoli juhtimisel tegid koostööd mitme riigi arvutiteadlased ja prokuratuurid. Projekti käigus töötati välja teenused ja kriminalistikavahendid krüptotehingute läbipaistvuse parandamiseks, tehingute trendide tuvastamiseks tumeveebi turgudel ja kohtus kasutatavate aruannete loomiseks.[144] Need vahendid täiendavad prokuratuuri väljaõppeprogramme küberkuritegevuse valdkonnas ja 2018. aastal loodud spetsialiseeritud riikliku õiguskaitse koostöö platvormi Cyberboard. Riskihinnangus jõutakse järeldusele, et tänu nendele erinevatele meetmetele on Šveits välja töötanud parima võimaliku regulatiivse mehhanismi, et võidelda krüptovaradest tuleneva ohuga. Kuigi see mehhanism ei kõrvalda kõiki haavatavusi, saab neid märkimisväärselt vähendadagi ainult rahvusvahelise lahenduse abil.[145]

Euroopa Parlamendi 2021. aasta resolutsioonis tehisintellekti kohta kriminaalõiguses ning tehisintellekti kasutamise kohta politsei- ja õigusasutuste kriminaalasjades leitakse, et „/…/ tehisintellekti rakendused võivad pakkuda õiguskaitse valdkonnas suurepäraseid võimalusi, eelkõige õiguskaitse- ja õigusasutuste töömeetodite parandamisel ning teatavat liiki kuritegudega, eelkõige finantskuritegudega, rahapesuga ja terrorismi rahastamisega, teatavat liiki küberkuritegevusega tõhusamal võitlemisel /…/, kuid samal ajal võivad nendega kaasneda märkimisväärsed ohud inimeste põhiõigustele; arvestades, et tehisintellekti üldine kasutamine massijälgimise eesmärgil oleks ebaproportsionaalne.“[146]

Uuritud on juhendatud masinõppe kasutamise võimalusi, et maandada rahapesuriske VASP-ide tegevuses[147], kes eelistavad rahapesuvastaste meetmete rakendamisel reeglipõhist süsteemi (*rules-based system*), sest esineb probleeme riiklike vastavuseeskirjade täitmisel ning finantsjärelevalvele ei suudeta selgitada masinõppe kasutamise vajadust. Teised uuringud[148] nn traditsioonilise rahapesu puhul pankades kinnitavad, et kuna enamik masinõppes kasutatavaid algoritme töötavad nn „musta kasti“ meetodil, ei ole alati võimalik selgitada, miks teatud ülekanded markeeritakse ja kinni peetakse. Finantsinstitutsioonidele kehtestatud nõuete kohaselt peavad nad olema suutelised selgitama peatatud ülekannete põhjuseid. Tüüpiline eelistus on seepärast

[144] TITANIUM: Tools for the Investigation of Transactions in Underground Markets (2020) - https://www.titanium-project.eu/ (15.02.2022).
[145] Šveitsi NRA, pp 4-5.
[146] Euroopa Parlament, 2021 - https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_ET.html (03.02.2022).
[147] Ruiz, E. P. Angelis, J. (2021) Combating money laundering with machine learning – applicability of supervised-learning algorithms at cryptocurrency exchanges. - https://www.emerald.com/insight/1368-5201.htm (12.02.2022).
[148] Jullum, M., Løland, A., Huseby, R., Ånonsen, G. and Lorentzen, J. (2020), “Detecting money laundering transactions with machine learning”, Journal of Money Laundering Control, Vol. 23 No. 1, pp. 173-186. - https://www.researchgate.net/publication/338726110_Detecting_money_laundering_transactions_with_machine_learning (22.02.2022).

kohandada lihtsam lähenemine, mis toimib halvemini, aga järgib vastavusnõudeid. Reeglipõhise süsteemi kasutamine vastavusnõuete järgimise tõttu on paradoksaalne. Näitena tuuakse 1Malaysia Development Berhadi (1MDB) skandaal ja Danske Bank, mis kasutasid seda lähenemist ja neile määrati ikka miljonite eurode ulatuses trahve. Kuigi reeglipõhised süsteemid võimaldavad teenuspakkujatel ülekannete peatamist õigustada ja vastavusnõudeid täita, ei tee need kõike võimalikku rahapesu tõkestamiseks ning neid karistatakse ikka. Lisaks annab reeglipõhine süsteem ülekannete eksponentsiaalsel kasvamisel kõrgel määral valepositiivseid vastuseid. Kokkuvõttes leitakse uuringus, et kõik vaadeldud algoritmid toimivad paremini kui traditsioonilised reeglitel põhinevad süsteemid. Sobiv lahendus oleks pooleldi juhitav uute algoritmidega masinõpe.

Siiski on praegused VASP-ide ebaseaduslike ülekannete märgistamiseks kasutatavad masinõppe tehnikad aeglased ja ei toimi reaalajas. Praktiliselt on soovitatav keskenduda algoritmide reageerimisaja parandamisele. Seda ülesannet ei suuda aga seda enam täita kohustatud isikute vastavusnõuete (*compliance*) üksused, sest nende uurimised võtavad aega, kuna neid teostavad tõenäoliselt isikud erinevates VASP-ides või geograafilistes piirkondades. VV tehinguid ei jõutagi kahtlaseks märkida, et neid reaalajas menetleda.[149]

Suurimate takistustena innovatsioonis AML/CFT turul näevad RegTechi pakkujad turvalisuse ning andmekaitse probleeme ja regulatsioonide puudust ning soetushinda. Samasugused head ja vead on tehnoloogiliste vahendite kasutamisega rahapesu tuvastamisel selle algetapis, kui tehisintellekt peaks mõistma kõrvalekaldeid VV ülekandes pangandussüsteemi. Samuti lisanduvad probleemid seoses sellega, et tehisintellekt suudab analüüsida seoseid ja tõlgendada andmeid kogumis, kuid ei suuda ette ennustada inimeste käitumist. Tehisintellekti kasutab finantssektor juba praegu pettuste ja rahapesu ennetamisel, maksete klassifitseerimisel, toodete soovitamisel, maksehäirete ennustamisel, krediidivõimelisuse hindamisel, kuid VV tehingute andmehulk ja tehingute kiirus, isikusamasuse (tegeliku kasusaaja) tuvastamine seab selles valdkonnas hoopis suuremad väljakutsed.[150] RAB on oma uuringus leidnud, et VASP-id ei monitoori piisavalt kliendisuhet ega tehinguid. Seda kahtlust süvendab veelgi asjaolu, et mõnedel VASP-idel puuduvad plokiahela analüütilised tööriistad, võimekus tuvastada tumeveebi või mikseritehinguid.[151]

Vaatamata nimetatud keerukatele infotehnoloogiliste takistustele on õiguskaitseorganitel VV seotud kuritegude puhul siiski õnnestunud kriminaaltulu jälitada ja konfiskeerida. Käesoleva

[149] Ruiz, E. P. Angelis, J. pp 9-10.
[150] Jullum, M., *et al*. (2020) pp. 173-186.
[151] Rahapesu andmebüroo 2022, lk 25.

peatüki kirjutamise ajal viimane avalikustatud juhtum on veebruarist 2022, mil USA Justiitsministeeriumil õnnestus arestida 3,6 mld USD väärtuses *bitcoin*e, mis on seotud 2016. aastal Bitfinexi häkkimisega. See on suurim viimase aja varastatud varade arestimine nii krüptovaluutas kui *fiat*-rahas. Lisaks sulges Saksa politsei koostöös USA õiguskaitseasutustega 2022. aasta aprillis Venemaal asuva maailma kõige suurema käibega (2021. aasta käive üle 1,7 mld USD) tumeveebi turu Hydra Market. OFAC lisas seejärel sanktsioonide nimekirja enam kui 100 Hydra krüptovaluuta aadressi ja Vene krüptoteenuse osutaja Garantex.[152] Sarnased juhtumid on olulised mitte ainult seetõttu, et need võimaldavad krüptorahal põhineva kuritegevuse ohvritele kahju hüvitamist, vaid ka kummutavad narratiivi, et krüptovaluutat ei saa jälitada, arestida ja see sobib ideaalselt kuritegelikus tegevuses. Kui küberkurjategijad teavad, et õiguskaitseorganid on võimelised krüptovaluutat arestima, võib see vähendada nende motivatsiooni seda tulevikus kasutada. Võimalus jälitada ja arvutada avaliku andmekogumi põhjal kokku kuritegelikku vara on suur erinevus krüptovaluuta põhise kuritegevuse ja *fiat*-raha põhise kuritegevuse vahel.[153]

Hinnanguliselt on Euroopas ja teadaolevalt kogu maailmas esimese laiapõhjalise, st piisavalt kontrollimeetmeid sisaldava ja samas tulevikku vaatavalt innovatiivse regulatsiooni plokiahela ja krüptovaluutade valdkonnas kehtestanud Liechtenstein.

Liechtensteini seadus *Tokens and TT Service Provider Act* (saksa k lühend TVTG) jõustus 2020. aasta jaanuaris.[154] TVTG koondab ühte plokiahela erinevad kasutusvõimalused, nagu finantsteenused, logistika, mobiilsus, energia, meedia ja palju muud mõiste "*token*i majandus" all. Aadresse, kuhu t*oken*id üle kantakse, nimetatakse TT-identifikaatoriteks. Seadus on kohaldatav "TT-süsteemidele", mis tähendab "usaldusväärsetel tehnoloogiatel põhinevaid ülekandesüsteeme", st plokiahelaid. Üldine mõiste valiti selleks, et tagada seaduse kohaldatavus ka tulevikus. Reguleeritud tehnoloogia määratlemiseks üldiste terminite valimine on TVTG ainulaadne omadus, mis tagab pikaajalise kohaldatavuse. Regulatsioonis on arvestatud, et virtuaalvarad toimivad plokiahelal ja hajusraamatul, mida nende detsentraliseerituse tõttu valitsused kontrollida ei suuda ja mis võimaldab finantskuritegusid toime panna ja karistusest hoiduda. Samal põhjusel puudub võrgusiku eest vastutav isik, keda selles toimuva ebaseadusliku tege-

[152] OFAC Sanctions Hydra Following Law Enforcement Shutdown of the Darknet Market. (15.04.2022).
[153] The Chainalysis 2022 Crypto Crime Report, blog - https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-criminal-balances-criminal-whales/ (03.02.2022).
[154] Teicmann, F. M. J.; Falker, M.-C. (2020) Money laundering via cryptocurrencies – potential solutions from Liechtenstein - https://www.emerald.com/insight/content/doi/10.1108/JMLC-04-2020-0041/full/html (20.01.2022).

vuse eest vastutusele võtta. Senistel püüetel plokiahela tehnoloogiat reguleerida on olnud piiratud edu. Euroopa Liidus on V AMLD kohaldamine põhjustanud arvukate krüpto *start-up*-ide turult lahkumise, mis sellise innovatsiooni väljatõrjumisega kahjustab siseriiklikku majandust. Enamik regulatsioone keskenduvad krüptovaluutadele ja jäetakse kõrvale plokiahela tehnoloogia kasutusvõimalused. Liechtenstein on aga esimene jurisdiktsioon, kus on rakendatud laiapõhjaline raamistik, mis reguleerib lisaks krüptovaluutadele ka plokiahela võimalikke praeguseid ja tulevasi kasutusvõimalusi. Siiski tuleb plokiahela regulatsioonid kehtestada rahvusvahelisel tasemel, et vältida kriminaalse tegevuse liikumist leebematesse jurisdiktsioonidesse. Liechtensteini valitsus on tõestanud, et muutuvale tehnoloogilisele keskkonnale on võimalik reageerida kiiresti ja sisuliselt efektiivsust ohverdamata. Nii võiks Liechtensteini TVTG olla lähtepunktiks plokiahela rahvusvahelisel reguleerimisel.[155]

Autori hinnangul peaks VV tehingute põhine analüüs toimuma infotehnoloogiliselt standardiseeritud vahenditega, mida turuosalised kasutada saaks. Kuna VV tehingutes kuritegudele viitavate tunnuste leidmisel on oluline eelkõige plokiahela analüüs, tuleks seda võimaldavad tööriistad töötada välja koos järelevalvet teostavate asutustega ja õiguskaitseorganitega.

RAB võiks olla vastutav taoliste tehniliste lahenduste standardite väljatöötamise, rakendamise ja sertifitseerimise eest.

Krediidiasutuste üheks probleemiks on asjaolu, et neil ei ole võimalust VV tehinguid peatada, nagu saab teha *fiat*-raha puhul. Väga palju sõltub olukord sellest, milliste kauplemisplatvormidega pank koostööd teeb ja mil määral suudab rahakoti teenuse pakkuja tuvastada plokiahela aadressivahemikud. See on veelgi keerulisem, kui reguleerimata teenusepakkuja asub välismaal. Tehingute monitoorimist peetakse rahapesu tõhusa tõkestamise keskseks vahendiks. See kehtib eelkõige suure kliendibaasiga ettevõtete kohta.

Praktikas määratletakse nn indikaatorid või parameetrid, mille järgi süsteem märgib asjaolu ebatavaliseks. Tunne-oma-klienti (KYC) kohustustest tulenevalt võib turvameedet nimetada tunne-oma-tehingut (*know-your-transaction real* – KYTr). *Fiat*-rahade KYTr-i kohustused saab üle kanda ka VV valdkonda, mida võib nimetada tunne-oma-tehingut-virtuaalselt (KYTv). Selles valdkonnas on võimalus süsteemipõhise tehingute jälgimisega uurida ülekandeid plokiahela analüüsi abil ja paljastada silmatorkavaid tehingud, mis viitavad rahapesule. Töövahend "Chainalysis KYT" võimaldab tuvastada enamike VV-de nagu *Bitcoin, Etherum, Litecoin* ja *Tether* tehingumustrites, jälgitavates rahakottides kahtlaseid kõrvalekaldeid ja anda nendest märku. Erasektori käsutuses olevate vahendite ja võimekuse usaldusväärsust kinnitab asjaolu,

[155] Liechtenstein Legal Gazette. The Tokens and TT Service Provider Act (2021) - https://www.regierung.li/files/medienarchiv/950-6-01-09-2021-en.pdf (07.01.2022)

et selle klientide seas on lisaks VV teenusepakkujatele Föderaalne Juurdlusbüroo (FBI), narkoagentuur (DEA) ja Europol.[156]

See analüüsivahend on üheks näiteks, mille sarnast võiks standardiseerituna kasutada Eestis registreeritavad VV teenusepakkujad ja õiguskaitse- ja järelevalveasutused.

VV teostatava rahapesu tõkestamisel on oluline tagada varade kihitamise etapis ülekannetes kasutatavate VV rahakotiaadresside jälgimine vastavate monitooringuvahenditega. Kuna aga kurjategijad on nendest vahenditest teadlikud, kasutavad nad segamisteenust ning privaatseid VV rahakotte (*unhosted wallet*). Selliste rahakottide kasutajad suhtlevad VV süsteemiga ilma vahendajateta ja nende tehingud ei pruugi kunagi kontrolli alla sattuda.

Selliste tehingute puhul riskide maandamiseks peaks teenusepakkujad sätestama oma riskihinnangule ja riskiisule vastavad piirangud. Võimalus oleks segamisteenust läbinud või privaatsest rahakotist pärit VV tehingud keelata, see tähendaks tuvastatud kahtlaste aadresside nimekirjade loomist (*blacklisting*) ja nende jagamist turuosaliste vahel.

Rahapesu integreerimise etapis peaks teenusepakkuja täiendavalt sätestama VV *fiat*-rahaks vahetamisel piirmäära, mille ületamisel annaks monitooringusüsteem sellest märku ja teostataks tehingu algataja osas kontroll. Kõrvalekallete tekkimisel oleks võimalik viivituseta edastada RAB-i teatis ebaharilikust või rahapesukahtlusega tegevusest.

3.2 Vastutus rahapesu tõkestamise nõuete rikkumise eest

Kuna rahapesu tõkestamine seisneb ennetusmeetmete rakendamises ja tõkestamise nõuete rikkumise eest väärteokaristuste ning rahapesu koosseisu täitvate tegude eest kriminaalkaristuse kohaldamises, annab autor järgnevalt erinevatele hinnangutele ja analüüsidele tuginedes ülevaate võimalikest täiendavatest haldus- ja karistusõiguslikest meetmetest finantssektoris ja kitsamalt VV valdkonnas.

Rahapesu ja terrorismi rahastamise tõkestamise valitsuskomisjon on teinud ettepaneku, et tuleks kaaluda valdkondliku karistusõigusliku raskuskeskme viimist rahapesu RahaPTS kohustatud subjektidele sätestatud hoolsusmeetmete ja riskijuhtimise instrumentide mitterakendamise sanktsioneerimisele.[157]

---

[156] Wronka, C. (2022), "Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures", Journal of Money Laundering Control, Vol. 25 No. 1, pp. 79-94. https://doi.org/10.1108/JMLC-02-2021-0017 (06.01.2022).

[157] Valitsuskomisjoni analüüs ja ettepanekud 2018, lk 52.

Valitsuses on olnud arutlusel haldustrahvimenetluse seaduse (HalTS) eelnõu, mille kohaselt võib haldustrahvi määrata haldusorgan seaduses ettenähtud juhul õigusrikkumise eest. Seda tehakse kindlatele nõuetele vastavas menetluses, millel on nii haldus- kui süüteomenetlusele omaseid tunnuseid ja mis kuulub nn kriminaal-administratiivõiguse valdkonda. Seni on EL-i õigusest tulenevaid kohustusi kohaldada teatud rikkumiste korral kõrgema määraga rahalisi sanktsioone (sh haldustrahve) Eesti õiguses üle võetud läbi sunniraha instituudi.[158] HalTS võimaldaks EL-i õiguses sätestatud trahvide kohaldamist haldustrahvimenetluses, millega lisanduks täiendav menetlusliik ohu ennetamisele ja tõrjumisele korrakaitseseaduse alusel, riiklikule järelevalvele, väärteomenetlusele ja kriminaalmenetlusele.[159]

Euroopa Liidu õiguses sätestatud halduskaristuste kohaldamise perspektiivi Eesti õiguses on analüüsinud Tartu Ülikooli õigusteadlased A. Soo, A. Lott ja A. Kangur. Teadlased leidsid, et olenemata sellest, kas Eesti seadusandja leiab sisulise õigustuse Eesti õiguskorda tekitada eraldi halduskaristused, tuleb arvestada, et menetluslikud garantiid peavad raskete halduskaristuste korral olema siiski samad mis süüteomenetluses. Halduskaristuste paigutamist haldusmenetluse raamidesse on autorite hinnangul põhjendatud kaaluda vaid juhul, kui väärteomenetlust ei õnnestu tõhustada. Võimalus oleks suunata halduskaristuse menetlus üksnes juriidilistele isikutele, eeskätt konkurentsi asjades ja finantsjärelevalves. Lahenduseks võib olla juriidiliste isikute õigusrikkumiste allutamine väärteomenetluse asemel haldusmenetlusele, mis võimaldab väärteomenetlust reformimata muuta Eesti sanktsioonisüsteemi piisavalt tõhusaks.[160]

Täiendava menetlusliigi võimaliku lisandumise kontekstis EL õigusele vastavuse tagamiseks on haldus- ja karistusõiguslike sanktsioonide puhul kirjanduses leitud, et ka näiteks erivaldkondi reguleerivad EL õigusaktid ja finantsjärelevalve asutused ei kasuta ühtset terminoloogiat. Seetõttu ei ole rikkumiste kategoriseerimine ja nendega sanktsioonid piisavalt õigusselged. Kohaldatava sanktsiooni mõistmiseks tuleb seda hinnata haldusõiguslike ja karistusõiguslike põhimõtete abil.[161] Õiguskantsleri arvamuse kohaselt tekiks riigil halduskaristuse korra tekitami-

---

[158] Haldustrahvimenetluse seaduse eelnõu. Eelnõude infosüsteem - https://eelnoud.valitsus.ee/main/mount/docList/e0350345-d819-4adc-bc56-37594d5f815f#d0lnNhIx (12.02.2022).

[159] Justiitsministeerium. Haldustrahvimenetluse seadus saadeti kooskõlastusringile - https://www.just.ee/uudised/haldustrahvimenetluse-seadus-saadeti-kooskolastusringile. (17.04.2022).

[160] Soo, A., Lott, A., Kangur, A. Võimalused Euroopa Liidu halduskaristuste ülevõtmiseks Eestis. Juridica 4/2020., lk 260. - https://www.juridica.ee/article_full.php?uri=2020_4_v_imalused_euroopa_liidu_halduskaristuste_lev_tmiseks_eestis&pdf=1 (12.01.2022).

[161] Kairjak, M. Karistus- ja haldusõiguse piiride hägustumine Euroopa Liidu finantsturgude õiguse uues sanktsioonisüsteemis. Juridica V/2015, lk 359. - https://www.juridica.ee/article_full.php?uri=2015_5_karistus-_ja_haldus_iguse_piiride_h_gustumine_euroopa_liidu_finantsturgude_iguse_uues_sanktsi&pdf=1 (12.04.2022).

sega laialdased võimalused nii rikkumise ärahoidmiseks, selle toimepanemise kahtlusel menetlemiseks kui ka karistamiseks. Aga arvestades tõendite kogumise ja ülekandmise paindlikkust võib riik valida isiku karistamiseks just sellise mooduse, mis riigi vaatepunktist on kas lihtsaim või meeldib riigile mingil muul põhjusel. Isik pannakse seevastu olukorda, kus ta peab arvestama kuni viie erineva menetlusliigi tagajärgedega. Sellises olukorras on isikul keeruline oma õigusi kaitsta ning pole võimalik ennustada, kuidas alustatud menetlus tema jaoks lõpeb. Seetõttu tasub hoolikalt kaaluda, kas uus menetlusliik on vajalik ning mis eesmärki see isiku põhiõiguste kaitset silmas pidades teenib.[162]

NRA tulemuste kohaselt ei ole teiste riikide koostöömehhanismidest tõusetuvaid probleeme võimalik Eesti koostöömehhanismide edasise tõhustamisega mõjutada, seega on asjakohane seonduvate haavatavuste mõju vähendamiseks täiendada karistusseadustikku eraldi rahapesualaste kohustuste rikkumise eest karistust ette nägeva normiga, kehtestades vastutuse kohustatud isiku poolt teadvalt hoolsusmeetmete ja protseduurireeglite kohaldamata jätmise eest. Sama meetmega on võimalik ka vähendada järelevalveasutuste võimekusega seonduvaid haavatavusi.[163]

Kriitikat järelevalveasutustele antud piiratud vahendite kohta on teinud Finantsinspektsioon, nentides, et finantssektori karistuspoliitika raamistik, väärteomenetlused, ei heiduta ja neid ei ole sisuliselt võimalik kasutada nii mõnegi keerukama ega suurema rikkumise korral. Kuna praegune süsteem toodab ja soodustab rikkumisi finantssektoris, siis tuleks luua lihtsamas vormis kiired ja tõhusad halduskaristused. Valitsuse päevakorras on paar aastat ootel olnud eelnõud 111SE (finantsvaldkonna väärteokaristuste reform) ja 94SE (KarS muudatused, EL õigusest tulenevad rahatrahvid) ehk tegu on eelnõudega, millega tõstetakse finantssektori väärtegude trahvimäärasid.[164]

Põhilised probleemid on tuvastatud senise liiga leebe VASP-ide regulatsiooniga, mille osas on RahaPTS-s tehtud eeldatavalt toimivaid ulatuslikke muudatusi. Autori hinnangul toimiks mõjusalt edaspidi VASP-ide puhul rikkumiste eest väärteo korras trahvimine. Nende teenusepakkujate puhul on nagu teiste finantsasutuste puhul kõige olulisem maine ja klientide hoidmine, mistõttu on ennetava meetmena kõige tõhusam karistushirm.

---

[162] Õiguskantsler. Arvamus haldustrahvimenetluse seaduse eelnõu kohta (2020) - https://www.oiguskantsler.ee/et/seisukohad/seisukoht/arvamus-haldustrahvimenetluse-seaduse-eeln%C3%B5u-kohta. (21.02.2022).

[163] Rahandusministeerium, NRA 2020, Lisa 1, lk 4.

[164] Finantsinspektsioon, blogi 13. jaanuar 2022, https://www.fi.ee/et/blogi/hambutud-hammustused-karistuspoliitikas. (16.01.2022).

RAB on kohaldanud VASP-idele sunniraha 2020. aastal kolmel ja 2021. aastal ühel korral, väärteomenetlusi viidi 2020. aastal läbi üks ja 2021. aastal selles valdkonnas väärteomenetlusi läbi ei viidud.[165]

Alates 15.03.2022 kehtiv RahaPTS § 96[1] sätestab, et virtuaalvääringu teenuse pakkuja juhi või töötaja poolt tehingu algatajaga seotud teabe välja selgitamata või kontrollimata jätmise või ärisuhte väliselt teenuse osutamise või muude virtuaalvääringu teenuse pakkuja kohustuste rikkumise eest karistatakse rahatrahviga kuni 300 trahviühikut ja juriidilist isikut karistatakse sama teo eest rahatrahviga kuni 400 000 eurot. Ka teiste, RahaPTS 10. peatükis sätestatud, rikkumiste eest on füüsilistele ja juriidilistele isikutele karistusena ette nähtud samas ulatuses rahatrahvid. Kuna EL-is on finantssektoris halduskaristusena nähtud ette meetmeid (*administrative penalties and other administrative measures*), mille puhul näiteks juriidilise isikule määratav maksimaalne haldustrahv on vähemalt 500 000 eurot, siis saab selles sektoris vajadusel rakendada sunniraha, et EL-i regulatsioonidega kooskõla saavutada.[166]

M. Mäeker ja A. Nõmm on oma käsitluses näiteks pankadele pandud avalik-õiguslike kohustuse osas kuritegevuse tõkestamisel väitnud, et kuna võitlust kuritegevuse ja rahapesu vastu kriminaalõiguslike meetmetega oleme kaotamas, oodatakse eraõiguslikelt isikutelt oluliselt suurema rolli võtmist kuritegude preventsioonis. Siiski tuleb leida parem tasakaal era- ja kriminaalõiguslike meetmete vahel. Autorid leiavad, et kuna kurjategijatest ollakse alati sammu maas, siis tuleb leida võimalused kriminaalõiguslike meetmetega neid tuvastada ja heidutada kuritegusid toime panemast.[167]

Autor on seisukohal, et võttes arvesse VV valdkonnas tuvastatud rahapesuriske, ei ole eraldi lisanduv haldustrahvimenetlus otstarbekas ja piisab seaduses sätestatud kohustatud isiku hoolsusmeetmete rikkumise sanktsioneerimisest. Samuti ei poolda autor selles kontekstis rahapesu kuriteo eest ettenähtud karistuse karmistamist. Karistamise eesmärk on mõjutada kurjategijat uute kuritegude toimepanemisest hoiduma ning kriminaalmenetlusega välditakse ebaseadusliku tulu ülekandmist seaduslikku majanduskäibesse. Arusaadav on järelevalveasutuste surve haldustrahvi menetluse kohaldamiseks finantssektoris krediidiasutuste rikkumistele reageerimiseks, mille puhul kohustatud juriidilise isiku vastutuseks piisaks rikkumise tuvastamisest ning füüsilise isiku süüd ei ole vaja tuvastada. VV tehingutes tuleb aga eelkõige lahendada

[165] Rahapesu andmebüroo, 2022 - https://www.fiu.ee/aastaraamatud-ja-uuringud/uuringud , lk 26.
[166] Seletuskiri ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu juurde, lk 86.
[167] Mäeker, M., Nõmm, A., lk 669.

paljude tehingute sooritajate anonüümsuse probleem ja nende võimaliku ebaseadusliku tegevusega seostamine. Selleks teostatav analüüs ja menetlus tugineb eelkõige VV aadressidel, mille päritolu tuvastamiseks ei kasutata traditsioonilisi vahendeid. Nagu töös eelnevalt selgus, et ei ole kriminaalõiguslikud vahendid rahvusvahelise kahtlaste rahavoogude transiidi tõendamisel toiminud eelkuritegude tõendamise keerukuse või võimatuse tõttu. Veel vähem saaks neid kasutada VV käibe puhul. Oluline on tagada teenusepakkuja hoolsuskohustuse täitmine, mis hõlmab isikute tuvastamist, tehinguandmete edastamist järelevalve teostamiseks. Tähelepanu tuleb koondada nimetatud kohustuste täitmata jätmise tuvastamisele ja rikkumiste eest proportsionaalsete ning mõjusate sanktsioonide väljatöötamisele olemasolevate menetlusliikide raames.

3.3 Teabevahetus ja koostöö

Rahapesuvastases võitluses tehnoloogilistele väljakutsetele vastamiseks peavad kohustatud isikud parandama kahtlastest tegevustest/tehingutest jälgimise ja nendest teavitamise süsteemi. Pangad peavad rahapesu vastu võitlemiseks üldjuhul tegema kolme asja: tundma oma kliendi tegevust, jälgima ja uurima ebaharilikke ülekandeid ning teatama kahtlasest käitumisest kontrolliasutusele. Pankade puhul muutub VV käibega seoses oluliseks võimekus eelkõige VASP-idelt klientide kontodele laekuva raha päritolu kontrollimine nii oma analüüsivahendite kasutamise kui RahaPTS 3. peatükis sätestatud hoolsusmeetmete rakendamise kaudu.

Taani Finantsinspektsioon näeb kõrge rahapesuriskiga valdkondades ühe lahendusena pankadele juurdepääsu andmist riigi kogutud andmetele. Riigiasutused valdavad teavet, mis võib olla kasulik finantsteenuse osutajatele, kes püüavad rahapesu ära hoida. Näiteks võib politsei jagada teavet, mida nad teavad kurjategijate käitumise kohta, et aidata pankadel kahtlasi tehinguid tuvastada. Lihtsustada ja edendada tuleks pankadevahelist infojagamist klientide kohta. Pankadel oleks suur abi klientide informatsiooni tsentraliseeritud andmebaasidest, mis on ühendatud avalike registritega ja mida reguleerib näiteks järelevalveamet. Puudub igasugune majanduslik mõte koguda igaüks eraldi klientide kohta samasugust infot. Samuti tuleb võimaldada pankadel jagada teavet klientide tegevuses tuvastatud ohumärkide (*red flags*) kohta. Rahapesijad kasuta-

vad mitmeid panku, mis muudab ühel ettevõttel probleemsete ülekannete tuvastamise keeruliseks. Üksteisega infot jagades on lihtsam kliendi pangategevusest suuremat pilti kokku panna.[168]

Nimetatud võimalusi tuleks kaaluda ka VV valdkonnas ja anda VASP-idele õigus taotleda andmeid registritest, kuna hoolsuskohustuse jm nõuete osas on nad võrdsustatud krediidiasutustega ja oma kohustuste täitmiseks tuleb nende kasutusse anda asjakohased vahendid. Uudse infovahetusplatvormi on juba välja töötanud ja praegu kohalikul finantsturul tegutsevate krediidiasutuste osalusel 2021. aastal edukalt käivitanud Eesti tehnoloogiaarendajad.[169] AML Bridge-nimeline teabevahetuskanal võimaldab pankadel omavahel lihtsas mitteformaalses vormis jagada teavet kahtlaste klientide ja tehingute osas rahapesu, sanktsioonide, pettuste jt valdkondades, kontrollida taustandmeid, reageerida võimalustel ka reaalajas nt pettusejuhtumitele. Teabevahetusprojekti eesmärgiks on laieneda taolise võrgustikuga üle Euroopa ja mujale maailma, et tõkestada kriminaalset tegevust, aidates kaasa õiguskaitseorganite edasisele uurimisele.

Eestis on valitsuskomisjon VV valdkonna ees seisevate väljakutsete lahendamiseks toonud välja seadusandluse võimalikud arengusuunad[170], mille käigus selgitatakse, kas institutsionaalse raamistiku partnerite vaheline koostöö on sujuv ja tõrgeteta, kas rollide jaotus on organisatsiooniliselt otstarbekalt lahendatud. Samuti kaalutakse institutsionaalse raamistiku partnerite vahelise koostöö formaliseerimise otstarbekust.

Pankade vaates on teabevahetuse puudujäägid ja sellega seotud areng ning innovatsioon pidurdunud jõupingutuste tõttu finantssüsteemi tugevdamiseks 2007.–2008. aasta ülemaailmse finantskriisi järel. Näiteks on 2017. aasta korrespondentpanganduse uuringu kohaselt enam kui 300 panga seas 92 riigis üle veerandi osalenutest vähendanud korrespondentpanganduse[171] suhteid (ingl CBR). Positiivne on, et pangad pööravad tähelepanu respondentpanga rahapesuvastasele võitluse (AML) mehhanismide efektiivsusele, tunne oma klienti ja kliendi hoolsuskohustuse täitmise (KYC/CDD) programmidele.[172] Suuremahuliste rahapesuskandaalide valguses

[168] Berg, J. „How to Combat Money Laundering in Europe. Denmark's financial regulator sees six ways to help banks identify high-risk activity." Bloomberg, 2021 - https://www.bloomberg.com/opinion/articles/2021-05-24/how-denmark-proposes-to-combat-money-laundering-in-europe (12.02.2022).
[169] Vt https://salv.com/aml-bridge-estonia/ (14.04.2022).
[170] Valitsuskomisjoni analüüs ja ettepanekud 2018, lk 35.
[171] Selgituseks, „korrespondentsuhe" on 2015.a Euroopa Liidu rahapesu direktiivi 2015/849 (AMLD IV) artikkel 3 p 8 sõnastuse kohaselt: a) pangateenuste osutamine ühe panga („korrespondentpank") poolt teisele pangale („respondentpank"); b) suhted krediidiasutuste ja finantseerimisasutuste vahel, sealhulgas sellised suhted, mille puhul korrespondentpank osutab respondentpangale sarnaseid teenuseid.
[172] World Bank. Decline in Access to Correspondent Banking Services in Emerging Markets: Trends, Impacts, and Solutions. https://openknowledge.worldbank.org/bitstream/handle/10986/29778/125422-replacement.pdf?sequence=1&isAllowed=y (16.02.2022).

pangandussüsteemis ja läbiviidud süüteomenetluste ning määratud trahvide tõttu on mõistetav, et krediidiasutused ei kiirusta sätestatud reeglitest ambitsioonikamaid samme astuma ja püüavad rangelt ettenähtud ning läbiproovitud vahendeid kasutada.

Samas on positiivne, et NRA raames läbiviidud küsitluse tulemuste kohaselt on finantssektori teadlikkus rahapesu tõkestamisest väga kõrge. Selle põhjuseks on asjaolu, et finantssektor on panganduskeskne, mida võib pidada selles osas kõige edasijõudnumaks sektoriks, kus investeeritakse automaatsetesse rahapesu ja terrorismi rahastamise tuvastamise lahendustesse, protseduurireeglitesse kui ka töötajate regulaarsesse koolitamisse.[173]

Mitmekülgset infojagamist VV ebaseadusliku kasutamise piiramiseks rõhutab Europol oma 2021. aasta vastavates soovitustes. Õiguskaitseasutused saavad ja peaksid maksimaalselt kasutama nii mitteametlikke kui ametlikke koostöökanaleid, et vahetada teavet, mis aitab tuvastada, uurida ja vastutusele võtta neid, kes kasutavad virtuaalseid varasid ebaseaduslikel eesmärkidel. See hõlmab INTERPOL-i ja Europoli pakutavaid ülemaailmseid koostöömehhanisme, nagu SIENA ja riiklike keskbüroode võrgustik (NCB), samuti mitmepoolseid kanaleid VASP-idega, mis asuvad erinevates jurisdiktsioonides. Näiteks raskete ja organiseeritud kuritegude korral peaks olema tavapärane kontrollida isikuandmeid ja krüptovaluuta tehinguid läbi Europoli, et võrrelda neid teiste menetluste andmetega.[174]

RAB-i 2022. aasta jaanuaris välja antud uuringu kohaselt laekus Riigiprokuratuurist perioodil 01.01.2019–30.08.2021 Politsei- ja Piirivalveametile (PPA) täitmiseks 126 õigusabitaotlust (ÕAT), kus seoses välisriigi õiguskaitseasutuste päringuga küsis PPA infot Eesti tegevusloaga virtuaalvääringu teenuse pakkujatelt. Kasvab järjest ka välispäringute arv, mille teiste riikide õiguskaitseasutused on teinud RABile seoses virtuaalvääringu teenuse pakkujatega. Valdavalt on 2021. aasta välispäringute sisu seotud pettuste, lunaraha, narkokuritegevuse jms tulemusena saadud varade liikumisega ja seoses virtuaalvääringu ettevõtete endi ja nendega seotud isikutega.[175]

Oluliseks rahapesuvastaseks meetmeks on info jagamine ja analüüsimine osaliste vahel nii avalikus kui erasektoris. Teavitamiskohustuse täitmise spetsiifilise vahendina võttis 2019. aastal Ühendkuningriigi rahapesu andmebüroo (UKFIU) kasutusele uued kahtlase tegevuse raporti

[173] Rahandusministeerium, NRA 2020, sektor 5, lk 8.
[174] Europol 2021. Combating virtual assetsbased money laundering and crypto-enabled crime. - https://www.europol.europa.eu/media-press/newsroom/news/thousands-gather-virtually-to-share-knowledge-of-virtual-assets-based-money-laundering-and-other-crypto-enabled-crimes (15.01.2022).
[175] Rahapesu andmebüroo. 2022, lk 21.

(*suspicious activity raport* - SAR) koodid[176], nende seas koodi "virtuaalvarad - XXVAXX". Koodide kasutamine on hoolsusmeetmete rakendamisel ja järelevalvele teavitamisel hea praktika ning need on üliolulised võimaldamaks rahapesu andmebürool ja teistel õiguskaitseasutustel teostada analüüse, et tuvastada rahapesu trende, kõrge riskiga juhtumeid ja võtta vajaduse korral viivitamatult kasutusele meetmed. Samuti võimaldavad need anda tagasisidet ettekannete esitajatele krüptovarade SARides tuvastatud trendide ja mustrite kohta.[177]

Eestis tuvastatud puudujääke selles osas ilmestab asjaolu, et ligi 75% aktiivselt tegutsevatest Eesti tegevusloaga VASP-idest (kokku 253) ei ole saatnud RABile 2021. aastal ühtki teadet kahtlaste tehingute kohta.[178]

Tuleb silmas pidada, et kohustatud isikuteks ei ole mitte ainult krediidi- ja finantsasutused, vaid RahaPTS § 2 sätestab loetelu isikutest, kelle osas nende majandus-, kutse- ja ametitegevuses seadust kohaldatakse. Need isikud peavad samuti hoolsusmeetmeid rakendama ja kahtlastest tegevustest järelevalveasutusele teada andma. Kogumis kõikide kohustatud isikute edastatud teavet analüüsides on võimalik panna paremini kokku tervikpilti VV keerukatest tehingutest.

USA õiguskaitseorganid kasutavad eelkõige FinCEN-i pakutavat teavet, mis on kogutud kohustatud isikute, teiste õiguskaitseorganite raportitest ja nendest saadud analüüsiga. FinCENi kasutuses on kaks võtmetähtsusega infoallikat, mis võivad osutuda otsustavaks digitaalvaradega seotud rahapesu või terrorikuritegude tuvastamisel. Need on: 1) kahtlase tegevuse raportid (SAR-id), mille on esitanud kohustatud finantsasutused, näiteks pangad või vahendajad tehingutes väärtpaberitega, mis on edastanud *fiat*-raha konverteerimiseks või vahetamiseks digitaalseks varaks VASP-i juures või sellega seotud ettevõttes või mis on saanud *fiat*-raha VASP-ilt või sellega seotud ettevõttelt ja 2) digitaalvarade pakkujate esitatud SAR-id. Teenusepakkujad tegutsevad sageli rahasaatjatena, võtavad vastu rahalisi vahendeid ja muudavad need digitaalvaraks või võimaldavad digitaalvara säilitamist ja/või nendega kauplemist ja vahetust. FinCEN kogub ka muud teavet, nagu välisriigi pangakonto, valuuta- ja rahainstrumendi ning valuutatehingute aruanded, mis kõik võivad sisaldada vihjeid uurimise jaoks ja tõendeid, mis on vajalikud digitaalvaradega seotud kuritegevuse tõkestamiseks ja nende eest vastutusele võtmiseks.[179]

[176] National Crime Agency. Publications. https://www.nationalcrimeagency.gov.uk/who-we-are/publications/517-glossary-codes-and-reporting-routes/file, p 9. (12.02.2022).
[177] UK. National risk assessment of money laundering and terrorist financing 2020, p 77.
[178] Rahapesu andmebüroo. 2022, lk 5.
[179] FATF Updated guidance for a risk-based approach... 2021 - https://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate) p 100. (26.02.2022).

USA föderaalsete uurimisasutuste tasemel on FBI teatanud, et luuakse uus meeskond, mis spetsialiseerub krüptovaluutadega seotud kuritegude uurimisele. Meeskond (*National Cryptocurrency Enforcement Team* - NCET) hakkab hindama, millist tüüpi krüptovaradega seotud kuriteod võivad vajada rohkem ressursse, et neid juhtumeid uurida ja menetleda. Keskendutakse krüptovahetusteenustele, segamisteenustele ja muud tüüpi digitaalvarade infrastruktuuri pakkujatele, mis võivad võimaldada krüptovaluutade kuritarvitamist.[180]

Saksamaa föderaalne kriminaalpolitsei (*Bundeskriminalamt* - BKA) on seadnud endale eesmärgiks värvata või koolitada töötajaid, kellel on asjakohased tehnilised teadmised. Tavalise kriminaalpolitsei koolituses selliseid teadmisi ei pakuta. Selle valdkonna eksperdid (nn küberkriminoloogid) peaksid ennetavalt mõtlema, kuidas tehnoloogiat saab kriminaalsel eesmärgil kasutada. Tavapärased uurimisvahendid, nagu teabe küsimine krediidiasutustelt ja teistelt kohustatud isikutelt ei ole VV detsentraliseeritud olemuse tõttu tulemusi andnud. Pangadokumentide äravõtmine või pangatöötajate tunnistajana ülekuulamine küsitlemine ei ole selles valdkonnas võimalik. Lihtsalt „raha jälje" ajamine, nagu *fiat*-raha puhul, ei pruugi eesmärki täita.[181] USA rahapesu ja terrorismi rahastamise vastase võitluse süsteemis pannakse suurt rõhku õiguskaitsealastele meetmetele. Kõigil õiguskaitseasutustel on otsene juurdepääs finantskuritegude õiguskaitse võrgustikule esitatud kahtlustäratava tegevuse teadetele. Ametite vahelise töökondade põhimõtte alusel integreeritakse kõigi tasandite ametivõimud. Seda lähenemisviisi kasutatakse laialdaselt rahapesu eeluurimistes ning see on osutunud väga edukaks olulistes, suurtes ja keerulistes juhtumites. Kehtestatud on proportsionaalseid ja hoiatavaid kriminaal-, tsiviil- ja halduskaristusi.[182]

Autori seisukoht on, et Eestis tuleks kavandada avaliku ja erasektori koostöö näiteks nn PPP (*Private-Public-Partnership*) vormis, et jagada parimaid praktikaid ja operatiivset teavet. Teabe jagamine strateegilisel tasandil – näiteks häkkimiskatsete, pettuse, rahapesu *modi operandi*, kasutatud seadmete, avastatud trendide, kahtlusaluste ja ohvrite kohta – võib aidata teenusepakkujatel ja teistel VASP-idel parandada oma tuvastamisalgoritme. See omakorda tähendab, et õiguskaitseorganid saavad paremini keskenduda kriminaalmenetlustele ning aidata kaasa mõlemal poolel ennetamise, teadlikkuse ja võimekuse suurendamisele.

[180] Yahoo. FBI „Launches New Crypto Crimes Unit“ 17.02.2022 - https://finance.yahoo.com/news/fbi-launches-crypto-crimes-unit-165525670.html (22.02.2022).
[181] Wronka, C. (2022), "Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures", Journal of Money Laundering Control, Vol. 25 No. 1, p 89.
[182] Euroopa Kontrollikoda. Eriaruanne. 2021. ELi jõupingutused pangandussektoris rahapesuga võitlemiseks on killustatud ja meetmete rakendamine on ebapiisav, IV lisa. EL ja USA - https://op.europa.eu/webpub/eca/special-reports/fight-money-laundering-13-2021/et/#chapter4 (22.02.2022).

Kokkuvõte

Rahapesu all mõistetakse traditsioonilise käsitluse järgi ebaseaduslikult saadud tulu legaliseerimist läbi finantssüsteemi ja kriminaaltulu suunamist seaduslikku majanduskäibesse. Sel viisil legaliseeritud tulu aga kahjustab majanduse normaalset toimimist. Rahapesu ja selle eelkuritegude avastamine ning tõendamine muutub kuritegude rahvusvahelise mõõtme ja virtuaalvääringute kasutuselevõtu tõttu järjest komplekssemaks ja tehnoloogiliselt keerukamaks. Seda suuremaid väljakutseid esitab areng valdkonda reguleerivatele organisatsioonidele ja riikide seadusandjatele, kes peavad rahapesuriske kiiresti maandama. Erinevate riikide riskihinnangutes on kasvava rahapesu ohu tõttu seoses virtuaalvääringute kasutamisega tõstetud riskitasemeid ja võetud kasutusele innovatiivsed tõkestusmeetmed.

Autor seadis eesmärgiks analüüsida ja välja selgitada, kas Eestis kehtiv õigus pakub ajakohaseid võimalusi virtuaalvääringute abil toime pandava rahapesu tuvastamiseks ja tõkestamiseks ning milline oleks tasakaal avaliku sektori ja eraõiguslikele isikutele pandud kohustuste vahel. Kuigi rahapesu on tõkestatud peamiselt kriminaalõiguslike meetmete kaudu, ei ole see lähenemine enam rahapesu tõkestamise esmane vahend. Eesti ja teiste riikide riskianalüüside ja uuringute põhjal virtuaalvääringute käibega seotud aktuaalsemaid rahapesuriske hinnates püüdis autor lisaks leida võimalusi efektiivseks võitluseks virtuaalvääringute abil toimepandava rahapesuga.

Selgus, et virtuaalvääringutega seotud suurimateks riskideks on finantssektoris virtuaalvääringu teenuse pakkujate loamenetluse puudujäägid ja hoolimata reeglite karmistamisest jätkuvad kahtlased ning ka välisriikide õiguskaitseasutuste tähelepanu pälvivad tehingud. Virtuaalvääringute riskid seisnevad tehingute anonüümsuses, eelkõige varade tegeliku kasusaaja poolelt ning asjaolust, et suur osa tehingutest sooritatakse ilma teenusepakkuja ja finantsvahendajata. Teenusepakkujad ei monitoori piisavalt kliendisuhet ega tehinguid ja paljudel neist puuduvad plokiahela analüütilised tööriistad ning võimekus tuvastada tumeveebi või mikseritehinguid. Samuti ei ole võimalust virtuaalvääringute tehinguid peatada, nagu saab teha *fiat*-raha puhul.

Riikliku riskihinnangu kohaselt on enam esinevaks kuriteoliigiks, mille toimepanemisega kõige rohkem kuritegelikku tulu finantssüsteemi jõuab, küberkuriteod. Küberkuritegevus on maailma mastaabis rahapesus kasutatud virtuaalvääringuid arvestades kasvanud umbes kolmandiku võrra aastas, koosnedes müügitehingutest tumeveebis või lunavara rünnakutest, mille tulu laekub enamasti virtuaalvääringutes, mitte *fiat*-valuutas. Raskem on arvestada välja seda, kui palju

vahetatakse rahapesuks näiteks traditsioonilisest uimastikaubandusest pärinevat *fiat*-raha ümber virtuaalvääringuteks. Koostööst teiste riikide õiguskaitseasutustega kogutud andmed viitavad sellele, et Eestit kasutatakse transiitriigina rahapesu protsessis välisriikidest saadetud varade kihistamise etapis. Selles etapis tehakse varaga keerulisi peitmistoiminguid ja varjatakse kuritegelikul teel saadud vahendite päritolu ning edasine integratsioonifaas toimub taas välisriigis. Enamiku rahvusvahelise koostöö juhtumite oletatav eelkuritegu oli kelmus, kolmandikul juhtudest polnud eelkuritegu teada. Oletatavalt kelmustest teenitud tulu pesemisel liikus Eesti tegevusloaga virtuaalvääringu teenuse pakkujate kaudu 140 miljonit eurot. Valdav enamus Politsei- ja Piirivalveametile saadetud õigusabitaotlustest on samuti seotud kelmustega. Aastatel 2015–2021 politsei menetluses olnud rahapesu kriminaalasjades olid 92% juhtudest eelkuriteoks kelmused, enamasti arvutikelmused.

Käesoleva töö kirjutamise ajal viimased muudatused RahaPTS-s seoses virtuaalvääringutega tehti 2022. aastal. Muudatused hõlmavad seaduse hoolsusmeetmete erisuste rakendamise osas teabe kogumise kohustust ülekande teostaja kohta (FATF-i nn „*travel rule*“) ja põhjaliku dokumentatsiooni esitamise kohustust Rahapesu Andmebüroole tegevusloa taotlemisel. Autori hinnangul seisnevad seaduse muudatuste probleemid sätestatud kohustuslike tehniliste lahenduste puudumises. Seaduses nõutavad teenuste osutamisel kasutatavad tehnoloogilised vahendid peavad hõlmama ka selliseid vahendeid, mille abil täidab ettevõtja RahaPTS §-s 25 sätestatud hoolsusmeetmeid. Regulatsiooni uudsuse tõttu puudub teave, kuidas nõutav infovahetus tehingute osapoolte ja järelevalveasutuste vahel tõhusalt toimuma hakkab. Seoses teabe kogumise kohustusega tehingu osapoolte kohta tuleb arvestada, et teistes riikides sarnaste registreerimisnõuete ja tehinguandmete kogumiseta on tõenäoline, et teenusepakkujate ebaseaduslik tegevus liigub leebema regulatsiooniga jurisdiktsioonidesse. Teadmata suuruses varalist kahju ja Eesti riigile mainekahju tekitanud virtuaalvääringute teenusepakkujate rikkumisi arvestades on aga karmistatud reeglid õigustatud.

Autori hinnangul on praegu RahaPTS-s kehtestatud virtuaalvääringuid ja teenusepakkujaid puudutav regulatsioon piisav ja tõhus vastavas valdkonnas rahapesu tõkestamiseks, kuid luua tuleks tehnoloogiliste vahendite eriregulatsioonid andmevahetuseks kõikide virtuaalvääringute käibega seotud turuosaliste vahel. Virtuaalvääringute tehingute põhine analüüs peaks toimuma infotehnoloogiliselt standardiseeritud vahenditega, millele turuosalised saavad juurdepääsu. RAB peaks olema vastutav taoliste tehniliste lahenduste standardite väljatöötamise, rakendamise ja heakskiitmise eest.

Tunne-oma-klienti (KYC) kohustused saab üle kanda virtuaalvääringute valdkonda, mida võib nimetada tunne-oma-tehingut-virtuaalselt (KYTv). Selles valdkonnas on võimalus süsteemipõhise tehingute jälgimisega uurida ülekandeid plokiahela analüüsi abil ja paljastada silmatorkavaid tehingud, mis viitavad rahapesule. Kuna kurjategijad on sellistest analüüsivahenditest teadlikud, kasutavad nad erinevaid teenuseid ja meetodeid, et muuta tehingute uurimine keeruliseks. Selliste riskide maandamiseks peaks teenusepakkujad sätestama oma riskihinnangule vastavad piirangud. Autori seisukoht on, et segamisteenuse ja muid hägustamisviise läbinud aadressid tuleb plokiahela analüüsivahenditega tuvastada. Tuvastatud seostele kriminaalsete võrkudega tuleb täita automaatselt teavitamiskohustust. Võimalus oleks läbi virtuaalvääringute teenusepakkujate teostatavates tehingutes segamisteenust läbinud või privaatsest virtuaalvara rahakotist algatatud tehingud keelata. See tähendaks tuvastatud kahtlaste aadresside nimekirjade loomist ja nende jagamist turuosaliste vahel.

Plokiahela analüüsi teel on uuritud küberkuritegevuse geograafilisi seoseid. On selgunud, et lisaks sellele, et Venemaa on näiteks *bitcoin´*ide kaevandamise mahult maailma suuruselt kolmas riik, panevad seal isikud ja rühmitused globaalses mastaabis toime ebaproportsionaalselt suure osa virtuaalvääringutega seotud kuritegevusest. Samuti on näha, et enamik väljapressitud varadest pestakse eelkõige Vene päritolu teenuseosutajate kaudu ning sealt oluline osa saadetakse samuti Venemaal asuvatele kasutajatele. Moskva finantskeskuses tegutseb mitu tosinat teenuseosutajat, mis teostavad märkimisväärses mahus rahapesu ja saavad varasid aadressidelt, mis on eranditult seotud ebaseadusliku tegevusega. Enamiku tulu päritolu on pettustest, tumeveebi turgudelt ja lunavara nõuetest. Vaatamata takistustele ebaseadusliku päritolu vara tuvastamisel on õiguskaitseorganitel virtuaalvääringutega seotud kuritegude puhul õnnestunud kriminaaltulu jälitada ja konfiskeerida. Sellised juhtumid on olulised, kuna lükkavad ümber arusaama, et virtuaalvääringuid ei saa jälitada, arestida ja need sobivad kasutamiseks kuritegelikus tegevuses. Kui küberkurjategijad teavad, et õiguskaitseorganid on võimelised virtuaalvääringuid arestima, võib see vähendada nende motivatsiooni seda tulevikus kasutada. Võimalus jälitada ja arvutada avaliku andmekogumi põhjal kokku kuritegelikku vara on suur erinevus virtuaalvääringute põhise kuritegevuse ja *fiat*-raha põhise kuritegevuse vahel.

Oluliseks rahapesuvastaseks meetmeks on info jagamine ja analüüsimine osaliste vahel nii avalikus kui erasektoris. Teavitamiskohustuse täitmise vahendina on olulised kohustatud isikute RAB-ile saadetavad kahtlase tegevuse raportid (SAR), mis võimaldavad õiguskaitseasutustel teostada analüüse, et tuvastada rahapesu trende, kõrge riskiga juhtumeid ja võtta vajaduse korral

viivitamatult kasutusele meetmed. Samuti võimaldavad need anda tagasisidet raportite esitajatele tuvastatud trendide ja mustrite kohta. Tuleb silmas pidada, et kohustatud isikuteks ei ole mitte ainult krediidi- ja finantsasutused, vaid RahaPTS § 2 sätestab loetelu isikutest, kelle osas nende majandus-, kutse- ja ametitegevuses seadust kohaldatakse. Need isikud peavad samuti hoolsusmeetmeid rakendama ja kahtlastest tegevustest järelevalveasutusele teada andma. Kogumis kõikide kohustatud isikute edastatud teavet analüüsides on võimalik panna paremini kokku tervikpilti VV keerukatest tehingutest. Laiendada tuleb avaliku ja erasektori koostööd, et jagada parimaid praktikaid ja operatiivset teavet. Teabe jagamine strateegilisel tasandil võib aidata teenusepakkujatel parandada oma kaitse- ja tuvastamisalgoritme. See omakorda tähendab, et õiguskaitseorganid saavad paremini keskenduda oma menetlustele ning aidata kaasa mõlemal poolel ennetamise, teadlikkuse ja võimekuse suurendamisele.

Autor analüüsis võimalikke muudatusi rahapesu tõkestamise nõuete rikkumise eest väärteokaristuste ning rahapesu koosseisu täitvate tegude eest kriminaalkaristuse kohaldamisel. Võttes arvesse virtuaalvääringutega seotud spetsiifilisi rahapesuriske, ei ole kavandatav haldustrahvimenetlus käsitletud valdkonnas otstarbekas ja piisab ennetava meetmena seaduses sätestatud kohustatud isiku hoolsusmeetmete rikkumise sanktsioneerimisest. Samuti ei poolda autor selles kontekstis rahapesu kuriteo eest ettenähtud karistuse karmistamist.

Eelkõige vajab lahendamist tehingute sooritajate anonüümsuse probleem ja nende võimaliku ebaseadusliku tegevusega seostamine. Tuleb tagada laiemalt virtuaalvääringute teenusepakkuja ja teiste turuosaliste hoolsuskohustuse täitmine, mis hõlmab isikute tuvastamist ja tehinguandmete edastamist järelevalve teostamiseks. Tähelepanu tuleb koondada nimetatud kohustuste täitmata jätmise tuvastamisele ja rikkumiste eest proportsionaalsete ning mõjusate sanktsioonide väljatöötamisele olemasolevate menetlusliikide raames.

Money laundering with virtual currencies and measures to prevent it. Summary

The aim of the thesis was to analyze and find out whether the law in force in Estonia offers up-to-date possibilities for identifying and preventing money laundering by means of virtual currencies, and what would be the balance between the public sector and the obligations imposed on private persons. Although money laundering has been prevented mainly through criminal law measures, this approach is no longer the primary tool for preventing money laundering.

The biggest risks related to virtual currencies are the shortcomings in the authorization procedure of virtual currency service providers in the financial sector. The risks of virtual currencies lie in the anonymity of transactions, in particular from the beneficial owner of the assets and the fact that a large part of the transactions is carried out without a service provider and a financial intermediary. Service providers do not adequately monitor customer relationships or transactions, and many of them lack blockchain analytical tools and the ability to detect dark web or mixer transactions.

According to the national risk assessment, the most common type of crime, which generates the most criminal proceeds into the financial system, is cybercrime. Cybercrime has grown by about a third a year, taking into account virtual currencies used in money laundering on a global scale, consisting of sales on the darkweb and ransomware attacks.

The data collected from cooperation with FIU authorities of other countries indicate that Estonia is used as a transit country in the money laundering process at the layering stage of assets sent from abroad. At this stage, complex concealment operations are carried out with the property and the origin of the funds obtained through crime is concealed, and the further integration phase takes place again in a foreign country. The presumed precrime of most cases was scam, in one third of cases the precrime was unknown. When laundering the income supposedly earned from scams, 140 million euros moved through Estonian licensed virtual currency service providers. The vast majority of legal aid applications sent to the Police and Border Guard Board are also related to scams. In money laundering cases investigated in period of 2015-2021, in 92% of cases the precrime was fraud, mostly computer fraud.

The problems with the amendments to the Money Laundering and Terrorist Financing Prevention Act (AMLTFA) lie in the absence of mandatory technical solutions provided for. The technological means used in the provision of services required by law must include the means by which the due diligence measures provided for in § 25 of the AMLTFA are performed. Due to

the novelty of the regulation, there is no information on how such information exchange between the parties to the transactions and the supervisory authorities will take place effectively. As regards the obligation to gather information about the parties to the transaction (travel rule), it should be taken into account that without similar registration requirements and collection of transaction data in other countries, it is likely that illegal activities will move to jurisdictions with less stringent regulation.

The regulation currently established in AMLTFA concerning virtual currencies and service providers is sufficient and effective in preventing money laundering, but special regulations of technological means should be created for the exchange of data between all market participants involved in the turnover of virtual currencies.

The analysis based on virtual currency transactions should be carried out using information technology standardised means to which market participants are given access. FIU should be responsible for the development, implementation and approval of standards for such technical solutions. In know-your-customer area, by monitoring system-based transactions, it´s possible to study transfers using blockchain analysis and expose conspicuous transactions that indicate money laundering.

Since criminals are aware of such analytical tools, they use a variety of services and methods to make it difficult to investigate transactions. In order to mitigate such risks, VASPs should set limits corresponding to their risk assessment. The author's view is that addresses that have undergone the mixing service and other forms of blurring must be identified by blockchain analysis tools. In addition, in accordance with the established links with criminal networks, the obligation to notify FIU must be automatically complied with. The possibility would be to prohibit transactions that have passed the mixing service or prohibit private virtual asset wallet transactions, that would mean creating lists of identified suspicious addresses and sharing them among market participants.

Law enforcement agencies have managed to trace and confiscate the proceeds of crime in cases involving virtual currencies. Such cases are important because they refute the notion that VCs cannot be traced, seized and they are suitable for use in criminal activities. If cybercriminals know that law enforcement agencies are capable of seizing virtual currencies, this can reduce their motivation to use it in the future. The ability to track and calculate criminal assets based on a public dataset is a big difference between virtual currency-based crime and fiat money-based crime.

An important anti-money laundering measure is the sharing and analysis of information between participants in both the public and private sectors. Suspicious activity reports (SAR) sent to the FIU by obligated persons are important as a means of fulfilling the notification obligation, which allow law enforcement authorities to carry out analyses in order to identify trends in money laundering, high-risk cases and, if necessary, to take immediate measures. They also allow feedback to be given on the trends and patterns identified by the authors of the reports. It should be borne in mind that the obligated persons by law are not only credit and financial institutions.

Public-private cooperation (PPP) needs to be expanded to share best practices and operational information. Sharing information at a strategic level can help service providers improve their protection- and detection algorithms. This in turn means that law enforcement agencies can better focus on their procedures and contribute to prevention, awareness and capacity building on both sides.

Taking into account the money laundering risks related to virtual currencies, the planned administrative fine procedure is not expedient, and it is sufficient to sanction the violation of the due diligence measures of an obligated person. The performance of the service provider's due diligence must be ensured, which includes the identification of persons, the transmission of transaction data for the performance of supervision. Attention must be focused on developing proportionate and effective sanctions for infringements within the framework of existing types of procedures.

Kasutatud kirjandus ja allikad

Kirjandus

1. Basel Institute on Governance. Basel AML Index 10th public edition 2021 - https://baselgovernance.org/basel-aml-index

2. Berg, J. How to Combat Money Laundering in Europe. Denmark's financial regulator sees six ways to help banks identify high-risk activity. Bloomberg, (2021) - https://www.bloomberg.com/opinion/articles/2021-05-24/how-denmark-proposes-to-combat-money-laundering-in-europe

3. Brown, C. Dividing Your Deposits Is a Federal Crime. Tennessee Bar Journal (2011). Vol. 47, No. 10 - https://www.tba.org/?pg=Articles&blAction=showEntry&blogEntry=9664

4. Bryans, D. (2014). Bitcoin and Money Laundering: Mining for an Effective Solution. Indiana Law Journal. Vol. 89 -- https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=11100&context=ilj

5. CipherTrace. Geographic Risk Report: VASP KYC by Jurisdiction - https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/

6. Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198). – https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/198

7. Crypto Crackdown: OFAC Sanctions SUEX Cryptocurrency Exchange, 2021 - https://www.jdsupra.com/legalnews/crypto-crackdown-ofac-sanctions-suex-3337719/

8. Durrieu, R. Rethinking Money Laundering & Financing of Terrorism in International Law: Towards a New Global Legal Order. Leiden, Boston, 2013. ProQuest Ebook Central - https://ebookcentral-proquest-com.ezproxy.utlib.ut.ee/lib/tartu-ebooks/detail.action?docID=1204118

9. EBA analysis of RegTech in the EU financial sector (2021) - https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1015484/EBA%20analysis%20of%20RegTech%20in%20the%20EU%20financial%20sector.pdf

10. Eesti Pank. Finantsstabiilsuse ülevaade 1/2018. Tallinn – https://www.eestipank.ee/publikatsioon/finantsstabiilsuse-ulevaade/2018/finantsstabiilsuse-ulevaade-12018

11. Eesti Pank. Finantsstabiilsuse ülevaade, 2/2021 - https://www.eestipank.ee/publikatsioonid/finantsstabiilsuse-ulevaade

12. Egmont Group Bulletin, Professional Money Laundering Facilitators, 2019 - https://egmontgroup.org/wp-content/uploads/2021/09/2019_Egmont_Group_Bulletin_Professional_Money_Laundering_Facilitators.pdf

13. Egmont Group. Money Laundering and the Financing of Terrorism. – https://egmontgroup.org/en/content/money-laundering-and-financing-terrorism

14. Euroopa Keskpank. - https://www.bankingsupervision.europa.eu/about/ssmexplained/html/fintech.et.html

15. Euroopa Komisjon. (2020) Ettepanek: Euroopa Parlamendi ja Nõukogu määrus, mis käsitleb krüptovaraturge ja millega muudetakse direktiivi (EL) 2019/193, COM(2020) 593 final

16. Euroopa Komisjon. Komisjoni aruanne Euroopa Parlamendile ja Nõukogule siseturgu mõjutavate ja piiriülese tegevusega seotud rahapesu ja terrorismi rahastamise riskide hindamise kohta. (2019) - https://m.riigikogu.ee/tegevus/dokumendiregister/dokument/febd712d-1712-461f-b716-7ec8660a3dda/

17. Euroopa Kontrollikoda. Eriaruanne. 2021. ELi jõupingutused pangandussektoris rahapesuga võitlemiseks on killustatud ja meetmete rakendamine on ebapiisav, IV lisa. EL ja USA - https://op.europa.eu/webpub/eca/special-reports/fight-money-laundering-13-2021/et/#chapter4

18. Euroopa Parlament, 2021 - https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_ET.html

19. European Banking Authority (2021) - https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20ML-TF%20risk%20factors%20%28revised%29%202021-02/Translations/1016926/Guidelines%20ML%20TF%20Risk%20Factors_ET.pdf

20. Europol 2021. Combating virtual assetsbased money laundering and crypto-enabled crime. - https://www.europol.europa.eu/media-press/newsroom/news/thousands-gather-virtually-to-share-knowledge-of-virtual-assets-based-money-laundering-and-other-crypto-enabled-crimes

21. FATF (2021), Second 12-month Review Virtual Assets and VASPs, FATF, Paris, France - https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf

22. FATF Recommendations (2012). Mitteametlik tõlge eesti keelde: Rahapesu ning terrorismi ja massihävitusrelvade leviku rahastamise vastu võitlemise rahvusvahelised standardid. FATF-i soovitused (2012). – http://www.fatf-

gafi.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Estonian.pdf

23. FATF Recommendations, Interpretative note to recommendation 3; Glossary – https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

24. FATF Report. (2014). - https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

25. FATF (2021), Updated guidance for a risk-based approach. - https://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate)

26. Feldmanis, L., Ploom, T. Rahapesu kriminaliseerimine: kelle suhtes ja millise põhjendusega. – Juridica 2007/3 https://www.juridica.ee/article_full.php?uri=2007_3_rahapesu_kriminaliseerimine_kelle_suhtes_ja_millise_p_hjendusega_&pdf=1

27. Financial Crimes Enforcement Network U.S. Department of the Treasury. Anti-Money Laundering and Countering the Financing of Terrorism National Priorities (2021) - https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf

28. Finantsinspektsioon, blogi 13. jaanuar 2022, https://www.fi.ee/et/blogi/hambutud-hammustused-karistuspoliitikas

29. Finantsinspektsioon, uudised. (2020) – https://fi.ee/et/uudised/swedbank-saab-trahvi-ja-ettekirjutuse-rahapesu-vastu-voitlemise-reeglite-rikkumise-eest

30. Finantsstabiilsuse ülevaade 1/2018. Tallinn: Eesti Pank 2018 – https://www.eestipank.ee/publikatsioon/finantsstabiilsuse-ulevaade/2018/finantsstabiilsuse-ulevaade-12018

31. Frechtling, D. (2017), "Recognising and thwarting transaction and payment laundering", Journal of Payments Strategy and Systems, Vol. 11 (2) - https://hstalks.com/article/2159/recognising-and-thwarting-transaction-and-payment-/

32. Freeman Law (2021) - https://freemanlaw.com/what-is-a-tumbler-and-is-cryptocurrency-tumbling-safe/

33. Grauer, K. Updegrave, H. (2021), "The 2021 crypto crime report" - https://go.chainalysis.com/2021-Crypto-Crime-Report.html

34. Haldustrahvimenetluse seaduse eelnõu. Eelnõude infosüsteem - https://eelnoud.valitsus.ee/main/mount/docList/e0350345-d819-4adc-bc56-37594d5f815f#d0lnNhIx

35. HM Treasury, Home Office. National risk assessment of money laundering and terrorist financing. (2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf

36. International Monetary Fund. – https://www.imf.org/en/About/Factsheets/A-Guide-to-Committees-Groups-and-Clubs#G10

37. Jullum, M., Løland, A., Huseby, R., Ånonsen, G. and Lorentzen, J. (2020), "Detecting money laundering transactions with machine learning", Journal of Money Laundering Control, Vol. 23 No. 1 - https://www.researchgate.net/publication/338726110_Detecting_money_laundering_transactions_with_machine_learning

38. Juntunen, J. and Teittinen, H. (2022), "Accountability in anti-money laundering – findings from the banking sector in Finland", Journal of Money Laundering Control, Vol. ahead-of-print No. ahead-of-print. - https://doi.org/10.1108/JMLC-12-2021-0140

39. Justiitsministeerium. Haldustrahvimenetluse seadus saadeti kooskõlastusringile - https://www.just.ee/uudised/haldustrahvimenetluse-seadus-saadeti-kooskolastusringile

40. Kairjak, M. Karistus- ja haldusõiguse piiride hägustumine Euroopa Liidu finantsturgude õiguse uues sanktsioonisüsteemis. Juridica V/2015 - https://www.juridica.ee/article_full.php?uri=2015_5_karistus-_ja_haldus_iguse_piiride_h_gustumine_euroopa_liidu_finantsturgude_iguse_uues_sanktsi&pdf=1

41. Karistusseadustik. Komm vlj. 5 vlj. Tallinn: Juura 2021. https://karistusseadustik.juuraveeb.ee/

42. Kärner, M. Direktiiv (EL) 2018/1673 rahapesu vastu võitlemise kohta kriminaalõiguse abil. – Juridica 2019/7, lk 520 - https://www.juridica.ee/article_full.php?uri=2019_7_direktiiv_el_2018_1673_rahapesu_vastu_v_itlemise_kohta_kriminaal_iguse_abil&pdf=1

43. Liechtenstein Legal Gazette. The Tokens and TT Service Provider Act (2021) - https://www.regierung.li/files/medienarchiv/950-6-01-09-2021-en.pdf

44. Morgan, S. (2021), "Cybercrime to cost the world $10.5 trillion annually by 2025" - https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

45. Mäeker, M., Nõmm, A. (2020). Pangasaladuse hoidjast politseinikuks: valikud rahapesu tõkestamisel. Juridica, 8, lk 664 - https://www.juridica.ee/article_full.php?uri=2020_8_pangasaladuse_hoidjast_politseinikuks_valikud_rahapesu_t_kestamisel&pdf=1

46. National Crime Agency. Publications. (2020)https://www.nationalcrimeagency.gov.uk/who-we-are/publications/517-glossary-codes-and-reporting-routes/file

47. Nizovtsev, Y.Y., Parfylo, O.A., Barabash, O.O., Kyrenko, S.G., Smetanina, N.V. (2021), "Mechanisms of money laundering obtained from cybercrime: the legal aspect", Journal of Money Laundering Control - https://doi.org/10.1108/JMLC-02-2021-0015

48. Oengo, O. F. Virtuaalvääringu teenuse regulatiivsed eripärad, senine areng ja perspektiiv. – Juridica 2020/8 https://www.juridica.ee/article_full.php?uri=2020_8_virtuaalv_ringu_teenuse_regulatiivsed_erip_rad_senine_areng_ja_perspektiiv&pdf=1

49. OFAC Sanctions Hydra Following Law Enforcement Shutdown of the Darknet Market, As Well As Russian Exchange Garantex (2022) - https://blog.chainalysis.com/reports/hydra-garantex-ofac-sanctions-russia/

50. Preller, F. (2008), Comparing AML legislation of the UK, Switzerland and Germany, Journal of Money Laun-dering Control, Vol. 11 No. 3 https://www.emerald.com/insight/content/doi/10.1108/13685200810889380/full/html

51. Prokuratuuri aastaraamat 2021. Rahvusvahelise küberkuritegevuse tõkestamise väljakutsetest tõendite kogumisel (2022) - https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2021/rahvusvahelise-kuberkuritegevuse-tokestamise-valjakutsetest

52. Raamatupidamise Toimkond. 2018. - https://www.rmp.ee/raamatupidamine/raamatupidamine-yldiselt/plokiahela-tehnoloogial-pohinevate-instrumentide-kajastamine-2018-09-11

53. Rahandusministeerium (2018). Rahapesu ja terrorismi rahastamise tõkestamise valitsuskomisjoni analüüs ja ettepanekud. - https://www.rahandusministeerium.ee/sites/default/files/rahapesu_tokestamise_valitsuskomisjoni_analuus_ja_ettepanekud.pdf

54. Rahandusministeerium, Eesti rahapesu ja terrorismi rahastamise siseriiklik riskihinnang 2021. – https://www.fin.ee/finantspoliitika-valissuhted/rahapesu-ja-terrorismi-rahastamise-tokestamine/riskihinnangud

55. Rahandusministeerium. Krüptovarade reguleerimise väljatöötamiskavatus (sic!). *Sine loco*, november 2019. – https://www.rahandusministeerium.ee/sites/default/files/news-relatedfiles/kruptovarade_reguleerimise_vtk.pdf

56. Rahapesu andmebüroo (RAB 2020), Virtuaalvääringu teenuse pakkuja uuring. - https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b

57. Rahapesu andmebüroo. Aastaraamatud. (2017-2018) - https://fiu.ee/aastaraamatud-ja-uuringud/aastaraamatud#item-4

58. Rahapesu Andmebüroo. Garantex Europe OÜ kaotas õiguse pakkuda virtuaalvääringutega seotud teenuseid. (2022) - https://fiu.ee/uudised/garantex-europe-ou-kaotas-oiguse-pakkuda-virtuaalvaaringutega-seotud-teenuseid

59. Rahapesu Andmebüroo. Virtuaalvääringu teenuse pakkujatega seonduvad riskid Eestis. (2022) - https://www.fiu.ee/aastaraamatud-ja-uuringud/uuringud

60. Rahapesu Andmebüroo. Rahapesu Andmebüroo väliskoostöö ülevaade 2021. (2022) - https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#virtuaalvringu-tee

61. Rahapesu ja terrorismi rahastamise tõkestamise seaduse ja teiste seaduste muutmise seaduse eelnõu 507 SE - https://www.riigikogu.ee/tegevus/eelnoud/eelnou/ffe848a6-7b78-43cf-b106-720915882205/Rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20seaduse%20ja%20teiste%20seaduste%20muutmise%20seaduse%20eeln%C3%B5u%20(507%20SE%20I)

62. Rahapesu ja terrorismi rahastamise tõkestamise valitsuskomisjoni analüüs ja ettepanekud (2018) - https://www.rahandusministeerium.ee/sites/default/files/rahapesu_tokestamise_valitsuskomisjoni_analuus_ja_ettepanekud.pdf

63. Reuters. „China bans financial, payment institutions from cryptocurrency business.“ (2021) - www.reuters.com/technology/chinese-financial-payment-bodies-barred-cryptocurrency-business- 2021-05-18/

64. Reuters. „Russia proposes ban on use and mining of cryptocurrencies.“ (2022) - https://www.reuters.com/business/finance/russian-cbank-proposes-banning-cryptocurrencies-crypto-mining-2022-01-20/

65. Riigikogu. Komisjoni aruanne Euroopa Parlamendile ja Nõukogule siseturgu mõjutavate ja piiriülese tegevusega seotud rahapesu ja terrorismi rahastamise riskide hindamise kohta. (2019) - https://m.riigikogu.ee/tegevus/dokumendiregister/dokument/febd712d-1712-461f-b716-7ec8660a3dda/

66. Riigikogu. Seletuskiri audiitortegevuse seaduse, finantskriisi ennetamise ja lahendamise seaduse ning teiste seaduste muutmise seaduse (finantsvaldkonna väärteokaristuste reform, EL-i õigusest tulenevad karistused, vara legaalse päritolu pööratud tõendamiskoormus) eelnõu juurde (771 SE seletuskiri, 2018) - https://www.riigikogu.ee/tegevus/eelnoud/eelnou/789782cb-80df-4e9e-9bcb-a09b5b318755/Audiitortegevuse%20seaduse,%20finantskriisi%20ennetamise%20ja%20lahendamise%20seaduse%20ning%20teiste%20seaduste%20muutmise%20seadus%20(finantsvaldkonna%20v%C3%A4%C3%A4rteokaristuste%20reform,%20EL-

i%20%C3%B5igusest%20tulenevad%20karistused,%20vara%20legaalse%20p%C3%A4ritolu%20p%C3%B6%C3%B6ratud%20t%C3%B5endamiskoormus)

67. Riigiprokuratuur. (2018) – https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2018/2018-riigiprokuratuuri-suudistusosakonnas

68. Rosin, K. Euroopa Liidu kriminaalõiguse areng Lissaboni leppe jõustumise järel. – Juridica 2015/IX - https://www.juridica.ee/article_full.php?uri=2015_9_euroopa_liidu_kriminaal_iguse_areng_lissaboni_leppe_j_ustumise_j_rel&pdf=1

69. Ruiz, E. P., Angelis, J. (2021) Combating money laundering with machine learning – applicability of supervised-learning algorithms at cryptocurrency exchanges. - https://www.emerald.com/insight/content/doi/10.1108/JMLC-09-2021-0106/full/pdf?title=combating-money-laundering-with-machine-learning-applicability-of-supervised-learning-algorithms-at-cryptocurrency-exchanges

70. Schwarz, N., Chen. K., Poh. K., Jackson, G., Kao. K., Fernando. F., Markevych, M. (2021) Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1) Some Legal and Practical Considerations - https://www.imf.org/en/Publications/fintech-notes/Issues/2021/10/14/Virtual-Assets-and-Anti-Money-Laundering-and-Combating-the-Financing-of-Terrorism-1-463654

71. Seletuskiri ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu juurde - https://eelnoud.valitsus.ee/main/mount/docList/a41d0022-7752-4009-9a08-1b97fc44be64#4NwfcK7w

72. SOCTA 2021 - https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf

73. Soo, A., Lott, A., Kangur, A. Võimalused Euroopa Liidu halduskaristuste ülevõtmiseks Eestis. Juridica 4/2020 - https://www.juridica.ee/article_full.php?uri=2020_4_v_imalused_euroopa_liidu_halduskaristuste_lev_tmiseks_eestis&pdf=1

74. Sootak J. Karistusõigus. Üldosa. (2018) - https://karistusoigus-yldosa.juuraveeb.ee/sisukord

75. Stessens, G. Money laundering: a new international law enforcement model. Cambridge: University Press 2000 - https://ebookcentral-proquest-com.ezproxy.utlib.ut.ee/lib/tartu-ebooks/detail.action?docID=144722

76. SWI swissinfo. „Swiss ‘Crypto Valley’ boasts 14 'unicorns'“ (2022) - https://www.swissinfo.ch/eng/swiss--crypto-valley--boasts-14--unicorns-/47291870

77. Swiss National Risk Assessment (NRA): Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding - https://www.sif.admin.ch

78. Teicmann, F. M. J.; Falker, M.-C. (2020) Money laundering via cryptocurrencies – potential solutions from Liechtenstein - https://www.emerald.com/insight/1368-5201.htm

79. The Chainalysis 2022 Crypto Crime Report - https://go.chainalysis.com/2022-crypto-crime-report.html

80. Tibar I. KarS § 394/1.5 – Karistusseadustik. Komm vlj. 5. vlj. (2021) - https://karistusseadustik.juuraveeb.ee/

81. Tibar, I. Rahapesu kujunemisloost ja olemusest. – Juridica 2007/7 - https://www.juridica.ee/article_full.php?uri=2007_8_rahapesu_kujunemisloost_ja_olemusest&pdf=1

82. Tibar, I. Tähelepanekuid uue rahapesu ja terrorismi rahastamise tõkestamise seaduse jõustumisega seoses. – Juridica 2018/1 - https://www.juridica.ee/article_full.php?uri=2018_1_t_helepanekuid_uue_rahapesu_ja_terrorismi_rahastamise_t_kestamise_seaduse_j_ustumisega_seoses&pdf=1

83. TITANIUM: Tools for the Investigation of Transactions in Underground Markets (2020) - https://www.titanium-project.eu/

84. Council of Europe. Recommendation No (80) 10 of the Commitee of Ministers to Member States on Measures Against the Transfer and the Safekeeping of Funds of Criminal Origin, 1980. – http://www.coe.int/t/dghl/monitoring/moneyval/Instruments/Rec%2880%2910_en.pdf

85. Truu, M. Pilk karistusõiguse lähtele: määratletuse põhimõttest süüteokoosseisu sõnastamisel ja tõlgendamisel. – Juridica 2019/9 - https://www.juridica.ee/article_full.php?uri=2019_9_pilk_karistus_iguse_l_htele_m_ratletuse_p_him_ttest_s_teokoosseisu_s_nastamisel_ja_t_lgendami&pdf=1

86. United States District Court for the Southern District of Florida (1982), "United States of America v. Four million two hundred and fifty-five thousand, six hundred and twenty-five dollars and thirty-nine cents" - https://law.justia.com/cases/federal/district-courts/FSupp/551/314/2366254/

87. UK. National risk assessment of money laundering and terrorist financing (2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf

88. Veebel, V. Kas Läänemere-äärne rahu on saavutatav regionaalsete pingutustega? Diplomaatia. 2018. https://diplomaatia.ee/kas-laanemere-aarne-rahu-on-saavutatav-regionaalsete-pingutustega

89. Vabariigi Valitsuse 2019- 2023.a tegevusprogramm. *Sine loco*, 2019. – https://www.valitsus.ee/et/eesmargid-ja-tegevused

90. Vedler, S. „Eesti finantssüsteemi ähvardab halli nimekirja kukkumine. Oht tuleb krüptoärist“. — Eesti Ekspress 09.02.2022

91. Wegberg, R., Oerlemans, J.-J., Deventer, O. (2018). Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. Journal of Financial Crime - https://www.emerald.com/insight/content/doi/10.1108/JFC-11-2016-0067/full/html

92. Wronka, C. (2021) - Anti-money laundering regimes: a comparison between Germany, Switzerland and the UK with a focus on the crypto business - https://doi.org/10.1108/JMLC-06-2021-0060

93. Wronka, C. (2021), "“Cyber-laundering”: the change of money laundering in the digital age", Journal of Money Laundering Control - https://doi.org/10.1108/JMLC-04-2021-0035

94. Wronka, C. (2022), "Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures", Journal of Money Laundering Control, Vol. 25 No. 1 - https://doi.org/10.1108/JMLC-02-2021-0017

95. Õiguskantsler. Arvamus haldustrahvimenetluse seaduse eelnõu kohta (2020) - https://www.oiguskantsler.ee/et/seisukohad/seisukoht/arvamus-haldustrahvimenetluse-seaduse-eeln%C3%B5u-kohta

96. Ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu - https://eelnoud.valitsus.ee/main/mount/docList/a41d0022-7752-4009-9a08-1b97fc44be64#JqPC82Xu

97. World Bank. Decline in Access to Correspondent Banking Services in Emerging Markets: Trends, Impacts, and Solutions. https://openknowledge.worldbank.org/bitstream/handle/10986/29778/125422-replacement.pdf?sequence=1&isAllowed=y

98. Yahoo. „FBI Launches New Crypto Crimes Unit“. (2022) - https://finance.yahoo.com/news/fbi-launches-crypto-crimes-unit-165525670.html

Kasutatud õigusaktid

99. Euroopa Liidu toimimise leping (konsolideeritud versioon). – ELT C 326, 26.10.2012.

100. Euroopa Nõukogu direktiiv, 10. juuni 1991, rahandussüsteemi rahapesu eesmärgil kasutamise vältimise kohta (91/308/EMÜ). – EÜT L 166, 28.06.1991, lk 77–83.

101. Euroopa Nõukogu rahapesu ning kriminaaltulu avastamise, arestimise ja konfiskeerimise konventsiooni ratifitseerimise seadus. 01.06.2002. – RT II 2000, 7, 41.

102. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/849, 20. mai 2015, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist ning millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 648/2012 ja tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2005/60/EÜ ja komisjoni direktiiv 2006/70/EÜ. – ELT L 141, 05.06.2015, lk 73-117.

103. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2018/1673, 23.oktoober.2018, rahapesu vastu võitlemise kohta kriminaalõiguse abil. – ELT L 284, 12.11.2018, lk 22-30.

104. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2018/843, 30. mai 2018, millega muudetakse direktiivi (EL) 2015/849, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist, ning millega muudetakse direktiive 2009/138/EÜ ja 2013/36/EL. – ELT L 156, 19.06.2018, lk 43–74.

105. Euroopa Parlamendi ja nõukogu direktiiv 2001/97/EÜ, millega muudetakse nõukogu direktiivi 91/308/EMÜ rahandussüsteemi rahapesu eesmärgil kasutamise vältimise kohta. – EÜT L 344, 28.12.2001, lk 76–82.

106. Euroopa Parlamendi ja nõukogu direktiiv 2005/60/EÜ, 26. oktoober 2005, rahandussüsteemi rahapesu ja terrorismi rahastamise eesmärgil kasutamise vältimise kohta. – ELT L 309, 25.11.2005, lk 15–36.

107. Karistusseadustik. – RT I, 21.05.2021, 9.

108. Krediidiasutuste seadus - RT I, 07.12.2021, 13.

109. Kriminaalkoodeks - RT 1992, 20, 288.

110. Lissaboni leping, millega muudetakse Euroopa Liidu lepingut ja Euroopa Ühenduse asutamislepingut. - ELT C 306, 17.12.2007.

111. Majandustegevuse seadustiku üldosa seaduse ning korrakaitseseaduse muutmise ja rakendamise seaduse muutmise seadus - RT I, 29.06.2014, 1.

112. Makseasutuste ja e-raha asutuste seadus - RT I, 10.07.2020, 21.

113. Narkootiliste ja psühhotroopsete ainete ebaseadusliku ringluse vastane Ühinenud Rahvaste Organisatsiooni konventsioon – RT II 2000 15, 92.

114. Rahapesu ja terrorismi rahastamise tõkestamise seadus – RT I, 12.03.2022, 19.

115. Rahvusvahelise organiseeritud kuritegevuse vastu võitlemise Ühinenud Rahvaste Organisatsiooni konventsioon - RT II 2003, 1, 1.

116. Tulumaksuseadus - RT I, 05.04.2022, 5

117. Ühinenud Rahvaste Organisatsiooni korruptsioonivastane konventsioon. – RT II 2010, 4, 10.

Kasutatud kohtupraktika

RKHKo 3-3-1-75-15

RKKK 3-1-1-34-05

RKKKm 1-17-5176

TlnRnKo, 1-12-12477/74