TARTU ÜLIKOOL

ÕIGUSTEADUSKOND

Eraõiguse osakond

Ketriin Laumets

RAHAPESU JA TERRORISMI RAHASTAMISE RISKIDE MAANDAMINE VIRTUAALVÄÄRINGU TEENUSTE PAKKUMISEL

Magistritöö

Juhendaja: *mag.iur*. Ethel Pagil

Kaasjuhendaja: Prof. Irene Kull

Tartu

2023

SISUKORD

SISSEJUHATUS

Virtuaalvääring on defineeritud rahapesu ja terrorismi rahastamise tõkestamise seaduses[1] (RahaPTS) kui 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. Erinevalt teistest finantsinstrumentidest on virtuaalvääringud üksnes digitaalsed ehk neil ei ole füüsilist vormi nagu paberrahal või müntidel ning neid ei ole väljastanud emiteerimise õigust omavad keskpangad, krediidiasutused ega e-raha asutused. Virtuaalvääringuid saab eristada lähtuvalt nende emiteerijast, tehnoloogilisest ülesehitusest ja kasutusvõimalustest. Viimase puhul saab virtuaalvääringud jaotada kolmeks: 1) virtuaalvääringud, mida kasutatakse kaupade ja teenuste eest maksmiseks; 2) virtuaalvääringud, mida kasutatakse investeerimise eesmärgil läbi väärtuse säilitamise või suurendamise; 3) virtuaalvääringud, mis annavad juurdepääsu toodetele ja teenustele.[2] Kuigi virtuaalvääringutega tehtavad tehingud on kiiremad, odavamad ja turvalisemad, on nendega kaasnenud ka pahupool. Virtuaalvääringutest on saanud atraktiivsed rahapesu ja terrorismi rahastamise vahendid. Euroopa Komisjoni riikideülese riskihinnangu[3] kohaselt on Euroopa Liidus virtuaalvääringutega seotud rahapesu ja terrorismi rahastamise risk väga kõrge, kuna virtuaalvääringu tehingute puhul on keeruline tuvastada tehingute osapooli ning tehingus liikunud vara päritolu.

Rahapesu eesmärk on kaotada näiliselt seos kuriteo ja selle tulemusena saadud vara vahel, tehes seda erinevate manipulatsioonide, näiteks vara üleandmise, vahetamise või varjamise kaudu, ning seejärel suunata vara legaalsesse majanduskäibesse.[4] Klassikaliselt jaguneb rahapesu kolmeks etapiks: paigutamine, kihistamine ja integreerimine.[5] Rahapesu virtuaalvääringute abil võib toimuda järgnevalt. Esimeses ehk paigutamise etapis suunatakse eelkuriteo toimepanemisel saadud vara finantssüsteemi. Teisisõnu, kuritegelikust tegevusest saadud vara, sealhulgas väljapressimise, omastamise või kelmuse teel saadud raha paigutatakse näiteks virtuaalvääringu teenuse platvormile, kus raha on võimalik vahetada virtuaalvääringuks. Teises etapis püütakse

[1] Rahapesu ja terrorismi rahastamise tõkestamise seadus. – RT I, 10.02.2023, 29.
[2] Allen, J. G., Lastra, R. M. Virtual currencies in the Eurosystem: challenges ahead. (2018, lk 9) – https://www.europarl.europa.eu/cmsdata/150541/DIW_FINAL%20publication.pdf (03.03.2023).
[3] Euroopa Komisjon. Supra-National Risk Assessment (SNRA). (2022, lk 101) – https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0344&from=EN (02.02.2023).
[4] Tibar, I. KarS § 394/6. – Karistusseadustik. Komm vlj. 5. vlj. Tallinn: Juura 2021.
[5] Mbiyavanga, S. Cryptolaundering: Anti-Money Laundering Regulation of Virtual Currency Exchanges. – Journal of Anti-Corruption Law 2019/3, No 1, lk 6.

kriminaaltulu päritolu varjata erinevate kihistamise võtete abil. Selleks liigutatakse kriminaaltulu erinevate riikide ja finantsasutuste vahel. Samuti kasutatakse kihistamist hõlbustavaid tehnilisi lahendusi, näiteks virtuaalvääringute segamisteenust[6]. Kolmandas ehk integreerimise etapis luuakse kriminaaltulule näiliselt seaduslik päritolu. Selleks vahetatakse virtuaalvääringud raha vastu või soetatakse virtuaalvääringute eest näiteks kinnisvara, mootorsõidukeid või muud luksuskaupa.

Virtuaalvääringud on kasutusele võetud ka terrorismi rahastamisel. RahaPTS-i järgi hõlmab terrorismi rahastamine terrorikuriteo ja selle toimepanemisele suunatud tegevuse ning terroristlikul eesmärgil reisimise rahastamist ning toetamist karistusseadustiku[7] (KarS) §-de 237^3 ja 237^6 tähenduses. Erinevalt rahapesust ei pea terrorismi rahastamiseks kasutatud vara olema saadud kuriteo tulemusel. Teisisõnu, terrorismi rahastamisel võib vara pärineda nii seaduslikust kui ka ebaseaduslikust allikast. Sarnaselt rahapesule on ka terrorismi rahastamisel välja kujunenud kolm etappi: kogumine, edastamine ja kasutamine.[8] Esimeses etapis kogutakse terrorismi toetamiseks vahendeid. Rahalisi vahendeid saab koguda nii legaalsel teel, näiteks töötasu saamisega, või illegaalsel teel, näiteks narkootilise aine käitlemisega. Teises etapis edastatakse saadud vahendid läbi mitme kanali terrorismi võrgustikku. Selles etapis toimub ebaseaduslikult saadud varaga rahapesu. Viimases etapis kasutatakse saadud vahendeid terrorismi toetamiseks, näiteks soetatakse terrorirünnaku jaoks virtuaalvääringute eest relvi.

Lisaks sellele, et virtuaalvääringu tehingutega seonduvat kõrget riski on täheldatud Euroopa tasandil, on ka Eestis virtuaalvääringuga seonduv kõrgendatud tähelepanu all. Nimelt oli aastal 2017 Eesti üks esimestest Euroopa riikidest, kus kehtestati virtuaalvääringu teenuse pakkumisele tegevusloakohustus. Virtuaalvääringu teenuse pakkuja (ingl k *virtual asset service provider*, edaspidi VASP) tegevusloa regulatsioon ei täitnud aga rahapesu ja terrorismi rahastamise riskide maandamise eesmärki. Tegevusloa said ka ettevõtted, kes Eestis ei tegutsenud ning kelle üle ei olnud Rahapesu Andmebürool (edaspidi RAB) võimalik järelevalvet teostada. Puudusi regulatsioonis ilmestab ka tegevuslubade hüppeline kasv. Kui aastal 2017 väljastati 6 tegevusluba, siis 2018. aastal kordades rohkem ehk 1137 tegevusluba. Samal ajal puudusid RahaPTS-is seaduslikud alused kõrget rahapesu ja terrorismi rahastamise riski kandvate VASPide tegevusloa

[6] Segamisteenuse kohta vaata lähemalt peatükki 1.2.
[7] Karistusseadustik. – RT I, 06.01.2023, 4.
[8] Financial Action Task Force. Terrorist Financing Risk Assessment Guidance. (2019, lk 29) – https://www.fatf-gafi.org/en/publications/Methodsandtrends/Terrorist-financing-risk-assessment-guidance.html (16.02.2023).

kehtetuks tunnistamiseks.[9] Riskide maandamiseks ning Eesti mainekahju vältimiseks karmistati 2020. aastal VASPi tegevusloa tingimusi ja neile kohalduvaid nõudeid. Kuna need ei osutunud piisavaks, et maandada kõrget rahapesu ja terrorismi rahastamise riski VASPide sektoris, täiendati 2022. aastal VASPidele kohalduvaid nõudeid veelgi.[10]

Hoolimata korduvast seaduse karmistamisest, on selge, et Eestis jätkub virtuaalvääringutega seonduvate riskide realiseerumine. Näiteks 2022. aasta novembris vahistati Tallinnas Eesti ettevõtjad, keda kahtlustatakse virtuaalvääringute kelmuses ja rahapesus. Tekitatud kahju küündib 575 miljoni dollarini.[11] Samuti on RABi 2022 aasta aastaraamatus[12] välja toodud virtuaalvääringu teenuse pakkujate (edaspidi VASP) sektori jätkuv kõrge rahapesu ja terrorismi rahastamise risk ning tuvastanud puudusi VASPide rahapesu ja terrorismi rahastamise tõkestamise eesmärki täitvate kohustuste täitmisel. Seega on aktuaalne uurida VASPide sektoris esinevaid rahapesu ja terrorismi rahastamise riske ning nende maandamisvõimalusi.

Eelnevast tulenevalt on magistritöö eesmärk välja selgitada, millises ulatuses täidavad kehtivad rahapesu ja terrorismi rahastamise tõkestamisele suunatud meetmed eesmärki maandada virtuaalvääringute teenuse pakkumisega seotud rahapesu ja terrorismi rahastamise riske ja pakkuda lahendusi, mis võimaldaks ilmnenud puudusi vähendada.

Magistritöö on jaotatud kolmeks peatükiks. Kasutades deduktiivset uurimismeetodit, kaardistatakse esimeses peatükis esmalt virtuaalvääringutega seotud peamised rahapesu ja terrorismi rahastamise riskitegurid. Seejärel käsitletakse järgnevates alapeatükkides iga riskitegurit eraldi ning selgitatakse välja, kas riskiteguritest tulenevad rahapesu ja terrorismi rahastamise riskid on kehtivas RahaPTS-is sätestatud meetmetega maandatud.

Teises peatükis käsitletakse VASPidele kehtestatud kohustuste täitmist rahapesu ja terrorismi rahastamise riski maandamisel. Nii RABi uuringust, kus käsitletakse VASPidega seonduvaid riske Eestis[13] kui ka Eesti rahapesu ja terrorismi rahastamise tõkestamise siseriiklikust riskihinnangust

[9] Rahapesu Andmebüroo. Virtuaalvääringu teenuse pakkujate uuring. (2020, lk 5) – https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#virtuaalvaaringu-tee--2 (02.02.2023).
[10] Seadusemuudatuste kohta vaata täpsemalt peatükki 3.1.
[11] Landeiro, I. Vahistatud Eesti ettevõtjaid kahtlustatakse 575 miljoni dollari krüptorahakelmuses – Postimees 21.11.2022.
[12] Rahapesu Andmebüroo. Rahapesu Andmebüroo aastaraamat 2022. (2022, lk-d 44, 49) – https://fiu.ee/aastaraamatud-ja-uuringud/aastaraamatud#item-1 (01.04.2023).
[13] Rahapesu Andmebüroo. Virtuaalvääringu teenuse pakkujatega seonduvad riskid Eestis. (2022, lk-d 24-25) – https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#virtuaalvaaringu-tee (02.02.2023).

(edaspidi Eesti riiklik riskihinnang)[14] selgub, et üks riskikohtadest on VASPidele kehtestatud kohustuste mittenõuetekohane täitmine. Eelkõige esineb Eesti VASPide seas puudujääke hoolsusmeetmete ja teatamiskohustuse täitmises. Sellest tulenevalt selgitab autor kvalitatiivset uurimismeetodit kasutades välja, kuidas hoolsusmeetmete ja teatamiskohustuse täitmine täidab rahapesu ja terrorismi rahastamise tõkestamise eesmärki, millised riskid esinevad vastavate kohustuste mittetäitmisel ja kuidas neid riske maandada.

Kuigi VASPidele kohalduvat regulatsiooni on korduvalt täiendatud erinevate rahapesu ja terrorismi rahastamise tõkestamise eesmärki täitvate meetmetega, siis on autor valinud kolmandas peatükis kvalitatiivse uurimismeetodiga analüüsimiseks kaks meedet, mis on autori hinnangul VASPide osas lühikese aja jooksul liialt koormavaks muutunud. Esimeses alaosas selgitab autor välja, kuidas täidab tegevusloa nõue rahapesu ja terrorismi rahastamise tõkestamise eesmärki ning analüüsib laiemalt, kas sage tegevusloa nõuete muutmine on riivanud VASPide õiguspärast ootust. Teises alaosas selgitab autor välja, kuidas täidab kõrge tegevusloa taotlemise ja muutmise riigilõivu nõue rahapesu ja terrorismi rahastamise maandamise eesmärki ja kas kehtiv riigilõivu suurus on proportsionaalne vastava eesmärgi saavutamiseks.

Eelnevast lähtuvalt otsitakse vastuseid järgmistele uurimisküsimustele:

1) Millised on virtuaalvääringutega seotud rahapesu ja terrorismi rahastamise riskid ja kas kehtiva RahaPTS-iga on võimalik neid maandada?
2) Millised on virtuaalvääringu teenuse pakkuja hoolsusmeetmete ja teatamiskohustuse mittenõuetekohase täitmisega seotud rahapesu ja terrorismi rahastamise riskid ja kuidas on neid võimalik maandada?
3) Kuidas on tegevusloa nõuete muutmine mõjutanud rahapesu ja terrorismi rahastamise riske ja VASPide õiguspärast ootust ning kas kehtiv riigilõivu suurus täidab riski maandamise eesmärki?

Autor on uurimisküsimustele vastamiseks kasutanud virtuaalvääringu teenuse pakkuja tegevust reguleerivaid õigusakte ning seadusandja tahte välja selgitamiseks ka vastavate õigusaktide eelnõusid ning nende seletuskirju. Kuna Eesti järgib rahapesu ja terrorismi rahastamise tõkestamise

[14] Eesti rahapesu ja terrorismi rahastamise tõkestamise siseriiklik riskihinnang 2020: 13. Virtuaalvääringute teenuste pakkujate riskide analüüs 2020-2021. (2021, lk 4) – https://www.fin.ee/finantspoliitika-valissuhted/rahapesu-ja-terrorismi-rahastamise-tokestamine/riskihinnangud (16.02.2023).

regulatsioonide väljatöötamisel muu hulgas rahapesuvastase töökonna (ingl k *Financial Action Task Force, FATF*) standardeid, siis tugines autor töö kirjutamisel ka FATFi standarditele, juhenditele ja uuringutele. Lisaks on töös kasutatud RABi avaldatud juhendeid ja Eesti VASPide kohta avaldatud uuringuid. Argumentatsiooni toetasid muu hulgas Eesti ja rahvusvahelised teadusartiklid, statistika ning kohtupraktika. Olukordade illustreerimiseks on autor kasutanud ka uudisartikleid.

Varasemalt on uurinud krüptovaluutadele RahaPTS-i kohaldumist Frank Valdmann, kes kaitses Tallinna Tehnikaülikoolis magistritöö „Rahapesu tõkestamise kohaldumine krüptovaluutadele Eestis“. Analüüsi tulemusena leidis Valdmann, et 2018. aastal kehtinud RahaPTS ei kohaldunud otseselt krüptovaluutadele, mis polnud oma olemuselt virtuaalvääringud, aga tulenevalt krüptovaluutade süsteemi ühetaolisest tehnilisest toimimisest ja virtuaalvääringutega seotusest, täitis sel ajal kehtinud RahaPTS rahapesu ja terrorismi tõkestamise eesmärki.[15] Juridica 8/2020 numbri artiklis „Virtuaalvääringu teenuse regulatiivsed eripärad, senine areng ja perspektiiv“ on Oskar Friedrich Oengo käsitlenud RahaPTS-i 10. märtsil 2020 jõustunud olulisemaid muudatusi virtuaalvääringu teenuse valdkonnas ning järeldanud, et Eesti on vastavate muudatustega teinud esimesed olulised muudatused rahapesu riskide maandamisel, aga laiapõhjalisemad uuendused on veel ees.[16] Aastal 2022 on Kaido Ivan kaitsnud Tartu Ülikoolis magistritöö „Rahapesu virtuaalvääringutega ja selle tõkestamise meetmed“, kus analüüsib virtuaalvääringuga seotud rahapesu ning selle tõkestamise meetmeid ka kriminaalõiguse vaatest.[17] Erinevalt eelnimetatud töödest, annab autor hinnangu 2023. aastal kehtiva RahaPTS-i kohta ning käsitleb lisaks rahapesule ka virtuaalvääringute kasutamist terrorismi rahastamises.

Iseloomustavad märksõnad: rahapesu, terrorismivastane võitlus, virtuaalvääringud, riskimaandus.

[15] Valdmann, F. Rahapesu tõkestamise kohaldumine krüptovaluutadele Eestis. Magistritöö. Juhendaja Kaido Künnapas. Tallinn: Tallinna Tehnikaülikool 2018.
[16] Oengo, O. F., Virtuaalvääringu teenuse regulatiivsed eripärad, senine areng ja perspektiiv. – Juridica 2020/8.
[17] Ivan, K. Rahapesu virtuaalvääringutega ja selle tõkestamise meetmed. Magistritöö. Juhendaja Indrek Tibar. Tartu: Tartu Ülikool 2022.

1. Virtuaalvääringutega seotud riskid ja nendele vastavad maandamismeetmed

1.1. Virtuaalvääringutega seotud riskide liigitus

Selgitamaks välja, millises ulatuses täidavad kehtivad rahapesu ja terrorismi rahastamise tõkestamisele suunatud meetmed eesmärki maandada virtuaalvääringute teenuse pakkumisega seotud rahapesu ja terrorismi rahastamise riske, tuleb esmalt tuvastada, millised maandamist vajavad riskid on virtuaalvääringutega seotud. Kuna õiguskirjanduses puudub ammendav nimekiri virtuaalvääringuga seotud rahapesu ja terrorismi rahastamise riskidest, tugineb autor riskide liigitamiseks ja kaardistamiseks nii Eesti riiklikule kui ka Euroopa Komisjoni riikideülesele riskihinnangule, asjakohaste õigusaktide seletuskirjadele, Euroopa finantsjärelevalve asutuste ja Rahapesu Andmebüroo uuringutele ning FATF-i juhenditele.

Eelnimetatud allikates on kõige olulisema riskitegurina välja toodud virtuaalvääringute anonüümsus. Euroopa Komisjoni riikideüleses 2022. aastal koostatud riskihinnangus on öeldud, et teatud virtuaalvääringu tehingute, eelkõige krüptovääringu tehingute läbipaistvus on piiratud ja tehingutega seotud isikute tuvastamine keeruline.[18] Tehingu asjaolud, nagu tehingu tegemise aeg, saadetud krüptovääringu kogus ja selle liikumine ühelt virtuaalvääringu rahakoti aadressilt teisele on nähtavad plokiahelas[19], kuid virtuaalvääringu rahakoti aadressid pole alati seostatavad konkreetsete isikutega. Seega on keeruline ja mõnel juhul ka võimatu tehingu osapoolte, tegelike kasusaajate, rikkuse allika ja vara päritolu tuvastamine.[20] Täpsemalt käsitleb autor anonüümsusega seonduvaid riske peatükis 1.2.

Virtuaalvääringutega seonduvad riskid tulenevad ka virtuaalvääringu digitaalsest olemusest, mis võimaldab virtuaalvääringute piiriülest levikut. FATF on 2021. aastal avaldatud riskipõhise lähenemise juhendis rõhutanud, et virtuaalvääringute globaalne levik võimaldab rahapesu või terrorismi rahastamiseks valida jurisdiktsioone, kus rahapesu ja terrorismi rahastamise nõuete

[18] Euroopa Komisjon. Supra-National Risk Assessment, lk 94.
[19] Virtuaalvääringute plokiahel on jagatud digitaalne andmebaas, mis salvestab tehinguid ning mida ei ole võimalik muuta, tehes andmed võltsimiskindlaks ja kestvaks. Tehingute detailid on avalikud ja lõpuni jälgitavad. Rahapesu Andmebüroo uuring 2020, lk 3.
[20] Rahapesu Andmebüroo uuring 2020, lk 18.

täitmine on nõrk või olematu või kus puudub suutlikkus teha rahvusvahelist koostööd.[21] Samuti esinevad RABi hinnangul riskid klientidega, kellega on pikk geograafiline distants, kuna sel juhul on keerulisem tunda kliendi tausta ja tuvastada tema tegevuses rahapesu ja terrorismi rahastamise kahtlusega tehinguid.[22] Kiired piiriülesed tehingud hõlbustavad ka virtuaalvääringu ülekannete tegemist kõrge terrorismi- ja/või rahapesuohuga piirkondadesse.[23] Täpsemalt käsitleb autor eelloetletud riske peatükis 1.3.

Riskid esinevad ka detsentraliseeritud virtuaalvääringu teenuse, isikult isikule (ingl *person to person = P2P*) tehingute ja personaalse virtuaalvääringu rahakoti (edaspidi: ingl *unhosted wallet*[24]) kasutamisel. Nimelt ei ole eelmainitud juhtudel alati tuvastatav keskne isik/vahendaja, kes omab tehingu toimumiste üle kontrolli või mõju. Seetõttu pole võimalik tuvastada ka isikut, keda pidada kohustatud isikuks, kellelt oleks võimalik nõuda rahapesu ja terrorismi rahastamise tõkestamise nõuete täitmist. Esineb risk, et kurjategijad kasutavad detsentraliseeritud virtuaalvääringu teenuseid, isikult isikule tehinguid ja *unhosted wallet'*it eesmärgiga vältida kokkupuudet kohustatud isikutega, mis võimaldab tegeleda varjatult rahapesu ja terrorismi rahastamisega.[25] Täpsemalt käsitleb autor vastavaid riske peatükis 1.4.

Lisaks eelnevale on tuvastatud ka Eesti-spetsiifilised virtuaalvääringu teenuse pakkumisega seonduvad riskid. Nii Eesti riikliku riskihinnangu[26] kui ka Rahapesu Andmebüroo uuringute[27] kohaselt on virtuaalvääringu teenuse pakkujatel vähene seotus Eestiga. Nimelt seob sageli tegevusloaga virtuaalvääringu teenuse pakkujaid Eestiga vaid see, et need on Eestis registreeritud – tegelik äritegevus, kliendid, ettevõtte juhatuse liikmed ja tegelikud kasusaajad asuvad välismaal. Samuti on riskikohaks virtuaalvääringu teenuse pakkujate ebapiisav hoolsusmeetmete kohaldamine. Näiteks esineb puudujääke isikusamasuse tuvastamisel ja ärisuhte seiramises.

[21] Financial Action Task Force. Updated Guidance: A Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. (2021, lk 16) – https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (02.02.2023).
[22] Rahapesu Andmebüroo uuring 2022, lk 17.
[23] Financial Action Task Force. Updated Guidance 2021, lk 16.
[24] Kuna eesti keeles puudub *unhosted wallet*'ile täpne vaste ja RahaPTS 507 SE seletuskirjas on kasutatud väljendit „*unhosted wallet*", siis kasutab autor töös läbivalt inglisekeelset väljendit.
[25] Euroopa Komisjon. Supra-National Risk Assessment, lk 95.
[26] Eesti riiklik riskihinnang 2021, lk-d 1-6.
[27] Rahapesu Andmebüroo uuring 2020; Rahapesu Andmebüroo uuring 2022.

Probleemkohaks on ka teatamiskohustuse vähene täitmine.[28] Täpsemalt käsitleb autor VASPidele kohalduvate kohustuste täitmist 2. peatükis.

Autor on eeltoodud argumentidest lähtudes seisukohal, et virtuaalvääringutega seotud riskid seonduvad peamiselt kolme riskiteguriga – anonüümsus, piiriülene levik ja kohustatud isiku puudumine. Käsitletud allikate järgi on kõik kolm käsitletavad nii rahapesu kui ka terrorismi rahastamise riskiteguritena. Järgnevalt selgitab autor virtuaalvääringutega seotud riske eelnimetatud riskitegurite kaudu ning analüüsib, kas tuvastatud riskid on Eesti rahapesu ja terrorismi rahastamise tõkestamise regulatsiooniga maandatud.

1.2. Virtuaalvääringute anonüümsus

Üheks peamiseks riskiteguriks, mis suurendab virtuaalvääringute väärkasutamist rahapesu ja terrorismi rahastamise eesmärgil, on virtuaalvääringuga seotud anonüümsus, mida kasutatakse tehinguga seotud osapoolte ja vara päritolu varjamiseks. Virtuaalvääringuga seotud anonüümsust kui riskitegurit on nimetatud muu hulgas nii 2022. aasta Euroopa Komisjoni riikideüleses riskihinnangus, Eesti 2021. aasta riiklikus riskihinnangus, FATFi juhistes, RahaPTS 459 SE seletuskirjas kui ka Rahapesu Andmebüroo uuringutes, mis käsitlevad virtuaalvääringu teenuse pakkumist Eestis. Virtuaalvääringu kasutaja ja tehingute anonüümsuse suurendamist võimaldavad erinevad tehnilised lahendused: osalise anonüümsusega virtuaalvääringud, suurendatud anonüümsusega virtuaalvääringud ja tehingute anonüümse(ma)ks muutmise teenused.

Nagu eespool nimetatud, on üheks anonüümsuse suurendamise võimaluseks kasutada tehingute tegemisel osalise anonüümsusega virtuaalvääringuid. Virtuaalvääringud jagunevad tsentraliseeritud ja detsentraliseeritud virtuaalvääringuteks. Esimeste puhul on väärigutel keskne administraator, kes virtuaalvääringuid emiteerib, haldab ja vajadusel eemaldab need käibelt. Detsentraliseeritud väärigutel keskset haldajat pole, vaid tegemist on hajus süsteemiga, kus osalejaid tegelevad ise virtuaalvääringu emissiooniga ja peavad avalikku pearaamatut kinnitades tehinguid matemaatikal põhineva konsensuse saavutamise algoritmi abil.[29] Üheks detsentraliseeritud virtuaalvääringu alaliigiks on krüptoväärigud, mille puhul süsteemis osalejad kasutavad tehingute kinnitamiseks krüptograafiat. Tuntuimaks krüptovääringuks on Bitcoin, mida

[28] Rahapesu Andmebüroo uuring 2022, lk 21.
[29] Financial Action Task Force. FATF report: Virtual Currencies Key Definitions and Potential AML/CFT Risks. (2014, lk 5) – https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (24.02.2023).

saab pidada osalise anonüümsusega virtuaalvääringuks. Nimelt on iga Bitcoini tehing kajastatud plokiahelas, sealhulgas on nähtav Bitcoini saatja ja saaja virtuaalvääringu rahakoti aadress (analoogne panga arvelduskonto numbriga), tehingu tegemise aeg ning saadetud Bitcoini kogus. Küll aga on virtuaalvääringu rahakoti aadress 26 – 35 tähest ja numbrist kombineeritud jada, mis ei ole konkreetse isikuga seostatav, sest virtuaalvääringu rahakoti loomisel ei nõuta alati isikut tuvastavate andmete esitamist. Kuna tehingud Bitcoiniga on kronoloogiliselt ja avalikult salvestatud plokiahelasse, siis on vara liikumise tee tagasiulatuvalt nähtav ja edaspidi jälgitav, aga kuniks ei ole tuvastatud seost virtuaalvääringu rahakoti aadressi ja selle kasutaja vahel, on Bitcoini kasutamine anonüümne.[30]

Pärast Bitcoini kui maailma esimese krüptovääringu kasutusele võtmist hakati looma alternatiivseid vääringuid, mis tagavad vääringu kasutajatele ja tehingutele veelgi suurema anonüümsuse. Sellisteks anonüümsust suurendavateks virtuaalvääringuteks on näiteks Monero ja Zcash. Eelnimetatud virtuaalvääringutega tehingute tegemisel ei ole erinevalt Bitcoinist plokiahelas nähtavad virtuaalvääringu saatja, saaja ja tehingusumma. Tehingutega seotud asjaolud on plokiahelas varjatud ning teada üksnes tehingu osapooltele.[31] Küll aga on võimalik tehingu asjaolusid avalikustada. Nimelt on virtuaalvääringu rahakoti kasutajal vaatamise võti (ingl *viewing key*), mis võimaldab selle teadjal näha vastava rahakotiga seotud tehingute andmeid.[32]

Üks suurimatest lunavararünnakutest, mis seostub Monero kuritegeliku kasutusega on 2017. aastal toimunud WannaCry küberrünnak. Nimelt loodi Põhja-Koreas pahavara, mis nakatas 150 riigis kokku ligi 300 000 arvutit ja muutis arvuti kasutajale juurdepääsu kõvakettal olevatele failidele võimatuks. Juurdepääsu taastamiseks nõuti ohvritelt lunaraha Bitcoinides.[33] Anonüümsuse suurendamiseks vahetati küberrünnakust saadud Bitcoinid Šveitsi virtuaalvääringu vahetuse teenusepakkuja kaudu Moneroks.[34]

[30] Euroopa Parlament. Virtual currencies and terrorist financing: assessing the risks and evaluating responses. (2018, 30-31) – https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf (24.02.2023).
[31] Ibid, lk 32.
[32] Electric Coin Company. Explaining viewing keys. (2020) – https://electriccoin.co/blog/explaining-viewing-keys/ (11.02.2023).
[33] Fruhlinger, J. WannaCry explained: A perfect ransomware storm. (2022) – https://www.csoonline.com/article/3227906/wannacry-explained-a-perfect-ransomware-storm.html (11.02.2023).
[34] Suberg, W. Bitcoin Exchange ShapeShift Helps Police As WannaCry Attacker Converts To Monero. (2017) – https://cointelegraph.com/news/bitcoin-exchange-shapeshift-helps-police-as-wannacry-attacker-converts-to-monero (11.02.2023).

Lisaks sellele, et vara liikumise jälgimist on võimalik raskendada kasutades osalise või suurendatud anonüümsusega virtuaalvääringuid, on kasutusel ka tehingute anonüümsemaks muutmise teenus ehk segamisteenus. Nimetatud teenuse puhul sooritatakse kliendi virtuaalvääringutega mitmeid tehinguid erinevate virtuaalvääringu rahakottide vahel, seejuures segades virtuaalvääringuid ka teiste klientide varaga ning seejärel kantakse pea samas väärtuses (miinus tehingutasu) virtuaalvääringud kliendi teisele virtuaalvääringu rahakoti aadressile.[35] Nii katkestatakse otsesed seosed esialgse ja lõpliku virtuaalvääringu rahakoti vahel, mistõttu on vara päritolu hiljem väga keeruline tuvastada.

Segamisteenust kasutatakse praktikas rahapesu ja terrorismi rahastamise varjamiseks. Aastal 2019 peatati maailma ühe juhtiva krüptovääringute segamisteenuse pakkuja Bestmixer.io tegevus. Leiti, et teenusepakkuja oli segamise kaudu tegelenud rahapesuga summas ligi 190 miljonit eurot.[36] Samal aastal toimus ka Sri Lankal ülestõusmispühale ajastatud terroriorganisatsiooni ISIS korraldatud terrorirünnak. On tuvastatud, et toimunud terroriakti rahastati krüptovääringutega, sealhulgas kasutati vara päritolu varjamiseks segamise meetodit.[37]

Kokkuvõttes eksisteerib risk, et osalise või suurendatud anonüümsusega virtuaalvääringuid ning anonüümsust pakkuvaid teenuseid kasutatakse rahapesu või terrorismi rahastamisega tegeleva isiku ja vara päritolu varjamiseks. Eelnimetatud riski maandamiseks tuleb kohaldada eelkõige ennetavaid meetmeid ehk hoolsusmeetmeid. Hoolsusmeetmete rakendamisel järgitakse „tunne oma klienti“ põhimõtet, mille kohaselt tuleb aru saada kliendi taustast ning teenus(t)e soovimise põhjustest. Kliendi tundmiseks tuleb mh kontrollida, kas klient on isik, kellena ta end esitleb, kas kliendi soov läheb kokku tema tegeliku tegevuse, võime ja vajadustega ning milline on kliendi äritegevus.[38] Hoolsusmeetmed jagunevad kohaldamise aja järgi kaheks: meetmed, mida kohaldatakse ärisuhte loomisel ning edasisel ärisuhte pideval jälgimisel ehk seirel. Hoolsusmeetmete kohaldamise kohustus on RahaPTS §-s 2 nimetatud kohustatud isikutel. RahaPTS § 2 lg 1 p 10 ja § 3 p 3 järgi on kohustatud isikuteks teiste hulgas virtuaalvääringu teenuse

[35] Mbiyavanga, S., lk 6.
[36] Europol. Multi-million euro cryptocurrency laundering service Bestmixer.io taken down. (2019) – https://www.europol.europa.eu/media-press/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down (26.02.2023).
[37] Amiram, D., Jørgensen, B.N, Rabetti, D. Coins for Bombs: The Predictive Ability of On-Chain Transfers for Terrorist Attacks. – Journal of Accounting Research 2022/60, No.2.
[38] Rahapesu Andmebüroo. Rahapesu ja terrorismi rahastamise riskide juhtimine ning hoolsusmeetmete kohaldamine Rahapesu Andmebüroo järelevalvatavatele kohustatud isikutele. (2022, lk 21) – https://fiu.ee/oigusaktid-ja-juhendid/juhendid#rahapesu-ja-terroris (26.02.2023).

pakkujad (edaspidi VASP) ehk ettevõtjad, kes pakuvad virtuaalvääringu rahakotiteenust, virtuaalvääringu vahetamise teenust, virtuaalvääringu ülekande teenust või tegelevad virtuaalvääringu väljastamisega. Järgnevalt analüüsib autor, kas isikutel, kes kasutavad tehingute tegemisel anonüümsust pakkuvaid virtuaalvääringuid või teenuseid, on kokkupuude VASPidega, kes maandavad anonüümsuse riski hoolsusmeetmete rakendamise kaudu.

Nagu sissejuhatuses mainitud, siis rahapesu esimeses ehk paigutamise etapis suunatakse eelkuriteo toimepanemisel saadud vara finantssüsteemi. Virtuaalvääringute puhul tuleb selleks esmalt luua ise või teenuseosutaja abil virtuaalvääringu rahakott ja selles sisalduv avalik ja privaatne võti (mitmekümnetest tähtedest ja numbritest koosnev kombinatsioon, näiteks f9600b8954df8b689cdc4…). Avalikust võtmest tuletatakse virtuaalvääringu rahakoti aadress, mis on sisuliselt avaliku võtme lühendatud versioon. Virtuaalvääringu rahakoti aadress on võrreldav panga arvelduskonto numbriga, mida saab avalikult jagada ja on aadressiks, kuhu virtuaalvääringuid saata. Samas rahakotis hoitakse ka privaatset võtit, mis on võrreldav parooliga. Privaatse võtme abil saab isik juurdepääsu virtuaalvääringu rahakoti aadressile saadetud virtuaalvääringutele. Võtmega kinnitatakse virtuaalvääringu saatmise ja saamise tehingud ning tõendatakse plokiahelas kuvatava virtuaalvääringu omandiõigust. Teaduskirjanduse kohaselt on virtuaalvääringu rahakotte võimalik luua ja hoida veebilehtedel, näiteks Coinbase või MyEtherWallet, või laadida nutitelefoni, arvuti töölauale või hoiustada eraldi riistvara andmekandjal, näiteks mälupulgal või kirjutades vastavad numbri- ja tähekombinatsioonid paberile.[39]

Virtuaalvääringu rahakotte saab rahakoti looja ja hoidja järgi jaotada kaheks. Kasutada saab kolmanda osapoole teenust, mille raames luuakse ja hoitakse kliendi avalikku ja privaatset võtit ning tagatakse nende turvalisus (ingl *hosted wallet*). Samuti saab virtuaalvääringu rahakotte, sealhulgas avalikku ja privaatset võtit luua ise ilma teenusepakkujata (ingl *unhosted wallet*), kasutades selleks Internetis tasuta kättesaadavaid digitaalseid tööriistu, sealhulgas näiteks OpenSLL tarkvara. Sellisel juhul peab isik ise tagama võtmete privaatsuse ja turvalisuse.[40] Nagu eelnevalt nimetatud, on RahaPTS-is kohustatud isikuks ka virtuaalvääringu rahakotiteenuse osutaja. RahaPTS § 3 p 10 järgi on selleks ettevõtja, kes pakub teenust, mille raames luuakse

[39] Kim, S. H., Taylor, S., jt. A comprehensive forensic preservation methodology for crypto wallets. – Forensic Science International: Digital Investigation 2022/42-43, lk 4-5.
[40] *Ibid*, lk-d 2-3.

klientidele või hoitakse klientide krüpteeritud võtmeid, mida saab kasutada virtuaalvääringute hoidmise, talletamise ja ülekandmise eesmärgil. Virtuaalvääringu rahakoti loomist teenusepakkujata RahaPTS-is ei reguleerita. Seega, isiku puhul, kes soovib luua virtuaalvääringu rahakoti, et teha tehinguid anonüümsust pakkuvate virtuaalvääringutega, kohaldatakse hoolsusmeetmeid siis, kui ta kasutab VASPi poolt pakutavat rahakotiteenust.

Suurendatud anonüümsusega virtuaalvääringute kasutamine on praktikas piiratud, sest vähesed teenuseosutajad pakuvad suurendatud anonüümsusega virtuaalvääringu vahetamise teenust fiat-raha vastu. Küll aga vahetatakse suurendatud anonüümsusega virtuaalvääringuid teiste virtuaalvääringute, eelkõige Bitcoini vastu.[41] Kui AMLD5 järgi on virtuaalvääringu vahetamise teenuse osutajaks üksnes ettevõtjad, kes vahetavad virtuaalvääringut ametlikuks vääringuks ehk fiat-rahaks ja vastupidi[42], siis Eesti seadusandja on lähtunud laiemast käsitlusest, järginud FATFi juhistes võetud seisukohta[43] ning kehtestanud RahaPTS § 3 p-s 10^1, et lisaks virtuaalvääringu vahetamisele fiat-rahaks ja vastupidi, on virtuaalvääringu vahetamise teenuseks ka virtuaalvääringu vahetamine teise virtuaalvääringu vastu. Seega, suurendatud anonüümsusega virtuaalvääringute vahetamisel rakendatakse hoolsusmeetmeid ka isikute suhtes, kes kasutavad VASPide virtuaalvääringu vahetamise teenust. Küll aga on võimalik *unhosted wallet'i* ja isikult isikule tehingute abil vahetada ja üle kanda virtuaalvääringuid ilma teenusepakkujata, mistõttu sellistel juhtudel isikute suhtes hoolsusmeetmeid ei rakendata.

Anonüümsust pakkuv teenus ehk segamisteenus ei ole sõnaselgelt RahaPTS-is reguleeritud. Seega tuleb analüüsida, kas segamisteenus võib kuuluda seaduses määratletud teenuste alla. Tüüpiline segamisteenus näeb välja järgmine: isik loob virtuaalvääringu rahakoti A, kuhu laekub kuritegelikul teel saadud vara. Isik kannab varad rahakotist A segamisteenuse rahakotti B. Seejärel sooritatakse virtuaalvääringutega suurel hulgal tehinguid paljude rahakottide vahel, segades vara ka teiste kasutajate virtuaalvääringutega.[44] Samas väärtuses virtuaalvääringud, mis on pärit teistest rahakottidest, laekuvad segamisteenuse rahakotti C, kust arvutatakse maha teenustasu. Ülejäänud summa kantakse isiku teise rahakotti D, kust ta saab juurdepääsu pestud virtuaalvääringutele.[45]

[41] Euroopa Parlament 2018, lk 35.
[42] 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 156/43, Art 1 lg 1 p c).
[43] Financial Action Task Force. Updated Guidance 2021, lk 22.
[44] Mbiyavanga, S., lk 6.
[45] Rahapesu Andmebüroo uuring 2020, lk 16.

Kuna sisuliselt on tegemist teenusega, kus ühe isiku virtuaalvääringud vahetatakse teise isiku virtuaalvääringute vastu, lihtsalt lühikese aja jooksul suurel hulgal virtuaalvääringu rahakottide vahel, siis on tegemist virtuaalvääringu vahetamise teenusega RahaPTS § 3 lg 10[1] mõistes. Seega on segamisteenuse osutajad VASPid, kes peavad klientide suhtes hoolsusmeetmeid rakendama.

Kokkuvõttes rakendatakse hoolsusmeetmeid anonüümsete virtuaalvääringutega tehingute tegijate peal siis, kui nad kasutavad virtuaalvääringu rahakoti loomiseks ja nendega tehingute tegemiseks VASPi teenuseid. Samuti rakendatakse hoolsusmeetmed ka segamisteenuse kasutajatele. Seevastu on võimalik vältida hoolsusmeetmete kohaldumist, kui isikud kasutavad enda loodud *unhosted wallet*'it ja virtuaalvääringu tehingud tehakse VASPi abita ehk otse ühel isikult teisele. Kuna need on seotud lähemalt teise riskiteguriga, milleks on kohustatud isiku puudumine, siis käsitleb autor vastavaid riske täpsemalt peatükis 1.4.

Järgnevalt annab autor hinnangu, kas VASPi klientidele kohalduvad hoolsusmeetmed täidavad eesmärki maandada anonüümsusest tulenevaid riske. Ärisuhte loomisel tuleb vastavalt RahaPTS §-le 20 kohustatud isikul tuvastada ja kontrollida: 1) kliendi või juhuti tehingus osaleva isiku isikusamasust; 2) esindaja isikusamasust ja esindusõigust; 3) tegeliku kasusaaja isikusamasust; 4) ärisuhte või juhuti tehtava tehingu eesmärki ja olemust; 5) riikliku taustaga isikuks, tema pereliikmeks või lähedaseks kaastöötajaks olemist; ning 6) asjakohasel juhul rikkuse allikat ja/või vara päritolu.

Kliendi, tema esindaja ning tegeliku kasusaaja isikusamasuse tuvastamisel kogutakse esmalt isikut identifitseeriv teave. RahaPTS §-s 21 ja §-s 22 on loetletud andmed, mida tuleb vastavalt füüsilise isiku ja juriidilise isiku kohta koguda. Üldreeglina peab kohustatud isik füüsilise isiku puhul tuvastama: 1) nime; 2) isikukoodi või selle puudumisel sünniaja ning elu-või asukoha; 3) teabe esindusõiguse ja selle ulatuse kohta; ja 4) sidevahendite andmed. VASPidele on kehtestatud RahaPTS § 25 lg-s 2[2] erisäte, mille kohaselt tuleb neil isikusamasuse tuvastamisel koguda kontaktandmetena vähemalt isiku telefoninumber ja elektronposti aadress. Seejärel tuleb saadud teavet kontrollida usaldusväärsest ja sõltumatust allikast (nt rahvastikuregister, kehtiv pass, äriregister) pärit andmete abil, et kohustatud isik veenduks andmete tõesuses. Isikusamasuse tuvastamisel saadud teabe kontrollimise eesmärk on veenduda, kas ärisuhet luua sooviv isik, on see isik, kellena ta end esitleb.

RABi juhendi[46] kohaselt on ärisuhte eesmärgi ja olemuse tuvastamise eesmärk saada ülevaade ja arusaam kliendist ning põhjusest, miks teenust vajatakse. Samuti tuleb asjakohasel juhul vastava eesmärgi mõistmiseks tuvastada ka kliendi rikkuse allikas ja/või vara päritolu, mis annab ülevaate, kui palju on kliendil rahalisi vahendeid ja kust on need pärit. Vastav teave on oluline eelkõige ärisuhte seireks, et kohustatud isik saaks hinnata, kas kliendi tegevus ja ärisuhte kestel tehtavad tehingud on kooskõlas ärisuhte loomisel kogutud teabega. Teisisõnu on teadaoleva info põhjal võimalik tuvastada kliendiprofiilile mittevastavaid ebatavalisi tehinguid, mis võivad viidata rahapesule või terrorismi rahastamisele.

Riikliku taustaga isiku tuvastamisel tuleb kindlaks teha, kas isik täidab või on täitnud avaliku võimu olulisi ülesandeid ning kas tema suhtes jätkuvalt esinevad sellega seotud riskid, eelkõige korruptsioonirisk. Avaliku võimu oluliste ülesannete täitjateks on RahaPTS § 9^1 lg 2 järgi näiteks riigipea, minister ja riigi kõrgeima kohtu kohtunik. Tuvastamise eesmärk on kindlaks teha, kas isiku puhul on tegemist riikliku taustaga isikuga, kellele tuleb RahaPTS § 36 lg 2 p 2 järgi kohaldada hoolsusmeetmeid tugevdatud korras.

Autori hinnangul on anonüümsusest tuleneva riski maandamiseks oluline eelkõige isikusamasuse tuvastamise käigus isikut identifitseeriva teabe kogumine ja selle kontrollimine. Kliendi nime, isikukoodi või sünniaja ning elu- või asukoha tuvastamine võimaldab VASPi loodud või tema teenuse käigus kasutatava kliendi virtuaalvääringu rahakoti aadressi siduda konkreetse isikuga. Seega osalise anonüümsusega virtuaalvääringutega tehtavad tehingud, mis toimuvad kliendi virtuaalvääringu rahakotiga, on VASPile plokiahelast nähtavad ja kliendiga seostatavad. Sellest tulenevalt on võimalik kohaldada ka ärisuhte kestel tõhusat seiret ehk tuvastada plokiahelast kliendiga seotud tehinguid, mis viitavad rahapesule või terrorismi rahastamisele. Kliendi kontaktandmetest telefoninumbri ja elektronposti aadressi kogumine võimaldab kliendiga ühendust võtta, kui see on vajalik hoolsusmeetmete rakendamiseks. Kliendi kohta teabe kogumine ja sidumine see virtuaalvääringu rahakoti aadressiga muudab tehingute toimumise läbipaistvaks, mille tulemusel muutub virtuaalvääringute kasutamine rahapesuks ja terrorismi rahastamiseks ebaatraktiivseks.

Anonüümsust suurendavate virtuaalvääringute puhul ei piisa üksnes kliendi ja tema virtuaalvääringu rahakoti aadressi tuvastamisest, kuna vastavate virtuaalvääringute puhul on

[46] Rahapesu Andmebüroo riskide juhtimise juhend 2022, lk 41.

kliendil võimalik muuta plokiahelas virtuaalvääringu rahakoti aadressiga seotud tehingud varjatuks. Küll aga on virtuaalvääringu rahakoti omanikul nn vaatamise võti, mis võimaldab võtme teadjal rahakoti aadressiga seotud tehinguid plokiahelas vaadata. Seega tuleks VASPidel anonüümsust suurendavate virtuaalvääringutega tehingute puhul küsida kliendilt ka tehingute vaatamise võtit, et VASPil oleks ärisuhte jooksul võimalik teostada ärisuhte seiret.

Segamisteenuse puhul viiakse kliendi virtuaalvääringutega läbi mitmeid tehinguid erinevate virtuaalvääringu rahakottide vahel, eesmärgiga vara liikumise jälgimist raskendada ja seeläbi vara päritolu varjata. Kuna segamisteenuse osutaja on VASP, rakendab ta kliendi suhtes anonüümsuse riski maandamiseks hoolsusmeetmeid, sealhulgas kliendi ja vara allika/päritolu tuvastamist ning vajadusel tehingus kasutatud vahendite allika ja päritolu tuvastamist. Rahapesu ja terrorismi rahastamise kahtluse korral edastab VASP teabe Rahapesu Andmebüroole.

Juhul, kui isik keeldub nõutud andmete esitamisest või ei esita infot vajalikul määral ning see on vajalik isikusamasuse tuvastamiseks ja/või ärisuhte eesmärgist ja olemusest arusaamiseks ja/või vara allika või päritolu tuvastamiseks, on tegemist olukorraga, kus kohustatud isikul ei ole võimalik hoolsusmeetmeid nõuetekohaselt täita. Sellisel juhul on VASPil RahaPTS § 42 lg 1 p 1 järgi keelatud luua isikuga ärisuhet. Samuti on VASPidele kehtestatud RahaPTS § 25 lg-s 2 keeld sõlmida leping või teha otsus anonüümse virtuaalvääringu rahakoti avamise kohta. Keelu rikkumise korral on tehing tühine. Seega olukordades, kus kliendi anonüümsust pole võimalik kõrvaldada, on riski maandamise meetmeks tehingu tegemise ja ärisuhte loomise keeld.

Eelnevast tulenevalt on virtuaalvääringu anonüümsusest tulenevad riskid maandatud, kui need toimuvad RahaPTS-is sätestatud kohustatud isikute kaudu, sest anonüümsus kõrvaldatakse kliendi isikusamasuse tuvastamisel ja kontrollimisel ning isiku seostamisel tema virtuaalvääringu rahakotiga. Ka segamisteenusega kaasnev anonüümsuse risk on maandatud, kuna tegemist on virtuaalvääringu teenuse pakkumisega, kus klientide suhtes tuleb kohaldada anonüümsust kõrvaldavaid hoolsusmeetmeid. Küll aga tuleb anonüümsust suurendavate virtuaalvääringute puhul täiendada RahaPTS-is kliendiandmete kogumise nõuet nn vaatamise võtme kogumisega, kuna see võimaldab kliendi virtuaalvääringu rahakotiga seotud tehingud teha plokiahelas nähtavaks, mis tagab VASPile võimaluse teostada ärisuhte seiret. Juhul, kui klienti pole võimalik tuvastada, on rahapesu ja terrorismi rahastamise riskid maandatud tehingu tegemise ja ärisuhte loomise keeluga. Anonüümsuse riskid esinevad ka *unhosted wallet'*i ja isikult isikule tehingute

puhul. Kuna *unhosted wallet'*i ja isikult isikule tehingute anonüümsus tuleneb teisest riskitegurist ehk kohustatud isiku puudumisest, siis käsitleb autor vastavat teemat lähemalt peatükis 1.4.

1.3.Virtuaalvääringute piiriülene levik

Järgmine riskitegur, mis on välja toodud nii 2022. aasta Euroopa Komisjoni riikideüleses riskihinnangus, Eesti 2021. aasta riiklikus riskihinnangus, FATFi juhistes, RahaPTS 507 SE seletuskirjas kui ka Rahapesu Andmebüroo uuringutes on virtuaalvääringu piiriülene levik. FATFi raporti[47] kohaselt on virtuaalvääringute globaalse kasutuse tinginud virtuaalvääringu digitaalne olemus ja võimalus teha kiireid rahvusvahelisi virtuaalvääringu ülekandeid Interneti teel.

Euroopa Komisjoni riikideüleses riskihinnangus on välja toodud, et üheks oluliseks riskiks on piiriüleste tehingute tegemine kõrge terrorismi- ja/või rahapesuohuga piirkondadest isikutega.[48] Samuti esineb suurem rahapesu ja terrorismi rahastamise risk klientide puhul, kes asuvad teises riigis, veel enam kõrge riskiga piirkonnas ehk jurisdiktsioonis, kus rahapesu, terrorismi rahastamise ja massihävitusrelvade leviku tõkestamise meetmed on puudulikud. Nendeks riikideks on näiteks Iraan, Põhja- Korea ja Myanmar.[49] Teistest riikidest kliente on raskem tuvastada, kuna kliendisuhte loomine ei toimu füüsiliselt samas kohas viibides ja isikut tõendavate dokumentide vormid on igas riigis ainulaadsed, mis teeb valeandmete ja võltsitud dokumentide tuvastamise keerulisemaks.[50]

Samuti on risk see, et rahapesijatel ja terrorismi rahastajatel on võimalik kasutada virtuaalvääringu teenuseid, mille osutajad asuvad jurisdiktsioonis, kus rahapesu ja terrorismi rahastamise tõkestamise regulatsioon ja järelevalve on nõrk ning kus puudub suutlikkus teha rahvusvahelist koostööd.[51] Rahapesu Andmebüroo aastaraamatute 2021 ja 2022[52] kohaselt olid Eestiski aastal 2021 VASPide sektoris puudujäägid. Muuhulgas toodi välja, et vastavas sektoris on ebapiisavad nõuded loataotlejale, sektorist puudub täielik riskipilt ja kohapealne järelevalve on raskendatud. Aastal 2022 on Eesti olnud jätkuvalt atraktiivne transiitriik rahapesuks ja terrorismi rahastamiseks.

[47] Financial Action Task Force 2014, lk 9.
[48] Euroopa Komisjon. Supra-National Risk Assessment, lk 98.
[49]Financial Action Task Force. "Black and grey" lists. (2023) – https://www.fatf-gafi.org/en/countries/black-and-grey-lis<ts.html (17.02.2023).
[50] Rahapesu Andmebüroo 2022 uuring, lk 17.
[51] Euroopa Komisjon. Supra-National Risk Assessment, lk 98.
[52] Rahapesu Andmebüroo. Rahapesu Andmebüroo aastaraamat 2021. (2021, lk 31) – https://fiu.ee/aastaraamatud-ja-uuringud/aastaraamatud#item-2 (19.02.2023); Rahapesu Andmebüroo aastaraamat 2022, lk-d 8, 26.

Eesti VASPe kasutatakse välisriikides saadud kriminaaltulu kihistamiseks ja terrorismi rahastamise korral tulu edastamiseks.

Klientidele, kes on pärit kõrge riskiga või koostööd mittetegevate riikide nimekirjast või kelle isikusamasuse tuvastamine tehakse kaugtuvastusena, tuleb kohustatud isikul määrata kõrgem riskiaste. Sel juhul tuleb rakendada hoolsusmeetmeid tugevdatud korras. RahaPTS § 38 lg 2 järgi võib kohustatud isik tugevdatud hoolsusmeetmete rakendamiseks koguda täiendavat teavet näiteks ärisuhte, tehingu või toimingu eesmärgi ja olemuse kohta ning kontrollida seda lisadokumentide ja teabe põhjal, mis pärinevad usaldusväärsest ja sõltumatust allikast. Samuti võib koguda täiendavat teavet ja dokumente ärisuhtes tehtavate tehingute tegeliku teostamise ja kasutatavate vahendite allika ja päritolu kohta, et välistada tehingute näilisus. Juhul, kui klient on pärit või tema elu- või asukoht on Euroopa Majanduspiirkonna välises riigis ja ärisuhte loomisel ei kohaldata hoolsusmeetmeid isikuga samas kohas viibides, tuleb RahaPTS § 31 lg 1 p 1 kohaselt kohustatud isikul tuvastada ja andmeid kontrollida infotehnoloogiliste vahendite abil. Kaugtuvastamise protseduur on täpsemalt reguleeritud rahandusministri kehtestatud määrusega „Infotehnoloogiliste vahendite abil isikusamasuse tuvastamine ja andmete kontrollimise tehnilised nõuded ja kord“[53]. Seega on RahaPTS-is kehtestatud tõhusad hoolsusmeetmed klientide tuvastamiseks, kes asuvad väljaspool Eestit, sh kõrge riskiga riikides.

Kui esineb risk, et piiriüleseid tehinguid tehakse rahapesu või terrorismi rahastamise eesmärgil, on oluline rakendada ärisuhte kestel kohalduvaid hoolsusmeetmeid ehk seirata ärisuhet. See hõlmab pidevat ärisuhte jälgimist, et tuvastada, kas teostatavad tehingud vastavad teadaolevale kliendiprofiilile ja kas on asjaolusid, mis viitavad võimalikule rahapesule või terrorismi rahastamisele. Tehingute jälgimist teostatakse kahel viisil: skriinimisega ehk tehingute reaalajas jälgimisega ja monitoorimisega ehk tehingute hilisema analüüsiga. Skriinimise eesmärk on tuvastada rahapesu ja terrorismi rahastamise kahtlaseid ja ebaharilikke tehinguid, riikliku taustaga või sanktsioneeritud isikuid ning etteantud piirmäärasid ületavaid tehinguid. Monitoorimiseks selekteeritakse tehingud, mida hiljem analüüsida, näiteks teatud perioodil tehtud piirmäära ületavad tehingud.[54] Kui seire käigus tuvastatakse terrorismi rahastamise või rahapesu kahtlane tehing, ebaharilik tehing, ebatavaline tegevus, piirmäära ületav tehing või rahvusvaheline

[53] Infotehnoloogiliste vahendite abil isikusamasuse tuvastamise ja andmete kontrollimise tehnilised nõuded ja kord. RaMm 23.05.2018 nr 25. – RT I, 04.12.2020, 9.
[54] Rahapesu Andmebüroo riskide juhtimise juhend 2022, lk 44-47.

finantssanktsiooni subjekt, siis on VASPil kohustus sellest teavitada Rahapesu Andmebürood (edaspidi RAB).

Kui esineb risk, et kurjategijad valivad endale soodsa jurisdiktsiooni, kus rahapesu ja terrorismi rahastamise nõuete kohaldamine on nõrk või puudulik, on oluline rahvusvaheliste standardite kehtestamine ning nende järgimine võimalikult paljude riikide poolt. Rahapesu ja terrorismi rahastamise valdkonnas on globaalse ulatusega rahvusvaheliste standardite kehtestajaks Financial Action Task Force (FATF). Üle 200 riigi ja jurisdiktsiooni on võtnud kohustuse rakendada FATFi standardeid, sealhulgas Eesti.[55]

Eesmärgiga maandada rahapesu ja terrorismi rahastamise riski, mis on tingitud virtuaalvääringu piiriülesest levikust ja VASPide piiriülesest teenuse pakkumisest, laiendas FATF 2019. aastal „travel rule"[56] nõude kohaldumisala VASPidele. Lihtsustatult tuleb „travel rule" nõude järgi virtuaalvääringu vahetamise ja ülekandeteenuse puhul koguda ja talletada andmeid nii virtuaalvääringu ülekande algataja kui ka saaja kohta ning jagada seda teavet ülekande saaja kohustatud isikuga (nt VASPi, krediidi- või finantseerimisasutusega). Ülekande osapoolte kohta kogutud teabe alusel otsustatakse virtuaalvääringu ülekande toimumine. Samuti on oluline mõlema osapoole tuvastamine, et edastada konkreetsed isikuandmed järelevalve- ja uurimisasutustele, kui monitoorimise käigus selgub, et isikute vahel toimuvad rahapesu ja terrorismi rahastamise kahtlased tehingud.[57] Järgnevalt käsitleb autor täpsemalt „travel rule" nõude sisu ja selgitab välja, kas vastav nõue on Eesti õigusesse FATFi standardist üle võetud.

„Travel rule" nõue kohaldub nii siseriiklike kui ka piiriüleste ülekannete puhul ja olukordades, kus ülekanne toimub (kas rahas või virtuaalvääringus): a) finantsasutuste vahel b) VASPi ja teise kohustatud isiku vahel (nt teine VASP või pank) c) VASPi ja mittekohustatud isiku vahel (nt *unhosted wallet'it* kasutav isik). Kuna finantsasutuste vaheline ülekannete tegemine ei hõlma VASPe ning VASPi ja mittekohustatud isiku vaheline ülekanne seondub järgmise peatükiga, siis

[55] Financial Action Task Force. Who we are. (2023) – https://www.fatf-gafi.org/en/the-fatf/who-we-are.html (17.02.2023).
[56] Kuna „travel rule" nõudel ei ole eestikeelset vastet ja RahaPTS 507 SE seletuskirjas on kasutatud väljendit „travel rule" nõue, siis kasutab autor töös läbivalt inglisekeelset väljendit.
[57] Financial Action Task Force. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. (2012, updated 2023) – https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html (01.03.2023), lk 78.

käsitleb autor järgnevalt „travel rule“ nõuet osas, mis puudutab virtuaalvääringu ülekandeid VASPi ja teise kohustatud isiku vahel.

Virtuaalvääringute piiriüleste ülekannete puhul tuleb ülekande algataja VASPil koguda, talletada ja edastada ülekande saaja VASPile või muule kohustatud isikule: 1) ülekande algataja täisnimi; 2) ülekande algataja kontonumber (virtuaalvääringute ülekandmisel virtuaalvääringu rahakoti aadress), kust ülekanne tehakse; 3) ülekande algataja aadress või riiklik isikukood või kliendi identifitseerimisnumber või sünnikuupäev ja -koht. Eelnimetatud andmed peavad olema ka ülekande algataja VASPi poolt kontrollitud. Andmete kogumine ja kontrollimine peab olema eelnevalt tehtud kliendisuhte loomisel. Lisaks eelnevale tuleb koguda ja edastada vastaspoolele ülekande saaja nimi ja kontonumber (virtuaalvääringute ülekandmisel virtuaalvääringu rahakoti aadress), kuhu ülekanne tehakse. Ülekande saaja nime on vaja skriinimiseks, et välja selgitada, kas tegemist on sanktsioneeritud isikuga või mitte ning selleks, et monitoorida, kas vastava isikuga on seotud rahapesu või terrorismi rahastamise kahtlaseid tehinguid.[58]

Ülekande saaja VASP peab aga saama ja talletama ülekande algataja VASPilt: 1) ülekande algataja nime, mida tuleb kasutada kahtlaste tehingute monitoorimiseks ja skriinimiseks, et kontrollida, kas tegemist on sanktsioneeritud isikuga; 2) ülekande algataja kontonumbri (virtuaalvääringute ülekandmisel virtuaalvääringu rahakoti aadress), kust ülekanne tehakse; 3) ülekande algataja aadressi või riikliku isikukoodi või kliendi identifitseerimisnumbri või sünnikuupäeva ja -koha; 4) ülekande saaja täisnimi; 5) ülekande saaja kontonumber (virtuaalvääringute ülekandmisel virtuaalvääringu rahakoti aadress), kuhu ülekanne tehakse. Samuti tuleb kinnitada, kas ülekande algataja VASPi poolt saadetud ülekande saaja nimi ja kontonumber/virtuaalvääringu rahakoti aadress ühtivad ülekande saaja VASPi poolt kontrollitud kliendiandmetega.[59]

Riigisiseste virtuaalvääringute ülekannete puhul tuleb ülekande algataja kohta koguda, talletada ja edastada ülekande saaja VASPile sama teave, mis piiriüleste tehingute korral. Küll aga ei ole nõutud vastaspoole nime, vaid üksnes ülekande saaja kontonumbrit (virtuaalvääringute ülekandmisel virtuaalvääringu rahakoti aadressi) või tehingu kordumatut tunnust, mis võimaldab tehingut jälgida tehingu algatajast ülekande saajani.[60]

[58] Financial Action Task Force. Updated Guidance 2021, lk 57-58.
[59] Financial Action Task Force. Updated Guidance 2021, lk 58.
[60] Financial Action Task Force Standards, lk 79.

Eesti seadusandja on kehtestanud „travel rule“ nõude 2022. aasta märtsis. RahaPTS § 25 lg 2^4 järgi tuleb ülekande algataja kohta koguda tema nimi, tehingu kordumatu tunnus, maksekonto või virtuaalvääringu rahakoti identifikaator, isikut tõendava dokumendi nimetus ja number ning isikukood või sünniaeg, sünnikoht ja elukoha aadress. Ülekande saaja kohta tuleb RahaPTS § 25 lg 2^5 koguda tehingu kordumatu tunnuse andmed ning maksekonto või virtuaalvääringu rahakoti identifikaatori andmed. Täiendavalt tuleb eelnimetatud andmed edastada viivitamata ja turvaliselt ülekande saaja VASPile või saaja krediidi- või finantseerimisasutusele. Samuti on reguleeritud RahaPTS § 47 lg-s 5^1 „travel rule“ nõude täitmisega seonduvate dokumentide, nende koopiate ja andmete säilitamine.

Eelnevast tulenevalt selgub, et RahaPTS-i on „travel rule“ nõue üle võetud üksnes osas, mis kohaldub siseriiklikele virtuaalvääringute ülekannetele. RahaPTS-is puuduvad nõuded, mis FATFi standardi järgi kohalduvad piiriülestele virtuaalvääringute ülekannetele. Eelkõige on puudulik ülekande saaja kohta kogutava teabe koosseis ja kehtestamata ülekande saaja VASPi kohustused. Piiriülestele tehingutele kehtivate nõuete kehtestamine on vajalik, kuna FATFi täiendavate juhiste kohaselt peaksid riigid, tulenevalt virtuaalvääringu piiriülesest levikust ja VASPide piiriülese teenuse osutamisest, käsitlema kõiki virtuaalvääringu ülekandeid (sh riigisiseseid) piiriüleste ülekannetena.[61] Samuti ei ole eluliselt usutav, et kõik virtuaalvääringu tehingud toimuvad Eestis riigisiseselt, et saaks piirduda riigisiseste virtuaalvääringu ülekannetele kohalduvate nõuetega.

Kehtiva regulatsiooni kohaselt tuleb ülekande saaja kohta koguda tehingu kordumatu tunnuse andmed ning maksekonto või virtuaalvääringu rahakoti identifikaatori andmed. Tehingu kordumatu tunnus on RahaPTS § 25 lg 2^6 järgi tähtede, numbrite või sümbolite kombinatsioon, mis võimaldab tehingut jälgida tehingu algatajast ülekande saajani. Nagu eelnevas peatükis selgitatud, siis ka virtuaalvääringu rahakoti identifikaator ehk aadress on numbrite ja tähtede kombinatsioon. Plokiahelast on võimalik näha, milliste virtuaalvääringu rahakoti aadresside vahel on tehingud toimunud. Seega mõlemad ülekande saaja kohta kogutavad andmed võimaldavad jälgida virtuaalvääringu liikumist ühest virtuaalvääringu rahakotist teise, aga ei hõlma andmeid, mille abil tuvastada, kes on konkreetne ülekande saaja isik. Tehingu kordumatu tunnus ega virtuaalvääringu rahakoti aadress ei sisalda isikuandmeid. See tähendab, et ülekande saaja isik on nende andmete kogumisel jätkuvalt tuvastamata.

[61] Financial Action Task Force. Updated Guidance 2021, lk 56.

RahaPTS § 42 lg 3 kohaselt ei tohi VASPid kliendi maksejuhist täita või rahalisi vahendeid või virtuaalvääringuid kättesaadavaks teha, kui VASP ei suuda täita RahaPTS §-s 25 sätestatud kohustusi. Kuna RahaPTS § 25 lg 2^5 järgi tuleb VASPil koguda ülekande saaja kohta üksnes tehingu kordumatu tunnus ja virtuaalvääringu rahakoti aadress, mis ei hõlma ülekande saaja isikut tuvastavaid andmeid, siis on kehtiva regulatsiooni kohaselt võimalik teha tehinguid tuvastamata isikutega. Seega on rahapesu ja terrorismi rahastamise riskid maandamata osas, mis puudutab vastaspoole tuvastamist, kuna kohustatud isikud võivad teadmatult teha tehinguid sanktsioneeritud isikutega, sh rahapesijate ja terrorismi rahastajatega.

Autori hinnangul tuleb vastava riski maandamiseks ehk vastaspoole tuvastamiseks lähtuda FATFi piiriüleste tehingute standardist ja täiendada RahaPTSi osas, mis puudutab ülekande saaja täisnime kogumist ja edastamist ning vastaspoole VASPi kohustust kontrollida ja kinnitada edastatud teabe õigsus. RahaPTSi kooskõlla viimiseks FATFi standarditega tuleb RahaPTSi täiendada nii, et ülekande algataja VASP kogub lisaks praegu nõutud andmetele ka ülekande saaja täisnime. Ülekande saaja nime teatab VASPile klient, kes soovib ülekande saajale virtuaalvääringuid saata. Vastavalt kehtivale regulatsioonile tuleb kogutud info saata ülekande saaja VASPile. Kui siinkohal lõppeb kehtiva regulatsiooni kohaselt infovahetus, siis autori hinnangul tuleb ülekande saaja kohta kogutud teabe õigsuse kontrollimiseks kehtestada ka ülekande saaja VASPile teabe õigsuse kinnitamise kohustus. Ülekande saaja VASP peab kinnitama, kas ülekande algataja VASPi poolt saadetud teave ülekande saaja kohta ühtib ülekande saaja VASPi poolt kontrollitud kliendiandmetega. Teisisõnu, tuleb ülekande saaja VASPil kontrollida, kas kliendibaasis on saadetud nime ja virtuaalvääringu rahakoti aadressiga isik. Ka RABi 2022. aastal avaldatud aastaraamatus on rõhutatud, et VASP on isik, kes saab anda infot tema teenuseid kasutava kliendi kohta ning seeläbi jõuda virtuaalvääringu rahakoti aadressi omanikuni.[62] Saanud kinnituse, et ülekande saaja kohta kogutud andmed ühtivad, on ülekande algataja VASPil kohustus kontrollida, kas tegemist on sanktsioneeritud isikuga. Kui isik on rahvusvahelise sanktsiooni subjekt, on ülekande tegemine keelatud. Avalikud andmebaasid sanktsioneeritud isikutest hõlmavad ka rahapesijaid ja terrorismi rahastajaid, mistõttu tõkestatakse sanktsioneeritud isikute rahaliste vahendite/virtuaalvääringute kasutamise ja käsutamise piiramise kaudu ka rahapesu ja terrorismi rahastamist.

[62] Rahapesu Andmebüroo aastaraamat 2021, lk 34.

RahaPTSi täiendamine osas, mis puudutab ülekande saaja täisnime kogumist ja edastamist ning vastaspoole VASPi kohustust kinnitada edastatud teabe õigsus, täidab eesmärki maandada rahapesu ja terrorismi riski. Nimelt on vastaspoole tuvastamine vajalik, et kontrollida, kas vastaspool on sanktsioneeritud isik, et vältida tehingute tegemist isikutega, kes on seotud rahapesu ja terrorismi rahastamisega ning tõkestada neil finantssüsteemi sisenemist VASPide kaudu. Samuti tõhustab see uurimis- ja järelevalvemenetlust, kui VASPil on teada tehingu mõlemad pooled. Ülekande saaja isiku tuvastamata jätmine raskendab uurimis- ja järelevalveasutustel rahapesu või terrorismi rahastamisega seotud isikute vastutusele võtmist.

Kuna „travel rule" nõude kohaldamisel kogutakse, talletatakse ja saadetakse erinevate osapoolte vahel isikuandmeid, siis on oluline, et osapooled lähtuksid isikuandmete kaitse nõuetest. RahaPTS § 25 lg 2^7 kohaselt tuleb andmed saata viivitamata ja turvaliselt saaja virtuaalvääringu teenuse pakkujale. RahaPTS 507 SE seletuskirja[63] järgi on andmed edastatud turvaliselt, kui on tagatud, et edastatavaid andmeid ei avalikustata lubamatult. Autori hinnangul tuleks praktika ühtlustamise eesmärgil sätestada täpsemad nõuded „travel rule" nõudes sätestatud teabe vahetamise kohta. Nimelt tuleb FATF juhiste kohaselt enne teabe saatmist läbida 3-etapiline protsess: 1) tuvastamine, kas ülekande saaja virtuaalvääringu rahakoti hoidja on VASP või on tegu *unhosted wallet*'it kasutava isikuga; 2) ülekande saaja VASPi tuvastamine; 3) hoolsuskontrolli kohaldamine ülekande saaja VASPile. Alles siis, kui on selge, et vastaspoolel on VASP, kes on läbinud hoolsuskontrolli, on teabe saatmine turvaline ja lubatud.[64]

Esimeses etapis tuleb kindlaks teha, kas vastaspoolel on *unhosted wallet*'it kasutav isik või on ülekande saaja rahakoti hoidjaks VASP. *Unhosted wallet*'i korral tuleb kohaldada „travel rule" nõuet erisustega, mida käsitleb autor lähemalt peatükis 1.3. Kui on tuvastatud, et vastaspoolel on VASP, tuleb teises etapis kindlaks teha, millise konkreetse VASPiga on tegu. Selleks on välja töötatud plokiahela analüüsimise meetodid, mille abil on võimalik tuvastada, kas tehing toimub teise VASPiga ja millisega konkreetselt. Vastavat tuvastamise teenust pakuvad kohustatud isikutele näiteks Chainalysis ja Elliptic. Kolmandas etapis tuleb vastaspoole VASPile teha

[63] Rahapesu ja terrorismi rahastamise tõkestamise seaduse ja teiste seaduste muutmise seadus 507 SE. Eelnõu. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/ffe848a6-7b78-43cf-b106-720915882205/rahapesu-ja-terrorismi-rahastamise-tokestamise-seaduse-ja-teiste-seaduste-muutmise-seadus (25.03.2023); Rahapesu ja terrorismi rahastamise tõkestamise seaduse ja teiste seaduste muutmise seadus 507 SE. Seletuskiri. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/ffe848a6-7b78-43cf-b106-720915882205/rahapesu-ja-terrorismi-rahastamise-tokestamise-seaduse-ja-teiste-seaduste-muutmise-seadus (25.03.2023).
[64] Financial Action Task Force. Updated Guidance 2021, lk-d 62-63.

hoolsuskontroll, et veenduda, kas tegemist on usaldusväärse osapoolega, kellele teave saata.[65] Hoolsuskontrolli raames tuvastatakse muuhulgas, kas VASPil on kehtiv tegevusluba, kas VASP järgib „travel rule" nõuet ja andmekaitsenõudeid. Hoolsuskontrolli läbi viimiseks on Global Digital Finance (GDF) rahapesu tõkestamise töökond välja töötanud „travel rule" nõude täitmiseks hoolsuskontrolli küsimustiku.[66]

Kui kõik kolm etappi on läbitud ehk tuvastatud on vastaspoolena VASP, kes on identifitseeritud ja kes on läbinud hoolsuskontrolli, võib vastaspoole VASPile saata teabe nii ülekande algataja kui ka saaja kohta. Saanud vastaspoole VASPilt kinnituse ülekande saaja andmete õiguse kohta, võib vastaspoole kliendi tuvastamisel ka virtuaalvääringu ülekandeid teha. Kui vastaspoole VASP on kord hoolsuskontrolli läbinud, ei ole selle uuesti rakendamine sama VASPi puhul vajalik, v. a kui ilmneb (nt negatiivsest meediakajastusest või järelevalveasutuse avaldatud teatest), et konkreetne VASP ei ole enam usaldusväärne osapool.[67] RahaPTSi täiendamine vastaspoole VASPi tuvastamise ja hoolsuskontrolli rakendamise osas täidab autori hinnangul lisaks andmete kaitsmise tagamisele ka rahapesu ja terrorismi rahastamise maandamise eesmärki. Nimelt võib hoolsuskontrolli läbinud VASPi pidada usaldusväärseks isikuks, kellelt saadud teave ülekande saaja kohta aitab virtuaalvääringu rahakoti omanikku tuvastada ja vajalikke rahapesu ja terrorismi rahastamise tõkestamise meetmeteid kasutada.

Eelnevast tulenevalt tuleb autori hinnangul piiriüleste tehingutega kaasnevate rahapesu ja terrorismi rahastamise riskide tõhusamaks maandamiseks täiendada kehtivat regulatsiooni järgnevalt: 1) Täiendada RahaPTS § 25 lg-t 2^5 nõudega koguda ülekande saaja kohta täisnimi; 2) Lisada RahaPTS §-i 25 kohustus ülekande saaja VASPil kontrollida ja kinnitada ülekande algataja VASPi poolt saadetud teave ülekande saaja kohta; 3) Täiendada RahaPTS § 25 lg-t 2^7 ülekande algataja VASPi kohustusega tuvastada ja kohaldada ülekande saaja VASPile hoolsuskontrolli.

[65] *Ibid.*
[66] NotaBene. Due Diligence Questionnaire for Travel Rule Data Sharing. (2022) – https://app.hubspot.com/documents/7222759/view/277011207?accessId=877505 (01.03.2023).
[67] Financial Action Task Force. Updated Guidance 2021, lk 62.

1.4. Kohustatud isiku puudumine

Aasta 2022 Euroopa Komisjoni riikideüleses riskihinnangus, FATFi juhistes, Rahapesu Andmebüroo uuringutes ja Euroopa Parlamendi uuringus, milles käsitleti virtuaalvääringute kasutamisest terrorismis, on välja toodud, et rahapesu ja terrorismi rahastamise riskiks on kohustatud isiku puudumine detsentraliseeritud virtuaalvääringu teenuses, isikult isikule (ingl *P2P*) virtuaalvääringuga tehingute tegemises ja *unhosted wallet'*ite loomisel.

Detsentraliseeritud rahandus (ingl *decentralized finance = DeFi)* on süsteem, kus traditsiooniliste vahendajate, näiteks pankade ja finantseerimisasutuste roll on automatiseeritud. Detsentraliseeritud süsteem põhineb nutilepingutel ehk programmeerimiskoodil, kuhu on kirjutatud tehingu täitmise tingimused. Kui tarkvarakood tuvastab, et nutilepingusse kodeeritud tingimused on täidetud, toimub automaatselt tehingu täitmine. Vastavat süsteemi kasutatakse ka detsentraliseeritud virtuaalvääringu vahetusplatvormidel. Tehingu osapooltel on võimalus oma virtuaalvääringu rahakotid ühendada platvormiga, seejärel leida platvormilt sobiv osapool, kellega virtuaalvääringuid vahetada ja sõlmida isikult isikule tehingute tegemiseks nutilepingud. Seejuures antakse nutilepingut sõlmides tahteavaldused, et kokkulepitud tingimuste täitumisel toimub lepingu automaatne täitmine. Finantsinspektsioon on selgitanud, et kuna detsentraliseeritud vahetusplatvormide puhul juhib kogu süsteemi programmeerimiskood, mitte füüsiline või juriidiline isik, siis puudub justkui keskne isik, kellele rahapesu ja terrorismi rahastamise tõkestamise nõuded kohalduksid.[68]

Eelnevast tulenevalt esineb risk, et reguleerimata detsentraliseeritud virtuaalvääringu vahetusplatvorme kasutatakse rahapesuks ja terrorismi rahastamiseks, kuna need ei kohalda klientide suhtes hoolsusmeetmeid ning kurjategijatel on seetõttu platvormi kasutamisel võimalik jääda anonüümseks. Detsentraliseeritud teenuste kasutajate arv on viimaste aastate jooksul kasvanud väga kiiresti. Kui aastal 2020 oli kasutajaid ligi 100 000, siis 2023. aasta alguseks oli kasutajaid ligi 6,7 miljonit.[69] Kasutajate arvu suurenemisega on tõusnud ka detsentraliseeritud teenuste kasutamine rahapesu eesmärgil.[70] Aastal 2021 kasutasid Põhja-Korea häkkerid

[68] Finantsinspektsioon. DeFi. (2022) – https://www.fi.ee/et/finantsinspektsioon/innovatsioonikeskus/defi (09.03.2023).
[69] Statista. Daily number of DeFi users worldwide up until January 9, 2023. (2023) – https://www.statista.com/statistics/1297745/defi-user-number/ (03.03.2023).
[70] Chainanalysis. The 2023 Crypto Crime Report (2023, lk 45) – https://blockbr.com.br/wp-content/uploads/2022/06/2022-crypto-crime-report.pdf (03.03.2023).

detsentraliseeritud virtuaalvääringu vahetusplatvorme, kus isikutuvastamise nõudeid ei rakendatud, et pesta häkkimise tulemusel saadud krüptovääringut, mille väärtus küündis ligi 2,8 miljoni euroni.[71] Kuna detsentraliseeritud virtuaalvääringu teenuste kasutajate arv, sealhulgas nende arv, kes kasutavad platvormi rahapesuks, on aasta-aastalt jõudsalt tõusmas, siis on oluline laiendada rahapesu ja terrorismi rahastamise tõkestamise regulatsiooni kohaldumisala ka detsentraliseeritud teenustele.

Järgnevalt selgitab autor välja, kas ja kuidas on detsentraliseeritud teenustega seonduv rahapesu ja terrorismi rahastamise risk Eesti regulatsioonis maandatud. RahaPTS-is ei ole detsentraliseeritud teenuseid sõnaselgelt reguleeritud. Küll aga on RahaPTS 507 SE seletuskirja[72] kohaselt VASPideks ka need isikud, kes pakuvad teenust detsentraliseeritult või kui ülesanded, mis seonduvad teenuse pakkumisega on jaotatud mitme isiku vahel. Seletuskirjast selgub, et üldjuhul on detsentraliseeritud teenuste puhul olemas isikud, kes on osalenud teenuse kujundamises või kellel on teenuse üle mõju või kontroll. Isikuteks, keda saab detsentraliseeritud teenuse puhul pidada VASPiks on näiteks: 1) virtuaalvääringu loomises või kasutatava rakenduse või kasutaja liidese arendamises osalejad, kes omavad mõju pakutava teenuse üle; 2) isik, kel on administratiivvõti[73]; 3) isik, kes kogub teenuse kasutajatelt tasu; 4) loojad, omanikud, haldajad ja muud isikud, kes omavad mõju või kontrolli teenuse tingimuste või muude parameetrite üle. Samuti tuleb hinnata, kas teenuse kasutajate ning keskkonna loojate, omanike, haldajate või muude teenusega seonduvate isikute vahel on ärisuhe, mis võib olla loodud ka nutilepingutega.

Seletuskirjas on loetletud ka isikud, keda VASPiks ei loeta. Näiteks ei ole kohustuslikuks isikuks teenuse rakendus ise. Rahapesu ja terrorismi rahastamise tõkestamise nõuded ei kohaldu ka isikutele, kes pakuvad kõrvalteenuseid ega kujunda oma tegevusega virtuaalvääringu teenuse tingimusi ega paku aktiivselt virtuaalvääringu teenust ning ei tee ühtegi tegevust virtuaalvääringu teenuse raames virtuaalvääringu teenust kasutava kliendi nimel. Nendeks on näiteks võrguteenused, valideerimisteenused, internetiteenused, pilveteenused, serverid ja muud VASPile osutatavad riistvara või tarkvara teenused. Samuti on kirjeldatud, et VASPiks ei pruugi olla tarkvara rakendust või virtuaalvääringu pakkumiseks ja/või kauplemiseks platvormi loov ja/või müüv isik, kui tegevus piirdubki üksnes rakenduse ja/või platvormi loomise ja/või müümisega.

[71] *Ibid*, lk 13.
[72] RahaPTS 507 SE seletuskiri, lk 7.
[73] Administratiivvõti annab juurdepääsu muu hulgas nutilepingu tingimuste muutmisele.

Autor nõustub Eesti seadusandja lähenemisega välistada detsentraliseeritud teenuse rakendus kohustatud isikute seast, olenemata sellest, et rakendust kasutatakse rahapesuks ja terrorismi rahastamiseks. Detsentraliseeritud rakenduse näol on tegemist arvutiprogrammiga, mis on õiguskirjanduse kohaselt „mõttetegevuse tagajärjel tekkinud immateriaalne hüve“.[74] Tegemist on TsÜS § 48 mõistes esemega, täpsemalt hüvega, mis on õiguse objektiks. Arvutiprogrammi kui intellektuaalset omandit kaitstakse AutÕS § 4 lg 3 p-i 3 alusel autoriõigusega. Kuna subjektiivsete õiguste ja juriidiliste kohustuste kandjateks saavad olla üksnes õiguse subjektid, kelleks on füüsilised ja juriidilised isikud[75], siis ei saa arvutiprogrammi pidada VASP-iks, kellele rahapesu ja terrorismi rahastamise tõkestamise kohustusi kehtestada.

FATFi juhiste kohaselt võivad VASPideks olla loojad, omanikud, haldajad ja muud isikud, kellel on kontroll või mõju detsentraliseeritud virtuaalvääringu teenuse üle ja kui nad osutavad virtuaalvääringu teenust või aitavad aktiivselt sellele kaasa. Näiteks võib olla mõju või kontroll varade või teenuse üle. VASPiks võib olla isik, kes saab teenusest kasu või kes saab määrata või muuta tehingu tingimusi ja parameetreid.[76] Seega on RahaPTS kooskõlas FATFi juhistega. Autor nõustub ka siinkohal Eesti seadusandja lähenemisega välistada kohustatud isikute seast kõrvalteenuse pakkujad, kellel puudub mõju ja kontroll teenuse üle. Olukord, kus kohustatud isikuks määratakse isik, kel puudub kontroll kliendisuhete ja teenuse üle, ei täida rahapesu ja terrorismi rahastamise tõkestamise eesmärki.

Samuti nõustub autor, et VASPiks ei peaks pidama isikuid, kelle tegevus piirdub üksnes rakenduse ja/või platvormi loomise ja/või müümisega. Loomisega piirdumisel ei pakuta platvormi või rakenduse kaudu virtuaalvääringu teenuseid, mistõttu ei esine rahapesu ega terrorismi rahastamise riske, mis vajavad maandamist. Müümisega piirdumisel antakse aga intellektuaalomandi õigused üle ostjale ja isiku mõju ja kontroll rakenduse/platvormi üle katkeb, mistõttu eelnevale omanikule kohustuste kehtestamine ei täidaks rahapesu ja terrorismi rahastamise maandamise eesmärki.

Lähtudes asjaolust, et detsentraliseeritud platvormide puhul on reeglina praktikas tuvastatavad isikud, kes peavad vastutama rahapesu ja terrorismi rahastamise tõkestamise eest ning Finantsinspektsiooni seisukohast, et puhtal kujul detsentraliseeritud lahendus, kus vastutav isik

[74] Varul, P. jt (koost). TsÜS § 49, p 3.1.3. – Tsiviilseadustiku üldosa seadus. Komm vlj. Tallinn: Juura 2010.
[75] Narits, R. Õiguse entsüklopeedia. Tallinn: Juura 2002, lk 124.
[76] Financial Action Task Force. Updated Guidance 2021, lk 27.

puudub, on praegu pigem teoreetiline kontseptsioon[77], on autor seisukohal, et detsentraliseeritud teenusega seonduvad riskid on kehtiva regulatsiooni kohaselt maandatud, kuna vastava teenuse pakkujad peavad kohaldama rahapesu ja terrorismi rahastamise tõkestamise meetmeid.

Kohustatud isik puudub ka juhul, kui isik loob ilma teenusepakkujata virtuaalvääringu rahakoti ehk *unhosted wallet*'i. Isik saab avalikult ja tasuta kättesaadava tarkvara abil genereerida virtuaalvääringu rahakoti aadressi, privaatse võtme ja avaliku võtme ning talletada neid näiteks enda arvutis, telefonis või paberil. *Unhosted wallet*'i loomisel ei tule läbida hoolsusmeetmete protsessi, mistõttu on isikul võimalik teha tehinguid anonüümse rahakotiga. Eksisteerib risk, et rahakotte kasutatakse rahapesuks ja terrorismi rahastamiseks. Aastal 2022 arreteeriti USA-s abielupaar, keda süüdistati 4,5 miljardi dollari väärtuses pettuse teel saadud Bitcoinide rahapesus. Keeruline rahapesuskeem hõlmas ka *unhosted wallet'*ite kasutamist.[78] Seega esineb vajadus *unhosted wallet'*itega tehtavate tehingute reguleerimise järele. Järgnevalt selgitab autor välja, kas ja kuidas on *unhosted walleti'*ga tehtavate tehingutega seonduv rahapesu ja terrorismi rahastamise risk Eesti regulatsioonides maandatud.

RahaPTS 507 SE seletuskirja[79] kohaselt tuleb tehingute puhul, mil kasutatakse *unhosted wallet*'it kohaldada alternatiivset lahendust „*travel rule*" nõudele. Selleks on RahaPTS § 25 lg-s 2[8] sätestatud reegel, mille järgi peab tehingu algataja VASP tagama tehingute jälgimise reaalajas ja iga tehingu riskianalüüsi ning säilitama „travel rule" nõudes loetletud andmed viisil, mis võimaldab need järelevalve- või uurimisasutusele vastavasisulise päringu korral viivitamata esitada.

Vastav regulatsioon kattub suurel määral FATFi kehtestatud standarditega. Nimelt teadvustab FATF, et virtuaalvääringu ülekande tegemisel ei pruugi mõlemal poolel kohustatud isikut olla. Näiteks juhul, kui klient kasutab VASPi teenust, aga ta soovib virtuaalvääringu ülekande teha *unhosted wallet'*i omanikule või *unhosted wallet'*i omanik soovib teha ülekande VASPi kliendile. 2021. aasta oktoobris laiendas FATF „travel rule" nõude kohaldumist ka tehingutele, mille üks

[77] Finantsinspektsioon. DeFi. (2022) – https://www.fi.ee/et/finantsinspektsioon/innovatsioonikeskus/defi (09.03.2023).
[78] D'Aversa, A. A Record $3.6 Billion Seizure and the Twisting Paths of Money Laundering in the Digital World. (2022) – https://www.moneylaunderingnews.com/2022/02/a-record-3-6-billion-seizure-and-the-twisting-paths-of-money-laundering-in-the-digital-world/ (03.03.2023).
[79] RahaPTS 507 SE seletuskiri, lk 12.

osapool on *unhosted walleti'*ti omanik. Sel juhul tuleb jätkuvalt järgida „travel rule" nõuet, aga erisustega, mis võtavad arvesse, et teisel pool pole kohustatud isikut.[80]

FATFi juhiste kohaselt tuleb ka sel juhul, kui vastaspooleks on *unhosted wallet*' i omanik, koguda identifitseerivat teavet kliendi ja vastaspoole kohta, aga seda ei saadeta vastaspoolele, kuna puudub usaldusväärne kohustuslik isik, kellega teavet jagada ja vahetada. *Unhosted wallet*'i omanikku identifitseerivat teavet ehk tema virtuaalvääringu rahakoti aadressi ja täisnime, tuleb küsida ülekande algatajalt ehk VASPi enda kliendilt. Kui klient vastaspoole isiku kohta infot ei oma, on tehingu tegemine keelatud. Juhul, kui klient omab piisavat teavet vastaspoole tuvastamiseks, saab seda kasutada vastaspoole skriinimiseks, et tuvastada, kas tegemist on sanktsioneeritud isikuga, millest tulenevalt ei ole tehingu tegemine lubatud.

Autori hinnangul ei saa piirduda üksnes kliendi antud infoga, kuna klient ei ole usaldusväärne ja erapooletu allikas. Näiteks juhul, kui klient soovib virtuaalvääringuid teisele isikule üle kanda rahapesu või terrorismi rahastamise eesmärgil, võib ta väita, et virtuaalvääringu rahakoti aadressi omanikuks on isik, kes seda tegelikult ei ole. Seda eesmärgiga varjata tegelikku teist osapoolt. Seega tuleks kliendi antud infot ka kontrollida. *Unhosted wallet*'i omaniku kohta teabe kogumise ja kontrollimise kohustus on kehtestatud ka Saksamaal[81] ja Singapuris[82]. Kuna puudub ülemaailmne register, mis sisaldab kõikide virtuaalvääringu rahakottide aadresse ja infot nende omanike kohta ning puudub ka vastaspoole kohustatud isik, kellelt saada teavet rahakoti omaniku kohta, siis ainukeseks võimaluseks on kliendilt saadud infot kontrollida väidetava rahakoti omaniku käest. Otsekontakti loomiseks tuleb ülekande saaja VASPil koguda vastaspoole kohta ka näiteks telefoninumber ja/või elektronposti aadress. Ülekande saaja kontrolli virtuaalvääringu rahakoti üle on võimalik tuvastada näiteks paludes vastaspoolel teha kontrollmakse VASPi

[80] Financial Action Task Force. Updated Guidance 2021, lk 65.
[81] Verordnung über verstärkte Sorgfaltspflichten bei dem Transfer von Kryptowerten (Kryptowertetransferverordnung –KryptoWTransferV, § 4 lg 3). Bundesgesetzblatt Jahrgang 2021 Teil I Nr. 69, ausgegeben zu Bonn am 29. September 2021. – https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-09-29-KryptoWTransferV/3-Verkuendete-Verordnung.pdf?__blob=publicationFile&v=4 (24.03.2023).
[82] Monetary Authority of Singapore. Guidelines to MAS Notice PS-N02 on Prevention of Money Laundering and Countering the Financing of Terrorism. (2020, lk-d 41-42) – https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Guidelines--to--Notice-PSN02-on-Prevention-of-ML-and-Countering-the-Financing-of-Terrorism.pdf (24.03.2023).

määratud summas. Tuvastanud *unhosted wallet*'i omaniku ja teostanud skriiningu, võib VASP lubada ülekannete tegemist kliendi ja *unhosted wallet*'i omaniku vahel.

Seega *unhosted wallet*'itega seonduva riski maandamiseks tuleb täiendada regulatsiooni osas, mis puudutab kliendilt vastaspoole täisnime ja kontaktandmete kogumist ning *unhosted wallet*'i omaniku tuvastamist. Vastaspoole tuvastamine maandab rahapesu ja terrorismi rahastamise riske varasemalt käsitletud sanktsioneeritud isiku skriinimise, tehingute monitoorimise ning uurimis- ja järelevalvemenetluse tõhustamise kaudu.

2. Hoolsus- ja teatamiskohustuse täitmine virtuaalvääringu teenuste riskide maandamisel

2.1. Virtuaalvääringu teenuse pakkujate hoolsusmeetmete täitmine riskide maandamisel

Virtuaalvääringutega seotud rahapesu ja terrorismi rahastamise tõkestamiseks tuleb riigil kehtestada riske maandav õigusraamistik, ent sellest üksi ei piisa. Rahapesu ja terrorismi rahastamise riskide maandamiseks on oluline, et kohustatud isikud ka kehtestatud nõudeid praktikas täidaksid. Eesti siseriiklikus riskihinnangus, RABi 2022. aasta aastaraamatus ja virtuaalvääringu teenuse pakkujate uuringutes on rõhutatud, et VASPide sektoris on puudujääke hoolsusmeetmete rakendamisel. Eelkõige on probleeme nõuetekohase isikusamasuse tuvastamise ja ärisuhte seirega. Praktikas tekkinud olukord, kus hoolsuskohustusi ei täideta piisavalt, tõstatab küsimuse õigusliku reguleerimise kohasusest ja vastavusest.

Isikusamasuse tuvastamine ning esitatud teabe kontrollimine on üks kliendisuhte loomisel rakendatavatest hoolsusmeetmetest, mille eesmärk on kindlaks teha kliendi, tema esindaja või tegeliku kasusaaja isik. Isikuandmete abil kontrollitakse isiku tausta ning kui vastava isiku suhtes tekib rahapesu või terrorismi rahastamise kahtlus, mida ei ole võimalik tugevdatud hoolsusmeetmete käigus kõrvaldada, tuleb riskide maandamiseks keelduda ärisuhte loomisest ja teavitada sellest RABi.[83] Vastavalt peatükis 1.2. analüüsitule, on isikusamasuse tuvastamine oluline hoolsusmeede ka virtuaalvääringu anonüümsusest tuleneva riski maandamiseks, kuna see võimaldab anonüümse virtuaalvääringu rahakoti aadressi siduda konkreetse isikuga ning seeläbi on võimalik seirata plokiahelas toimuvaid isikuga seotud tehinguid. Samuti kasutatakse isiku kohta kogutud andmeid, et määrata kliendile riskiaste, millest oleneb, kas isiku ja tema tegevuse suhtes tuleb kohaldada lisaks tavapärastele meetmetele ka tugevdatud hoolsusmeetmeid ja kõrgendatud tähelepanu. Näiteks olukorras, kus kohustatud isik tuvastab, et klient, tema esindaja või tegelik kasusaaja on kõrge riskiga riikliku taustaga isik, tuleb isikule määrata kõrge riskiaste ja kohaldada muu hulgas tugevdatud korras ärisuhte seiret.[84] Kuna isikusamasuse tuvastamine on oluline osa otsustamisel, kas isikuga kliendisuhet luua, tehingut teha või milline on edasine ärisuhte

[83] Rahapesu Andmebüroo. Juhend kahtlaste tehingute tunnuste kohta. (2022, lk 2) – https://fiu.ee/oigusaktid-ja-juhendid/juhendid#juhend-kahtlaste-teh (04.03.2023).
[84] Rahapesu Andmebüroo riskide juhtimise juhend 2022, lk 39.

hoolsusmeetmete kohaldamise ulatus ja viis, siis on tegemist ühe peamise rahapesu ja terrorismi rahastamise tõkestamise meetmega.

RABi järelevalvetoimingute käigus on selgunud, et suur osa VASPidest ei teosta isikusamasuse tuvastamist ja esitatud teabe kontrollimist nõuetekohaselt. Isikusamasuse tuvastamine toimub RahaPTS § 21 lg-s 3 nimetatud dokumentide alusel, aga VASPid on selle kohustuse vastu sageli eksinud. Tuvastatud on juhtumeid, kus VASPid aktsepteerivad isikusamasuse tuvastamisel dokumente, mis ei vasta nõuetele või kus isikut tõendav dokument jäetakse üldse küsimata.[85] Samuti on esinenud olukordi, kus VASP peab rakendama täiendavaid hoolsusmeetmeid ja nõudma lisadokumentide esitamist, ent tegelikkuses piirdutakse ainult ühe esitatud dokumendiga.[86] RABi aastaraamatus on kirjeldatud kaasust, kus RAB teostas Garantex Europe OÜ kui Eesti ühe suurima VASPi juures kohapealset kontrolli ning tuvastas, et üle 90% klientide puhul oli rikutud isikusamasuse tuvastamise kohustust. Samuti täheldati järelevalvemenetluse käigus, et mõne päeva jooksul registreeriti märkimisväärselt palju uusi kasutajaid, mis viitas asjaolule, et VASP ei teostanud klientide taustakontrolli.[87] Kuigi RahaPTS-is on sätestatud isikusamasuse tuvastamise nõuded, siis praktikas on turuosalistel vastava kohustuse täitmisega raskusi. See tähendab, et rahapesijate ja terrorismi rahastajate pääsemine finantssüsteemi virtuaalvääringu teenuse pakkujate sektori kaudu ei ole VASPide poolt piisavalt takistatud.

Lisaks ärisuhte isikusamasuse tuvastamisele on VASPidel probleeme ka ärisuhte seirega**.** Ärisuhte seirel tuleb skriinimise ja monitoorimise abil jälgida kliendiga seotud tehinguid ja välja selgitada, kas tehingud on kooskõlas kliendi kohta eelnevalt kogutud teabega. Sealhulgas tuleb kohustatud isikul pöörata tähelepanu keerukate, ebatavaliste ja suure väärtusega tehingutele, millel puudub mõistlik või nähtav majanduslik eesmärk. Kohustatud isikul tuleb hinnata, kas kliendi tegevus viitab rahapesule või terrorismi rahastamisele.[88] Seire tulemusel saadud teabe põhjal otsustatakse, kas kliendi riskiaste vajab tõstmist ja seega ka kliendi suhtes täiendavate või tugevdatud hoolsusmeetmete kohaldamist. Samuti oleneb seire käigus saadud teabest RABi teavitamine ning tehingu tegemise ja kliendisuhte jätkamise võimalikkus. Kuna ärisuhte seire aitab eristada teistest finantssüsteemi sisenenud isikutest neid, kes tegelevad rahapesu ja terrorismi rahastamisega, mis

[85] Eesti riiklik riskihinnang 2021, lk 4.
[86] Rahapesu Andmebüroo 2020 uuring, lk 13.
[87] RAB aastaraamat 2022, lk 50.
[88] Rahapesu Andmebüroo riskide juhtimise juhend 2022, lk 44.

omakorda võimaldab vastavate isikute suhtes rakendada meetmeid, mis takistavad ebaseaduslikku tegevust, siis on ka ärisuhte seirel oluline roll rahapesu ja terrorismi rahastamise tõkestamisel.

RAB on järelevalvetoimingute käigus tuvastanud, et kuigi ärisuhte seiret tuleb kohaldada kõikide klientide puhul, on ettevõtete seas levinud valikuline seiramine, kas lähtuvalt ärisuhte riskiprofiilist või tehingulimiidist. Samuti on täheldatud, et seiramise nõudeid ei täideta nõuetekohaselt tugevdatud hoolsusmeetmete kohaldamise käigus. Nimelt tuleb hoolsusmeetmete tugevdatud korras kohaldada ärisuhte seiret tavapärasest sagedamini. See hõlmab muu hulgas kliendi riskiprofiili uuesti hindamist kuue kuu jooksul alates ärisuhte loomisest. Mitmed VASPid ei ole aga RABi sõnul riskiprofiili ettenähtud aja jooksul uuesti hinnanud.[89] Lisaks viitab puudulikule ärisuhte seirele asjaolu, et üksnes veerand Eesti VASPidest täitis aastal 2021 RABi teatamiskohustust. Märkimisväärne on, et enamik VASPe, kelle käive ulatub kümnetesse või sadadesse miljonitesse eurodesse, ei ole RABile esitanud ühtki teadet.[90] Pole eluliselt usutav, et nii suure käibega VASPidel ei ole äritegevuses ainsatki klienti, kelle ärisuhte skriinimise või monitoorimise käigus tekib rahapesu või terrorismi rahastamise kahtlus, mis vajab RABi teavitamist. Seega, lisaks tõdemusele, et VASPide sektoris esineb puudujääke terroristide ja rahapesijate finantssüsteemi sisenemise tõkestamisel, on kitsaskohaks ka ärisuhte seire puudulikkus. Seeläbi on praktikas suurel hulgal VASPidel tagamata virtuaalvääringu teenuse sektoris rahapesu ja terrorismi rahastamisega tegelevate isikute tuvastamine ja nende tegevuse tõkestamine.

Asjaolu, et turuosalised ei täida hoolsusmeetmeid või ei tee seda nõuetekohaselt, tekitab õigustatult küsimuse, et millest on tingitud VASPide puudulik tegevus või tegevusetus. Eesti riikliku riskihinnangu kohaselt on tegemist VASPide suutmatuse ja/või soovimatusega nõudeid täita.[91] VASPide suutmatus täita nõuetekohaselt hoolsusmeetmeid tuleneb RABi hinnangul mitmest asjaolust. Esiteks on põhjus tehniliste lahenduste ebapiisavuses: "Enamikul Eesti tegevusloaga virtuaalvääringu pakkujatest puuduvad tõhusad ja tegevusala spetsiifikat arvestavad seire- ja monitooringusüsteemid, mis võimaldaksid õigeaegselt rahapesu või terrorismi rahastamise kahtlusega tehinguid tuvastada."[92] Näiteks on ainult üksikutel VASPidel süsteemid, mis võimaldavad tuvastada plokiahelast segamistehinguid või mitmeid omavahel seotud tehinguid, mis

[89] Rahapesu Andmebüroo uuring 2020, lk-d 12-13.
[90] Rahapesu Andmebüroo uuring 2022, lk 24.
[91] Eesti riiklik riskihinnang 2021, lk 4.
[92] Rahapesu Andmebüroo uuring 2022, lk 5.

tervikuna tekitavad rahapesu või terrorismi rahastamise kahtluse. Seega enamikul Eesti VASPidel puuduvad tõhusad süsteemid, mille abil minimeerida riski, et VASPi kasutatakse rahapesuks või terrorismi rahastamiseks. Teiseks põhjuseks on RAB välja toonud VASPi töötajate madala teadmiste taseme. Nimelt ei ole töötajate teadmised piisavad kliendisuhte nõuetekohaseks loomiseks või sellest keeldumiseks ning kliendiga seotud tehingute seiramiseks. Näiteks on selgunud, et vaid väike osa VASPidest kasutab kliendi virtuaalvääringute liikumise jälgimiseks plokiahelast nähtuvaid avalikke tehinguandmeid.[93] Seega on VASPide seas hoolsusmeetmete täitmata jätmine või mittenõuetekohane täitmine põhjustatud nii soovimatusest oma tegevus nõuetega vastavusse viia kui ka tõhusate tehniliste lahenduste ja teadmiste puudusest.

Rahapesu Andmebüroo juht Matis Mäeker ja Finantsinspektsiooni juhatuse liige Andre Nõmm on selgitanud, et rahapesu ja terrorismi rahastamise tõkestamine toimub kahetasandiliselt: 1) preventiivsete meetmete kohaldamisega, mis on pandud avalik-õigusliku kohustusena erasektorile; 2) kuriteo toimepanijate vastutusele võtmist ja teo käigus saadud vahendite konfiskeerimist võimaldavate kriminaalõiguslike meetmete kohaldamisega, mille eest vastutab riik.[94] Autor nõustub, et peamine roll rahapesu ja terrorismi rahastamise ennetamisel on erasektori kohustatud isikutel ning kurjategijate vastutusele võtmise roll riigil. Siiski on praktikas hakanud piirid hägustuma, kuna riik toetab erasektorit ka ennetustegevustes. Näiteks avaldab RAB soovitusi, mis aitavad kohustatud isikutel koostada protseduurireegleid ja sisekontrollieeskirju, millega maandada ja juhtida rahapesu ja terrorismi rahastamise riske, või juhendeid, mis annavad ülevaate kahtlaste tehingute tunnustest, mida monitoorimisel või skriinimisel tähele panna. Kuigi põhivastutus ennetamisel on erasektoril, sealhulgas VASPidel, siis on nii riigi, ettevõtjate kui ka tarbijate huvides, et riik teeks ettevõtjatega koostööd ja toetaks erasektorit viisil, mis võimaldab tõhusalt rahapesu ja terrorismi rahastamist ennetada.

Nagu eelnevalt nimetatud, siis üheks põhjuseks, miks suur osa VASPe ei täida nõuetekohaselt hoolsusmeetmeid, on vajalike teadmiste puudumine. Kuigi nõuetekohane hoolsusmeetmete rakendamine ja selleks vajalike teadmistega inimeste värbamine on VASPi kohustus, siis autori hinnangul tuleb ka riigil toetada teadmiste ja oskuste taseme tõstmist VASPi sektoris. Seda enam, et virtuaalvääringute teenuse pakkumine on jätkuvalt kõrge riskiga tegevusala, mis on osaliselt

[93] Rahapesu Andmebüroo uuring 2020, lk 13.
[94] Mäeker, M., Nõmm, A. Pangasaladuse hoidjast politseinikuks: valikud rahapesu tõkestamisel. – Juridica 2020/8, lk 662.

tingitud VASPide teadmatusest, kuidas rahapesu ja terrorismi rahastamise riskide maandamismeetmeid nõuetekohaselt rakendada ning finantsjärelevalve asutustel on kompetents turuosaliste teadmiste tõstmiseks, et seeläbi vastavat riski maandada. RAB on avaldanud küll teoreetilist materjali rahapesu ja terrorismi rahastamise riskide juhtimise ja hoolsusmeetmete kohaldamise kohta, aga RABi tagasiside põhjal on näha, et see pole olnud piisav, kuna suurel osal VASPidest on jätkuvalt hoolsusmeetmete kohaldamisega probleeme. Autori hinnangul tuleks sarnaselt Saksamaale, kus finantsjärelevalve asutus Bundesanstalt für Finanzdienstleistungsaufsicht korraldab VASPidele regulaarselt seminare, koolitusi ja töötubasid[95], ka Eestis pakkuda eelnimetatud teabe ja oskuste saamise võimalusi. Tulenevalt RABi tagasisidest on VASPe vaja koolitada ja praktilisi nõuandeid jagada nii isikusamasuse tuvastamise ja kontrollimisel kasutatavate dokumentide kohta kui ka tõsta teadlikkust, kuidas virtuaalvääringu tehinguid analüüsida plokiahelas kajastuva teabe põhjal. VASPidele suunatud seminaride, koolituste ja töötubade läbiviimise eesmärk on aidata turuosalistel mõista neile kohalduvaid rahapesu ja terrorismi rahastamise tõkestamise nõudeid ja selgeks teha, kuidas neid äritegevuses nõuetekohaselt järgida.

Teine nõuetekohast hoolsusmeetmete täitmist takistav põhjus on tõhusate ja tegevusala spetsiifikat arvestavate tehniliste lahenduste puudumine. RahaPTS § 70 lg 3^2 p-i 5 järgi tuleb virtuaalvääringu teenuse tegevusloa taotlemisel esitada muu hulgas andmed kavandatavate teenuste osutamiseks vajalike IT-süsteemide ning muude tehnoloogiliste vahendite ja süsteemide kohta. Samuti tuleb esitada kirjeldus IT-süsteemidest ja muudest tehnoloogilistest vahenditest, millega teenuse osutaja tagab hoolsusmeetmete, teatamiskohustuse ja rahvusvahelise sanktsiooni seadusest tulenevate kohustuste täitmise. RABile on RahaPTS § 72 lg 1^1 p-i 4 alusel antud õigus keelduda tegevusloa andmisest, kui ettevõtja IT-süsteemid ja muud tehnoloogilised vahendid ei ole teenuse osutamiseks piisavad. Ometi on praktikas jätkuvalt VASPe, kelle süsteemid ei vasta tasemele, mis maandaksid tõhusalt rahapesu ja terrorismi rahastamise riske. Kuigi sobivate tehniliste lahenduste tagamine nõuetekohaseks äritegevuseks on VASPi kohustus, tuleks autori hinnangul riskide maandamiseks riigil välja töötada ja kasutusele võtta skriinimis- ja monitoorimissüsteemi standard ning kehtestada vastava sertifikaadi omamine VASPi tegevusloa saamise kohustusliku tingimusena. Standardi väljatöötamine ja vastava sertifikaadi kehtestamine tegevusloa nõudena annaks ühelt poolt

[95] Bundesanstalt für Finanzdienstleistungsaufsicht. Veranstaltungen der BaFin. (2023) – https://www.bafin.de/DE/DieBaFin/Service/Veranstaltungen/veranstaltungen_node.html#ID_13385960 (27.03.2023).

ettevõtjale selged juhised nõuetekohaste süsteemide väljatöötamiseks, ning teiselt poolt RABile ning laiemalt kogu finantsturule kindluse, et VASPide tehnilised lahendused on nõuetekohased, kvaliteetsed ja tõhusad rahapesu ja terrorismi rahastamise tõkestamiseks. Kuna riskid on VASPide sektoris jätkuvalt kõrged, tuleks muuta ka eelpool kirjeldatud tegevusloa andmisest keeldumise alust. Kui kehtiva õiguse kohaselt on RABil õigus keelduda ebapiisavate süsteemide ja tehniliste vahendite korral, siis autori hinnangul tuleb riskide maandamiseks muuta sätet nii, et RABil on kohustus keelduda VASPi tegevusloa andmisest. Vastavad muudatused maandaksid riski, et nõrkade süsteemidega VASPe kasutatakse rahapesuks ja terrorismi rahastamiseks.

Enne standardi kehtestamist aitab ebasobivatest süsteemidest tuleneva riski maandamiseks ka see, kui VASP saab oma valmisolevate lahenduste sobivusele tagasisidet ning vastavalt sellele oma süsteemid nõuetega kooskõlla viia. Näiteks Hollandi keskpank De Nederlandsche Banki ja finantsjärelevalve asutus Autoriteit Financiële Markten on loonud ühise infopunkti - InnovationHub[96], kuhu saavad pöörduda kõik ettevõtted, kel on küsimusi seoses järelevalve või neile kohalduvate nõuetega. Sealhulgas on VASPidel võimalik saada tagasisidet enda tehniliste süsteemide nõuetelevastavuse kohta. Nii Rahapesu Andmebürool kui ka Finantsinspektsioonil on tegevusloamenetluses kohustus ja seega ka võimekus kontrollida, kas teenuse osutamisel kasutatavad infotehnoloogilised süsteemid ja muud tehnilised vahendid võimaldavad täita ettevõtjale kohalduvaid nõudeid. Seega võiks ka Eesti finantsjärelevalve asutused luua ühise infopunkti, mis võimaldab VASPidel saada tagasisidet oma skriinimis- ja monitoorimissüsteemide sobivusele ja vastavalt sellele oma süsteeme täiendada. Eelnevast tulenevalt on autor seisukohal, et maandada rahapesu ja terrorismi rahastamise riski, mis on tingitud tõhusate ja VASPide tegevusala spetsiifikat arvestavate tehniliste lahenduste puudumisest, tuleb: 1) luua skriinimis- ja monitoorimissüsteemi standard; 2) kehtestada RahaPTS-is vastava sertifikaadi omamine VASPi tegevusloa kohustusliku tingimusena; 3) kehtestada RahaPTS-is RABile kohustus keelduda tegevusloa andmisest, kui VASPil puudub sertifikaat, mis tõendab IT-süsteemide ja tehniliste lahenduste vastamist standardile; ning 4) alternatiivselt luua tehnilisele lahendusele tagasiside saamise võimalus.

Olukorras, kus VASP tegutseb hooletult ehk ettevõtja ei soovi oma tegevust nõuetega kooskõlla viia ja jätkab seaduse rikkumist, on RABile antud pädevus kasutada mõjutusvahendeid nagu

[96] De Nederlandsche Bank. InnovationHub and Regulatory Sandbox. (2023) – https://www.dnb.nl/en/sector-information/supervision-stages/prior-to-supervision/innovationhub-and-regulatory-sandbox/ (27.03.2023).

sunniraha või trahviraha määramine. Näiteks RahaPTS-i järgi saab juhatuse liiget, kes on andnud korralduse hoolsusmeetmete rakendamata jätmiseks trahvida kuni 300 trahviühikuga ning juriidilist isikut kuni 400 000 euro suuruse rahatrahviga. Samas määras trahv on ettenähtud ka olukorraks, mil rikutakse kliendi, juhuti tehingus osaleva isiku või isiku esindaja isikusamasuse tuvastamise ja kontrollimise kohustust. Kui VASP rikub tema tegevust reguleerivates õigusaktides sätestatut korduvalt või olulisel määral, on RABil võimalik RahaPTS § 75 lg 2 p-i 7 alusel tegevusluba kehtetuks tunnistada. Seega RahaPTS-is on olemas võimalused, kuidas pahatahtlikke turuosalejaid vastutusele võtta või tegutsemine virtuaalvääringu teenuse turul ära keelata. Sellest hoolimata on meil turul tegutsemas VASPe, kes nõudeid jätkuvalt ei täida. Kuna sama probleem esineb ka VASPide puhul, kes ei täida teatamiskohustust, käsitleb autor vastavat teemat lähemalt järgmises peatükis.

2.2.Virtuaalvääringu teenuse pakkujate teatamiskohustuse täitmine riskide maandamisel

Virtuaalvääringu teenuse pakkujad on lisaks hoolsusmeetmete kohaldamisele kohustatud täitma ka teatamiskohustust RABile. Eesti riiklikus riskihinnangus, RABi 2022. aasta aastaraamatus ja virtuaalvääringu teenuse pakkujate uuringutes on täheldatud, et suurem osa VASPidest ei täida teatamiskohustust nõuetekohaselt. Samuti on VASPe, kes ei täidagi teatamiskohustust. Seega tõstatab ka VASPide mittenõuetekohane teatamiskohustuse täitmine küsimuse õigusliku reguleerimise kohasusest ja vastavusest.

RahaPTS-is kehtestatud teatamiskohustuse täitmiseks tuleb RABile esitada teade, kui VASP tuvastab tegevuse või asjaolud, mille osas: 1) esinevad tunnused, mis osutavad kuritegelikust tegevusest saadud tulu kasutamisele või sellega seotud kuritegude toimepanemisele (ebahariliku tehingu/tegevuse teade); 2) VASP teab või tal on kahtlus või mille tunnused osutavad rahapesule või sellega seotud kuritegude toimepanemisele (rahapesu kahtluse teade); 3) VASP teab või tal on kahtlus või mille tunnused osutavad terrorismi rahastamisele või sellega seotud kuritegude toimepanemisele (terrorismi rahastamise kahtluse teade); või 4) rahaline kohustus suurusega üle 32 000 euro täidetakse sularahas (sularahatehingu teade).[97] Rahvusvahelise sanktsiooni seaduse[98] § 21 lg 1 järgi on VASPil kohustus esitada teade RABile ka siis, kui tuvastatakse, et isik on finantssanktsiooni subjekt, kelle tehing rikuks finantssanktsiooni või kui VASPil on selles kahtlus

[97] Rahapesu Andmebüroo riskide juhtimise juhend 2022, lk 58.
[98] Rahvusvahelise sanktsiooni seadus – RT I, 08.03.2022, 3.

(rahvusvaheline finantssanktsiooni teade). Teatamiskohustuse täitmisel annab RAB asjakohasel juhul tagasisidet, kas ja milliseid riskide maandamise meetmeid tuleb kohustatud isikul rakendada. Lisaks on õiguskirjanduses peetud teavitamiskohustust võtmetähtsusega meetmeks rahapesu ja terrorismi rahastamise tõkestamisel, kuna saadud teabe analüüsimisel on RABil võimalik välja selgitada, kas esineb alus edasiseks uurimiseks ning edastada vastav teave nii siseriiklikele kui ka välisriikide õiguskaitseasutustele.[99] Teisisõnu on teadete abil võimalik tuvastada ja uurida potentsiaalseid rahapesu ja terrorismi rahastamise kahtluseid tehinguid, mis võivad viia kuritegevuse tuvastamiseni ning lõppastmes osutuda vajalikuks, et õiguskaitseasutused saaksid kurjategijad vastutusele võtta. Lisaks eelnevale seisneb autori hinnangul teatamiskohustuse tähtsus selles, et teadete kogumisel ja analüüsimisel on RABil võimalik seadusandjale anda tagasisidet, kas kehtiv regulatsioon täidab tõhusalt rahapesu ja terrorismi rahastamise tõkestamise eesmärki ja teha vajadusel ettepanekuid õigusaktide täiendamiseks.

RABi statistika kohaselt täitsid aastal 2021 teatamiskohustust 24% ja aastal 2022 47% kõikidest Eesti VASPidest.[100] Kohustuse täitjate arv on ühe aastaga märgatavalt tõusnud, aga üle poole VASPidest ei ole siiani ühtki teadet esitanud. Konkreetselt terrorismi rahastamise kahtlusega teateid on aastal 2021 esitanud üksnes 1%[101] ja aastal 2022 2,5%[102] kõikidest Eesti VASPidest. Seega ka terrorismi rahastamise kahtlusega teadete esitajate arv on mitmekordistunud, ent tegemist on siiski väga väikese osaga VASPidest. Teatamiskohustuse mittetäitjate hulgas on nii suuremaid kui ka väiksemaid ettevõtteid. RABi aastaraamatus on kirjeldatud kaasust, kus Eesti ühe suurima käibega VASPi Holdtech OÜ osas alustati järelevalvemenetlus, mille käigus tuvastati muu hulgas, et VASP on süsteemselt jätnud hoolsusmeetmeid kohaldamata ning rahapesu ja terrorismi rahastamise kahtlusega teated esitamata.[103] Lisaks asjaolule, et teatajate arv on virtuaalvääringu teenuse pakkujate sektori kõrget riskitaset ja mahte arvestades endiselt ebapiisav, on RAB tuvastanud puudusi ka esitatud teadete kvaliteedis ja mahus. Eelkõige ei ole teadetes piisavalt infot, näiteks tehingu ja kahtluse kohta või on tehingu osapooled lisamata. Samuti esinevad vormi- ja

[99] Cotoc, C-N. jt. Efficiency of Money Laundering Countermeasures: Case Studies from European Union Member States. – Risks 2021/09 No 120, lk-d 1-2.
[100] Rahapesu Andmebüroo. Tagasiside 2022. aastale. Rahapesu Andmebüroo tagasiside virtuaalvääringu teenuse pakkujatele. (2023, lk 4) – https://fiu.ee/aastaraamatud-ja-uuringud/tagasiside-teatajatele#tagasiside-virtuaalv (06.04.2023).
[101] Eesti riiklik riskihinnang 2021, lk 4.
[102] Rahapesu Andmebüroo aastaraamat 2022, lk 26.
[103] Rahapesu Andmebüroo aastaraamat 2022, lk 50.

teate kvalifitseerimise vead.[104] Seega on VASPide sektoris probleeme nii teatamiskohustuse vähese täitmisega kui ka esitatud teadete kvaliteediga.

Kuna teadete esitamine sõltub ärisuhte seire käigus kahtlust tekitavate asjaolude tuvastamisest, siis sarnaselt eelnevas peatükis käsitletud seiramiskohustusele, on ka teadete esitamise vähesus tingitud sellest, et enamik VASPidel puuduvad tegevusala spetsiifikat arvestavad skriinimis- ja monitoorimissüsteemid, mille abil teatamist vajavaid asjaolusid tuvastada. RABi hinnangul viitab madal teatamisaktiivsus ka sellele, et VASPi töötajatel puuduvad vajalikud teadmised. Nimelt on VASPide järelevalveasutus väljendanud, et: „Riskikohana näeb RAB puudulikke teadmisi teatamiskohustuse täitmisest – millised teateliigid on olemas, millistele tunnustele need vastavad ning kuidas ja millal tuleb RABile teha teade.“[105] Näiteks VASPi kontaktisikute kandidaatide puhul on täheldatud, et lisaks teatamiskohustust puudutavate teadmiste puudumisele, ei ole neil ka piisavaid teadmisi ettevõtte tehnilistest vahenditest, mida hoolsusmeetmete rakendamisel kasutatakse või millised on nendega seotud protsessid. Tuginedes eeltoodud argumentidele, on autor seisukohal, et VASPid, kel puuduvad tehnilised lahendused, mis tuvastaks RABi teavitamist vajavaid olukordi, ja teadmised, mis võimaldaksid nõuetekohast teatamiskohustuse täitmist, kujutavad finantssektoris riski, kuna läbi nende ettevõtete on võimalik tegeleda rahapesu ja terrorismi rahastamisega ilma, et VASP seda kontrolliks, RABile teavitaks ja tegevust tõkestaks.

Kuna virtuaalvääringu tehingud on kajastatud plokiahelas, siis on RABi teavitamist vajavate tunnuste tuvastamiseks vaja kasutada skriinimis- ja monitoorimissüsteeme, mis võimaldavad plokiahela analüüsimist. Süsteemid peavad olema arendatud nii, et need tuvastaksid ka virtuaalvääringu tehingu iseäralikke kahtlaseid tunnuseid, näiteks kui isik on kasutanud virtuaalvääringute segamisteenust või kui isik soovib teha tehingut *unhosted wallet*’i omanikuga, kes on tuvastamata. Kuna VASPide tegevusala spetsiifiliste skriinimis- ja monitoorimissüsteemide pakkujate arv ülemaailmselt on endiselt madal[106], on vajalike süsteemide väljaarendamise raskuskese VASPidel. Vastavalt eelmises peatükis käsitletule tuleb autori hinnangul puudulikest süsteemidest tuleneva riski maandamiseks luua skriinimis- ja monitoorimissüsteemi standard, täiendada tegevusloa tingimusi nõudega, et ettevõtjal peab olema standardile vastavust tõendav

[104] Rahapesu Andmebüroo tagasiside aastale 2022, lk 7.
[105] Rahapesu Andmebüroo uuring 2022, lk 21.
[106] Wronka, C. Money laundering through cryptocurrecies - analysis of the phenomenon and appropriate prevention measures. – Journal of Money Laundering Control 2022/25 No 1, lk 92.

sertifikaat ning kehtestada kohustus keelduda tegevusloa andmisest, kui ettevõtja ei oma vastavat sertifikaati.

Teine probleem on madal teadmiste tase. Isegi, kui VASPil on tõhusad süsteemid rahapesu ja terrorismi rahastamise kahtlaste tehingute tuvastamiseks, peavad töötajal olema ka teadmised ja oskused, kuidas saadud infot analüüsida ja RABile teatamiskohustust nõuetekohaselt täita. RahaPTS § 17 lg-te 2 ja 7 kohaselt peab VASPi juhatus määrama kontaktisiku, kelle ülesanded on muu hulgas ebatavalistele, rahapesu ja terrorismi rahastamise kahtlusega tehingutele viitava teabe kogumise korraldamine ja analüüsimine. Samuti on kontaktisiku ülesandeks rahapesu või terrorismi rahastamise kahtluse korral vastava teabe edastamine RABile. Teavitamiskohustuse täitmiseks on RAB oma kodulehel avaldanud erinevaid juhiseid: 1) Juhend kahtlaste tehingute tunnuste kohta[107]; 2) Kõrgema terrorismi rahastamise riskiga riikide ehk nn riskiriikide nimekiri[108]; 3) Rahapesu Andmebüroole esitatava teate esitamise juhend[109] 4) Rahapesu Andmebüroole esitatava teate vorm[110]. Seega, teoreetiline materjal teatamiskohustuse täitmiseks on olemas ja kättesaadav, aga praktilises teostuses esineb jätkuvalt puudusi.

RahaPTS § 17 lg 6 alusel on RABil õigus kontrollida VASPi määratud kontaktisiku sobivust ning kui RABi kontrolli tulemusel selgub, et kontaktisik ei ole oma varasema tegevuse või tegevusetuse tõttu usaldusväärne, võib VASP kontaktisiku töölepingu usalduse kaotuse tõttu erakorraliselt üles öelda. See tähendab, et VASPid võivad praktikas värvata isikuid, kes tegelikult ei ole pädevad kontaktisiku ülesannete täitmiseks ning kui RABi kontrollimise käigus selgub, et tegemist ei ole sobiva isikuga, on ettevõtetel õigus, mitte kohustus tööleping kontaktisikuga erakorraliselt üles öelda. Seega esineb risk, et VASPi kontaktisikutel puudub vajalik pädevus nõuetekohaseks teatamiskohustuse täitmiseks. Eelkirjeldatud RABi tagasiside põhjal on selge, et vastav risk on realiseerunud.

Autori hinnangul tuleb vastava riski maandamiseks luua kontaktisiku kutsestandard ning täiendada RahaPTS §-s 17 kontaktisikule kehtestatud tingimusi nõudega, et kontaktisikul peab olema

[107] Rahapesu Andmebüroo. Juhend kahtlaste tehingute tunnuste kohta. (2022) – https://fiu.ee/oigusaktid-ja-juhendid/juhendid#juhend-kahtlaste-teh (23.03.2023).
[108] Rahapesu Andmebüroo. Rahapesu Andmebüroo kahtlaste tehingute tunnuste juhendi lisa: Kõrgema terrorismi rahastamise riskiga riikide nimekiri. (2022) – https://fiu.ee/oigusaktid-ja-juhendid/juhendid#juhend-kahtlaste-teh (23.03.2023).
[109] Rahapesu Andmebüroo. Täpsustav juhis teate esitamiseks Rahapesu Andmebüroole. (2020) – https://fiu.ee/oigusaktid-ja-juhendid/juhendid#esitatava-teate-tait (23.03.2020).
[110] Rahapesu Andmebüroo. Rahapesu Andmebüroole esitatava teate vorm. (2020) – https://fiu.ee/oigusaktid-ja-juhendid/juhendid#esitatava-teate-vorm (23.03.2020).

kutsestandardile vastavust tõendav kutsetunnistus. Kontaktisikule kvalifikatsiooninõude kehtestamine tagab ühelt poolt ettevõtjale kindluse, et kontaktisik on pädev oma tööülesandeid nõuetekohaselt täitma ja teiselt poolt kindluse RABile ja laiemalt kogu finantsturule, et VASPidele kehtestatud teatamiskohustus ei jää kontaktisiku teadmiste ja/või oskuste ebapiisavuse tõttu täitmata. Kuna RahaPTS § 72 lg 1 p-i 2 alusel peab VASPi tegevusloa saamiseks ettevõtja määratud kontaktisik vastama RahaPTS § 17-s sätestatud nõuetele, siis kvalifikatsiooninõude lisamine RahaPTS §-i 17 välistaks olukorrad, kus tegevusluba antakse VASPile, kelle kontaktisikul puuduvad piisavad teadmised ja oskused kvaliteetse teatamiskohustuse täitmiseks. Eeltoodud argumentidest tulenevalt on autor seisukohal, et kontaktisiku kutsestandardi loomine ja sellega seotud kvalifikatsiooni nõude kehtestamine kontaktisikule, maandab riski, et VASPid ei täida nõuetekohaselt rahapesu ja terrorismi rahastamise tõkestamise eesmärki täitvat teatamiskohustust.

VASPidele, kes pahatahtlikult rikuvad rahapesu ja terrorismi rahastamise kahtlusest teavitamise kohustust, on RABil võimalik määrata sunniraha. Samuti on RABil õigus määrata teatamiskohustuse rikkumise eest füüsilisele isikule rahatrahv kuni 300 trahviühikut või arest ja juriidilisele isikule rahatrahv kuni 400 000 eurot. Kui eelnimetatud mõjutusvahendite rakendamine ei motiveeri VASPi enda tegevust seadusenõuetega vastavusse viima, on RABil õigus ka RahaPTS § 72 lg 2 p-i 7 järgi tunnistada VASPi tegevusluba kehtetuks. Seega on RABil olemas õiguslikud meetmed, mille abil mõjutada VASPi oma tegevus nõuetega kooskõlla viima ning vajadusel ka ettevõttelt VASPina tegutsemine õigus ära võtta, mis täidab eesmärki eemaldada turult teenusepakkuja, kes nõuete mittekohaldamisega aitab potentsiaalselt rahapesu ja terrorismi rahastamisele kaasa. Küll aga on eelnevalt käsitletud statistika põhjal võimalik järeldada, et turul tegutsevad jätkuvalt isikud, kes teatamiskohustust ei täida. RABi 2022. aastal avaldatud uuringust selgub, et RAB on 2021. aastal teostanud VASPide osas 14 kohapealset järelevalvekontrolli ja 606 kaugkontrolli. Järelevalvekontrolli tulemusena tunnistati kehtetuks 1 tegevusluba ning ei tehtud ühtegi ettekirjutust puuduste kõrvaldamiseks. Samas tunnistati kehtetuks 329 tegevusluba ja peamiselt põhjusel, et VASPid ei vastanud RABi korduvatele infopäringutele.[111] Arvestades, et eelviidatud 2022. aasta statistika järgi ei täida üle poole VASPidest teatamiskohustust ning terrorismi rahastamise kahtlusega teadete esitamise kohustust ei täida 97,5% VASPidest, tuleb autori hinnangul RABil rakendada VASPide osas kõrgendatud tähelepanu, suurendada järelevalvekontrollide läbiviimist, teha vajadusel ettekirjutusi ja rakendada ettenähtud sanktsioone

[111] Rahapesu Andmebüroo uuring 2022, lk 26.

VASPide osas, kelle tegevus ei ole kooskõlas neile kehtestatud nõuetega. Seda enam, et 2022. märtsis jõustunud RahaPTS muudatustega pidid kõik VASPid tagama, et nende tegevuskoht asuks Eestis, on RABil nüüd soodsad võimalused kohapealsete järelevalvekontrollide läbiviimiseks. Vastasel juhul on maandamata risk, et turul on VASPid, kes ei takista oma äritegevuses rahapesu ja terrorismi rahastamise riski realiseerumist.

3. Tegevusloa nõue ja riigilõiv virtuaalvääringu teenuste riskide maandamisel

3.1.Tegevusloale kehtestatud nõuded ja virtuaalvääringu teenuste riskide maandamine

Alates 2017. aastast, mil Eestis hakati esmakordselt virtuaalvääringu teenuse pakkujate tegevuslubasid väljastama, on VASPide tegevusloa nõudeid korduvalt muudetud. Seadusandja on tegevusloa taotlemise või selle kehtima jäämise nõudeid iga paari aasta järel juurde lisanud ja olemasolevaid nõudeid karmistanud. Rahandusministeeriumi 2021. aastal algatatud ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse (edaspidi ÜMIVS) eelnõu seletuskirjast[112] nähtub, et VASPide tegevusloa nõudeid plaanitakse veelgi karmistada. Veelgi enam, 2023. aastal on jõustumas Euroopa krüptovaraturgude määrus (ingl *Markets in Crypto-Assets*, MiCA), mille alusel peavad VASPid, kes soovivad jätkata virtuaalvääringu teenuste osutamist, taotlema uue tegevusloa. Seega on VASPidele kohalduv õigusraamistik olnud pidevas muutuses, veelgi enam, lühikese aja jooksul on nõuded muutunud ettevõtja perspektiivist ebasoodsamaks. Ettevõtjad, kes taotlesid VASPi tegevusloa 2017. aastal, on iga paari aasta järel pidanud oma äritegevuses tegema ulatuslikke muudatusi, et olla vastavuses uute nõuetega ning vältida tegevusloa kehtetuks tunnistamist.

Eesti PS §-s 10 on loetletud mitmed põhiseaduse aluspõhimõtted, millest üks on õigusriigi põhimõte. Vastav põhimõte väljendub muuhulgas ka õiguskindluses. Riigikohus on õiguskindluse põhimõtet selgitanud järgmiselt: „Õiguskindlus tähendab nii selgust kehtivate õigusnormide sisu osas (õigusselguse põhimõte) kui ka kindlust kehtestatud normide püsimajäämise suhtes (õiguspärase ootuse põhimõte)“.[113] Tulenevalt asjaolust, et VASPide tegevusloa nõudeid on lähima paari aasta jooksul korduvalt täiendatud ja karmistatud ning järjekordsed muudatused leiavad aset lähiaastatel, selgitab autor välja, kuidas on tegevusloa nõuete muutmine mõjutanud rahapesu ja terrorismi rahastamise riske ja kas sagedased VASPide tegevusluba puudutavad seadusemuudatused on kooskõlas õiguspärase ootuse põhimõttega.

Riigikohus on 2004. aastal selgitanud, et õiguspärase ootuse kohaselt peab: „ […] igaühel olema võimalus kujundada oma elu mõistlikus ootuses, et õiguskorraga talle antud õigused ja pandud

[112]Ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seadus. Eelnõu. – https://eelnoud.valitsus.ee/main#lfDlLOyf (07.04.2023); Ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seadus. Seletuskiri. – https://eelnoud.valitsus.ee/main#lfDlLOyf (07.04.2023).
[113] RKPKJo 3-4-1-20-04.

kohustused püsivad stabiilsetena ega muutu rabavalt isikule ebasoodsas suunas.“[114] Riigikohus on eespool tsiteeritud selgitust veel täiendanud 2014. aastal, leides järgmist: „Õigusi on võimalik täisväärtuslikult kasutada vaid siis, kui isik ei pea kartma, et riik rakendab ettenägematuid ebasoodsaid tagajärgi. Riigi sõnamurdmisega saab tegemist olla siis, kui isik on oma tegevusega täitnud eeldused, millest tulenevalt tal on tulevikus õigus enda suhtes soodsa regulatsiooni kohaldamisele, kuid riik kehtestab sellest hoolimata tema suhtes uue, vähem soodsa regulatsiooni.“[115]

Esmakordselt hakati virtuaalvääringu teenuse tegevuslubasid[116] Eestis väljastama 2017. aasta lõpus. Kui esimesel aastal väljastati 6 tegevusluba, siis aastal 2018 väljastati 1137 ja aastal 2019 veel 1304 tegevusluba. Väljastatavate tegevuslubade kiire kasv oli RABi uuringu kohaselt tingitud madalast turule pääsemise lävendist ning järelevalve teostamise raskusest. Samuti puudus RABil seaduslik alus keelduda loa väljastamisest ettevõtetele, kel puudus igasugune tegelik seos Eestiga.[117] Rahapesu ja terrorismi rahastamise riskide maandamiseks ning ka Eesti mainekahju ära hoidmiseks hakati kehtivat korda täiendama uute nõuetega.

2020. aasta märtsis jõustunud RahaPTSi redaktsiooni[118] kohaselt karmistati VASPide tegevusloa taotlemise nõudeid ning kehtestati ettevõtjatele, kel tegevusluba olemas, täiendavaid nõudeid. Muudatusi oli mitmeid, ent autor toob järgnevalt välja nendest peamised. Esiteks pidid ettevõtjad tagama ja tõestama, et ettevõtte registrijärgne asukoht, juhatuse asukoht ning tegevuskoht asuvad Eestis. Teiseks, ettevõtja juhtorgani liikmetele ja prokuristile kehtestati sobivusmenetlus, mille raames hinnatakse, kas isik on usaldusväärne, omab vajalikke teadmisi, oskusi, kogemust, et täita kohustusi tema positsioonile kohase kvaliteediga ja kas tal on laitmatu ärialane maine. Kolmandaks kehtestati ettevõtjale 12 000 euro suurune miinimum kapitalinõue, mis pidi olema täies ulatuses rahaliselt sisse makstud ning riigilõivuseaduses tõsteti tegevusloa taotluse läbivaatamise riigilõiv 345 eurolt 3300 eurole. Ettevõtjad pidid oma tegevuse viima eelpoolkirjeldatud muudatustega kooskõlla ja esitama seda tõendavad dokumendid RABi-le hiljemalt 30.06.2020, et vältida tegevusloa kehtetuks tunnistamist.

[114] RKPJKo 3-4-1-20-04; RKPJKo 3-4-1-24-11.
[115] RKÜKo 3-4-1-1-14.
[116] 2017. aastal väljastati virtuaalvääringu raha vastu vahetamise teenuse ja virtuaalvääringu rahakotiteenuse pakkujate teguvuslubasid. Aastal 2020 loodi vastavate teenuste koondamiseks üldnimetus „virtuaalvääringu teenus“.
[117] Rahapesu Andmebüroo uuring 2020, lk 5.
[118] Rahapesu ja terrorismi rahastamise tõkestamise seadus. – RT I, 31.12.2019, 20.

Tulenevalt Eesti riiklikus riskihinnangus tuvastatud kõrgetest rahapesu ja terrorismi rahastamise riskidest virtuaalvääringu teenuse pakkujate sektoris ning aastatel 2021 ja 2022 toimud Moneyval[119] hindamisest karmistati 2022. aasta märtsis jõustunud RahaPTS redaktsiooniga[120] VASPidele kohalduvaid nõudeid veelgi. Näiteks suurendati mitmekordselt VASPi osa- ja aktsiakapitali miinimumnõudeid ja tegevusloa läbivaatamise riigilõivu. Kehtestati esmakordselt tegevusloa muutmise taotluse läbivaatamise riigilõiv, omavahendite miinimumnõue, audiitor- ja sisekontrolli kohustus ning täiendavad hoolsusmeetmed. Samuti täiendati tegevusloa taotlemisel esitatavate andmete ja dokumentide nimekirja ning kehtestati kõrgendatud nõuded VASPi asu- ja tegevuskohale, juhatuse liikmetele ja kontaktisikule. Tegevusloa kehtetuks tunnistamise vältimiseks tuli VASPidel viia enda tegevus kooskõlla uute täiendavate nõuetega ning seda tõendavad dokumendid esitada RABille hiljemalt 15.06.2022.

Lisaks eeltoodule algatas 2021. aasta jaanuaris rahandusministeerium ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse (ÜMIVS) eelnõu.[121] Vastava eelnõu eesmärk on kehtestada ühisrahastuse, investeerimisinstrumendi ja virtuaalvääringu teenuse osutajatele asutamise, tegevuse (sh investorkaitse alased nõuded), lõpetamise ja vastutuse nõuded. Samuti viiakse eelnõu kohaselt eelnimetatud teenuse pakkujate üle tehtav finantsjärelevalve Finantsinspektsiooni pädevusse. Pärast kahte eelnõu kooskõlastusringi on eelnõu kohaldamisala piiritletud krüptovaraga ja ühisrahastusprojektidega, mida pakutakse finantsvahendusplatvormide kaudu. Sellest tulenevalt on uuendatud ka eelnõu nime, milleks on krüptovara ja ühisrahastuse seaduse (edaspidi KrÜS) eelnõu.[122] Vastava eelnõu § 3 lg 1 kohaselt kuulub virtuaalvääring krüptovara hulka ning § 120 lg 2 alusel peab KrÜSi kehtima hakkamisel VASP taotlema krüptovara teenuse osutaja tegevusluba Finantsinspektsioonilt, kuna RAB-i väljastatud tegevusluba muutub kehtetuks. Rahapesu ja terrorismi rahastamise tõkestamise nõuded jäävad RahaPTS-is VASPidele kehtima. KrÜS eelnõu § 132 järgi pidi vastav seadus jõustuma 1. juulil 2023 ning § 120 lg-s 2

[119] Moneyval (ingl k *The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism*) on Euroopa Nõukogu ekspertkomitee, mille ülesandeks on hinnata riikide rahapesu ja terrorismi rahastamise tõkestamise valdkonna meetmete rakendamise taset. Hindamiste tulemused avaldab MONEYVAL raportitena. Euroopa Nõukogu. At a glance. (2023) – https://www.coe.int/en/web/moneyval/home (06.04.2023).
[120] Rahapesu ja terrorismi rahastamise tõkestamise seadus. – RT I, 12.03.2022, 19.
[121] Ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seadus. Eelnõu. – https://eelnoud.valitsus.ee/main#lfDlLOyf (07.04.2023).
[122] Krüptovara ja ühisrahastuse seadus. Eelnõu. – https://advokatuur.ee/uploads/files/Kr%C3%9CS%20EN.pdf (07.04.2023); Krüptovara ja ühisrahastuse seadus. Seletuskiri. – https://advokatuur.ee/uploads/files/Kr%C3%9CS%20SK.pdf (07.04.2023).

sätestatud ülemineku perioodi kohaselt oleksid VASPid pidanud hiljemalt 2024. aasta aprilliks taotlema uue tegevusloa. Kuna eelnõu on jätkuvalt kooskõlastusfaasis, siis on eelnõu algataja jätnud jõustumise aja lahtiseks ning magistritöö kirjutamise ajal ei ole veel teada, kas, millal ja millises versioonis KrÜS jõustub.

Ka Euroopa Liidu tasandil on täheldatud vajadust krüptovara teenuse reguleerimise järele. Euroopa Komisjon avalikustas 2020. aastal digitaalse rahanduse paketi[123], mis hõlmab krüptovaraturgude määruse (ingl Markets in Crypto Assets ehk MiCA) loomist. Eesmärk on Euroopa Liidus luua ühtne krüptovarateenuse pakkumise reeglistik. Krüptovaraturgude määruse viimase kinnitatud teksti[124] kohaselt kehtestatakse krüptovara teenuse pakkujatele muuhulgas uue ehk nn MiCA tegevusloa taotlemise kohustus. MiCA tegevusloaga saab edaspidi teenuseid osutada ka teistes Euroopa Liidu liikmesriikides, ilma et peaks igas liikmesriigis eraldi tegevusluba taotlema. Määruse vastuvõtmise hääletus toimub 2023. aasta aprillis ning selle jõustumisel on ettevõtjatel aega Art 123 lg 2 alusel 18 kuud, et taotleda uus MiCA tegevusluba. Kuna tegemist on otsekohalduva Euroopa Liidu õigusaktiga, mis reguleerib krüptovarateenuse osutamist, sh tegevusloa nõudeid, siis saab KrÜSis pärast krüptovaraturgude määruse jõustumist reguleerida krüptovarateenuseid üksnes määruses lubatavas ulatuses. Näiteks tuleb liikmesriikidel määrata pädev asutus, kes teostab krüptovara teenuse pakkujate üle järelevalvet ja kelle pädevusse kuulub tegevusloamenetlus. Tulenevalt KrÜS eelnõust, võib eeldada, et Eesti pädevaks asutuseks määratakse Finantsinspektsioon.

Eelnevast nähtub, et VASPid on pidanud tegema ulatuslikke investeeringuid ja ümberkorraldusi, et viia enda tegevus kooskõlla iga paari aasta tagant kehtestatud uute nõuetega, ning ees ootavad järjekordsed muudatused, kus virtuaalvääringu teenuse pakkumise jätkamiseks on VASPidel vaja taotleda uus tegevusluba. Sage tegevusloa regulatsiooni muutmine ja seda ettevõtjale ebasoodsas suunas takistab autori hinnangul virtuaalvääringu teenuse pakkujate sektoris ettevõtluse teostamist. Äritegevuse kooskõlla viimine uute muudatustega nõuab ettevõtjalt täiendavate kulutuste tegemist, täiendava inimressursi leidmist ja uute tehnoloogiliste lahenduste välja töötamist. Stabiilsuse

[123] Euroopa Parlament. Digital finance package. (2020) – https://finance.ec.europa.eu/publications/digital-finance-package_en (17.03.2023).
[124] Euroopa Liidu Nõukogu. Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. (2022). – https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf (27.03.2023).

puudumine õiguskeskkonnas raskendab äritegevust ja selle pikemaajalist planeerimist. Õigusrahu puudumist on ette heitnud ka turuosalised.[125]

Selgitamaks välja, kas eelkirjeldatud õiguskeskkonna stabiilsuse puudumine VASPide sektoris on põhiseaduspärane, analüüsib autor järgnevalt, kas toimunud ja tulevikus toimuvad seadusemuudatused on kooskõlas VASPide õiguspärase ootuse põhimõttega. Euroopa Kohtu kohtujuristi Dr. iur. Priit Pikamäe on põhiseaduslikkuse järelvalve praktikat uurides jõudnud järeldusele, et õiguspärase ootuse rikkumise tuvastamiseks tuleb: „[…] kõigepealt tuvastada, kas isikul on tekkinud õiguspärane ootus mingi õigusolukorra püsimajäämise suhtes, ning jaatava vastuse korral hinnata neid avaliku võimu argumente, millega põhjendatakse selle muutmise vajadust.“[126] Pikamäe sõnul on õiguspärase ootuse tekke tuvastamiseks Riigikohtu praktika alusel välja kujunenud 2-astmeline test. Nimelt tuleb hinnata, kas kumulatiivselt on täidetud kaks järgmist tingimust: 1) isikul on subjektiivne õigus teatavale hüvele; 2) isik on asunud seda õigust kasutama ajal, kui õigusakti muudeti.[127] Seega tuleb esmalt tuvastada, kas VASPidel on subjektiivne õigus teatavale hüvele.

Eesti Vabariigi Põhiseaduse (edaspidi PS) § 31 järgi on Eesti kodanikel ja kui seadus ei sätesta teisiti, siis ka Eestis viibivatel välisriikide kodanikel ja kodakondsuseta isikutel õigus tegeleda ettevõtlusega. Õigusfilosoofi ja riigiõigusteadlase Robert Alexy sõnul tuleb põhiõiguse kaitseala puhul teha vahet kahel aspektil: esemelisel ja isikulisel kaitsealal.[128] Riigikohtu praktika kohaselt hõlmab ettevõtlusvabaduse esemeline kaitseala kõiki tegevusalasid, mille puhul pakub isik enda nimel kaupu või teenuseid ning kui tegemist on tulu eesmärgil toimuva tegevusega.[129] Lisaks füüsilistele isikutele laieneb ettevõtlusvabadus PS § 9 lg 2 alusel ka juriidilistele isikutele. Kuna virtuaalvääringu teenuse pakkujateks on ettevõtjad, kes pakuvad oma majandustegevusena klientidele virtuaalvääringu rahakoti, vahetamise, ülekande või pakkumise teenust, mis on seotud virtuaalvääringu väljastamisega, siis kuuluvad VASPid ettevõtlusvabaduse isikulisse kaitsealasse ning virtuaalvääringu teenuse osutamine esemelisse kaitsealasse.

[125] FinanceEstonia. FinanceEstonia esitas ettepanekud krüptovara ja ühisrahastuse seaduse eelnõule. (2022) – http://www.financeestonia.eu/news/financeestonia-esitas-ettepanekud-kruptovara-ja-uhisrahastuse-seaduse-eelnoule/ (14.03.2023).
[126] Pikamäe, P. Ootused-lootused ehk õiguspärase ootuse põhimõte põhiseaduslikkuse järelevalve praktikas. – Juridica 2019/9, lk 702.
[127] Pikamäe, P., lk 703.
[128] Alexy, R. Põhiõigused Eesti põhiseaduses. – Juridica 2001/eriväljaanne.
[129] RKPJKo 3-4-1-6-00.

PS § 31 teine lause annab seadusandjale võimaluse sätestada ettevõtlusvabaduse kasutamisele tingimused ja korra. Seadusandja võib tulenevalt avalikust huvist või teiste isikute õiguste ja vabaduste kaitse eesmärgil kehtestada ettevõtlusele erinevaid piiranguid.[130] Kuna virtuaalvääringu ja virtuaalvääringu teenuse pakkumisega seotud rahapesu ja terrorismi rahastamise riskid on kõrged, siis tuleb FATFi juhiste[131] järgi avalikust huvist lähtuvalt kehtestada VASPidele tegevusloa taotlemise kohustus. VASPide tegevuse reguleerimisel kohustatakse VASPe rakendama rahapesu ja terrorismi rahastamise ennetamise ja tõkestamise meetmeid, sealhulgas isikusamasuse tuvastamist, tehingute monitoorimist, teatamiskohustuse täitmist, tehingute tegemisest keeldumist jm. Samuti võimaldab VASPide järelevalvele allutamine järelevalveasutustel mõista, millised on virtuaalvääringu teenusega seotud riskid turul ja nendele vastavalt reageerida. Ka Eesti seadusandja on avalikust huvist lähtuvalt kehtestanud RahaPTS § 70 lg 1 p-s 4 VASPidele tegevusloa taotlemise kohustuse. Seega saab isik tegeleda ettevõtlusega virtuaalvääringu teenuse pakkumise sektoris siis, kui tal on selleks kehtiv tegevusluba. Eelnevast tulenevalt leiab autor, et subjektiivne õigus hüvele seisneb isikute, kellel on virtuaalvääringu teenuse pakkumiseks tegevusluba, õiguses osutada vastavat teenust.

Järgmisena tuleb hinnata, kas VASP on asunud subjektiivset õigust kasutama ajal, mil õigusakti muudeti. Siinkohal tuleb eristada kahte olukorda. Esiteks situatsiooni, kus VASP osutas tegevusloaga lubatud teenust ajal, mil tegevusluba puudutavat regulatsiooni muudeti VASPile ebasoodsas suunas. VASPid, kes said virtuaalvääringu teenuse osutamise loa aastatel 2017-2019, on pidanud aastatel 2020 ja 2022, mil nende tegevusele kehtestati täiendavaid tingimusi, viima oma tegevuse kooskõlla uute nõuetega, et vältida teenuse osutamise õigusest ilma jäämist. See on nõudnud ettevõtjatelt täiendavate ressursside leidmist, näiteks kvalifitseeritud personali palkamist, uute tehnoloogiliste lahenduste välja töötamist ja rakendamist, kapitali- ja omavahendite suurendamist. Kuna tegevusluba annab ettevõtjale õiguse teenuse osutamiseks ning virtuaalvääringu teenuse tegevusloa puhul ei ole tegemist tähtajalise loaga, siis on autori hinnangul tegevusloa omajatel tekkinud ootus, et nad saavad lubatud teenust pakkuda ilma, et õigusraamistik iga paari aasta järel muutuks ning nende äritegevuse jätkamine satuks seadusemuudatuste tõttu korduvalt ohtu.

[130] Erlich, A., Henberg, A., Kask, O. PSK § 31/22. – Eesti Vabariigi põhiseadus. Komm vlj. 5. vlj. Tartu: Sihtasutus Iuridicum 2020.
[131] Financial Action Task Force. Updated Guidance 2021, lk-d 107-108.

Teises situatsioonis on VASP samuti asunud teenust osutama, ent tegevusloa regulatsiooni muudatused pole veel jõustunud. Nimetatud olukord on magistritöö kirjutamise ajal KrÜSi ja MiCA-ga, milles planeeritakse VASPidele uue tegevusloa taotlemise kohustuse kehtestamist, ent kumbki regulatsioon ei ole veel vastu võetud ega jõustunud. Seega ei ole ka VASPidel õiguspärast ootust veel tekkinud. Küll aga on autoril võimalik anda hinnang MiCA kinnitatud teksti, KrÜSi eelnõu ning selle seletuskirja põhjal, kas planeeritavate muudatuste jõustumisel võib tekkida vastuolu VASPi õiguspärase ootuse põhimõttega ning vajadusel teha ettepanekuid selle vältimiseks. Kui isikutele, kel on virtuaalvääringu teenuse osutamiseks tegevusluba, kehtestatakse kohustus taotleda uus tegevusluba, siis vastava kohustuse jõustumisel tekib autori hinnangul VASPidel õiguspärane ootus. Nimelt kord tegevusloa taotlenud ettevõtjal on õigustatud ootus, et läbinud tegevusloa taotlemise protsessi, ei ole vaja seda uuesti korrata regulatsioonide muudatuste tõttu.

Järgmisena tuleb välja selgitada, kas toimunud on õiguspärase ootuse riive. Riigikohtu praktikas domineerib põhimõte, et õiguspärase ootuse põhimõtte kontrollimine toimub põhiõiguse riive põhiseaduspärasuse tuvastamise raames.[132] Kuna eelnevalt selgus, et VASPide subjektiivne õigus teatavale hüvele on õigus osutada tegevusloaga lubatud teenust, mis on kaitstud ettevõtlusvabadusega, siis tuleb järgnevalt hinnata, kas toimunud on ettevõtlusvabaduse riive. Riigikohus tõlgendab ettevõtlusvabaduse kaitseala riivet laialt. Nimelt on Riigikohtu praktika kohaselt tegemist riivega juba siis, kui avalik võim mõjutab ettevõtlusvabadust ebasoodsalt, näiteks siis, kui ettevõtlusega tegelemise tingimusi muudetakse seni kehtinud õigusliku raamistikuga võrreldes ebasoodsamaks.[133] Nagu eelnevalt kirjeldatud, siis VASPide tegevusele kehtestati täiendavad nõudeid, näiteks kapitali ja omavahendite miinimumsuurus, sobivusmenetlus, juhatuse asukoht ja ettevõtte tegevuskoht ning täiendavad hoolsuskohustused. Kuna tegemist on nõuetega, mis piiravad tegevuse osutamist, vara vaba kasutamist, tööjõu ja tegevuskoha vaba valimist, siis on muudatuste näol tegemist ettevõtlusvabaduse riivega. Vastavad piirangud on ettevõtlusvabaduse riivena nimetatud ka PS-i kommentaarides.[134] Kuna korduvad seadusemuudatused on riivanud VASPide ettevõtlusvabadust ning seeläbi on puudunud kindlus õiguskeskkonna püsima jäämisele, siis on tegemist õiguspärase ootuse riivega. Lisaks tekib

[132] Pikamäe, P., lk 701.
[133] RKPJKo 3-4-1-1-02; RKPJKo 3-4-1-27-13.
[134] Kalmo, H., Kask, O. PSK § 10/24;25;28. – Eesti Vabariigi põhiseadus. Komm vlj. 5. vlj. Tartu: Sihtasutus Iuridicum 2020.

ettevõtlusvabaduse riive tulevikus, kui VASPidele kehtestatakse kohustus taotleda uus tegevusluba sisuliselt samal alal teenuse pakkumise jätkamiseks. Ka sel juhul tekib VASPidel ettevõtlusvabaduse riive kaudu õiguspärase ootuse riive.

Viimasena tuleb hinnata avaliku võimu argumente, millega põhjendatakse seaduse muutmise vajadust. Õiguspärane ootus ei ole absoluutne ehk isikute õiguste piiramine ei ole lubamatu, kui seda õigustab avalik huvi. Pikamäe on õiguspärase ootuse põhimõtet selgitanud järgmiselt: „Õiguskindlust tagama pidava õiguspärase ootuse põhimõte ei keela ega saagi keelata riigivõimul kehtivat õigust ümber kujundada ega seda kehtetuks tunnistada. Kuigi seadusandja selline tegevus võib kahjustada õiguse adressaatide õiguspärast ootust olemasoleva normistiku püsimajäämise suhtes, võib see siiski osutuda põhiseaduspäraseks, kui esineb ülekaalukas avalik huvi, mis kaalub üles adressaatide huvi senise olukorra püsimajäämise vastu.“[135] Seega, et selgitada välja, kas õiguspärase ootuse riive on õigustatud, tuleb hinnata, kas avalik huvi kaalub üles VASPi huvi õigusraamistiku püsimajäämise vastu.

Avalik huvi on määratlemata õigusmõiste, ent õiguskirjanduses on mõiste sisustamisel leitud, et avaliku huvi eesmärk on avaliku hüve loomine või säilitamine. Avalik hüve on omakorda miski, „millest on huvitatud riigi kui kogukonna liikmed tervikuna, seejuures ei pea hüve puudutama kõiki kogukonna liikmeid.“[136] Nii Euroopa Liidu kui ka Eesti seadusandjate poolt on avalikuks huviks peetud ka rahapesu ja terrorismi rahastamise tõkestamist.[137] Tõkestamise abil tagatakse finantssektori stabiilsus, usaldusväärsus ja läbipaistvus. 2020. aasta märtsis jõustunud muudatused olid seletuskirja järgi tingitud vajadusest maandada rahapesu ja terrorismi rahastamise riske. Nimelt täheldati puudusi virtuaalvääringu tegevusloa regulatsioonis ning nenditi, et rahapesu ja terrorismi rahastamise riskid on hüppeliselt tõusnud, kuna turule sisenemise lävend on madal. Täiendavate nõuete eesmärk oli tugevdada järelevalve teostamist ja tegevusloamenetlust ning seeläbi taastada virtuaalvääringu teenuse pakkujate üle kontroll.[138] Seetõttu kehtestati muu hulgas

[135] Pikamäe, P., lk 706.
[136] Ikkonen, K. Avalik huvi kui määratlemata õigusmõiste. – Juridica 2005/3, lk 194.
[137] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/848, 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 141/73, pp 44; RahaPTS 507 SE seletuskiri, lk 18.
[138]Rahapesu ja terrorismi rahastamise tõkestamise seaduse ning riigilõivuseaduse muutmise seadus 8 SE. Eelnõu. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/24832445-95e0-4ffc-adbe-ec44d87d5eb1/rahapesu-ja-terrorismi-rahastamise-tokestamise-seaduse-ning-riigiloivuseaduse-muutmise-seadus (25.03.2023); Rahapesu ja terrorismi rahastamise tõkestamise seaduse ning riigilõivuseaduse muutmise seadus 8 SE. Seletuskiri. –

nõue, et VASPi kontaktisik, registrijärgne asukoht, juhatuse asukoht ja tegevuskoht peavad olema Eestis või kui tegemist on välisriigi ettevõtjaga, peab ta tegevusloa taotlemiseks Eestis avama filiaali. Kuna ettevõtja tegevuskoht on see, kus toimub teenuse osutamine ja kus täidetakse peamisi juhtimis- ja kontrollfunktsioone, siis nende üle tõhusa järelevalve tegemiseks on oluline, et tegevuskoht asuks järelevalve asutusega samas riigis ehk Eestis. Ka kontaktisiku Eestis asumise nõue täidab tõhusama järelevalve eesmärki, kuna sel juhul on RABil kontaktisikuga lihtsam ühendust saada ja tagada kiirem ligipääs uurimis- või järelevalve tegevuses vajalikele andmetele. Kokkuvõttes olid 2020. aasta märtsis jõustunud RahaPTSi muudatused tingitud kiireloomulisest vajadusest maandada märkimisväärselt tõusnud rahapesu ja terrorismi rahastamise riske VASPi tegevusvaldkonnas ja saavutada tõhus järelevalve VASPide tegevuse üle. Kehtestatud muudatuste kaudu oli seadusandja eesmärk tagada VASPide sektoris, aga ka üldisemalt kogu finantssektoris, stabiilsus ja usaldusväärsus, mis on oluline avalik huvi. Kuna järelevalveasutusel ei olnud varasemalt kehtinud seaduse alusel piisavalt võimalusi, et teostada tõhusat järelevalvet ning kõrged riskid olid maandamata, siis kaalus avalik huvi autori hinnangul VASPide subjektiivsed õiguses üles ning kehtestatud muudatused, mis riivasid VASPide õiguspärast ootust, olid põhiseaduspärased.

2022. aasta märtsis jõustunud muudatused olid seletuskirja järgi tingitud aastal 2021 avaldatud Eesti riikliku riskihinnangu tulemustest. Nimelt tuvastati, et kehtivad VASPide tegevusloa nõuded ei ole piisavad, et maandada virtuaalvääringu teenuse pakkumisest tulenevaid rahapesu ja terrorismi rahastamise riske. Virtuaalvääringu teenuse pakkujate sektori usaldusväärsuse ja läbipaistvuse suurendamiseks lisati nõudeid, mis annaksid järelevalveasutusele tegevusloa taotlejate ja omajate kohta rohkem infot, et teha informeeritud otsus tegevusloa andmise, sellest keeldumise või kehtetuks tunnistamise kohta. Samuti tagasid uued nõuded VASPide kapitaliseerituse ja kompetentse juhtimise. Näiteks kehtestati ettevõtja juhtorgani liikmele ja prokuristile sobivusmenetluse läbimise kohustus, mille raames hinnatakse, kas isik on sobiv pakkuma avalikkusele kõrgendatud hoolikust ja usaldusväärsust nõudvaid teenuseid ja tema ärialast mainet. Selleks hinnatakse isiku teadmisi, oskusi, kogemusi, haridust ja kutsealast sobivust. Finantsinspektsiooni juhatuse liikme Siim Tammeri sõnul tagavad kõrgendatud nõuded juhtidele või muu seadusega oluliseks peetavale isikule finantssektori suurema aususe, läbipaistvuse ja

https://www.riigikogu.ee/tegevus/eelnoud/eelnou/24832445-95e0-4ffc-adbe-ec44d87d5eb1/rahapesu-ja-terrorismi-rahastamise-tokestamise-seaduse-ning-riigiloivuseaduse-muutmise-seadus (25.03.2023).

ennetab finantssektori kuritegelikel eesmärkidel ära kasutamist.[139] Seega ka 2022. aasta märtsis jõustunud muudatused olid tingitud pakilisest vajadusest maandada rahapesu ja terrorismi rahastamise riske, sest eelnevalt kehtinud nõuded ei olnud selleks piisavad. Autori hinnangul oli rangemate nõuete kehtestamine VASPi sektoris suurel määral vajalik ka Moneyval hindamise edukaks läbimiseks. Kui hindamise tulemusel oleks Eesti sattunud nn „FATFi halli nimekirja", kuhu kuuluvad riigid, kus on nõrk rahapesu ja terrorismi rahastamise tõkestamise regulatsioon, siis oleks see Eestile tähendanud suurendatud järelevalvet FATFi poolt, täiendavat halduskoormust, mainekahju ja raskendatud rahvusvaheliste ärisuhete loomist. 2023. aasta jaanuaris avaldatud Moneyval raporti[140] kohaselt tunnustati Eestit jõupingutuste eest riskide maandamisel. Kuna seadusemuudatused on põhjendatavad avaliku huviga tõkestada Eestis rahapesu ja terrorismi rahastamist ning tagada finantskeskkonna usaldusväärsus, läbipaistvus ja stabiilsus, siis oli riive VASPide õiguspärasele ootusele, et õiguskeskkonna püsiks stabiilne, põhiseaduspärane.

Tegevusloa nõuete muutmine ja täiendamine on aidanud maandada teatud rahapesu ja terrorismi rahastamise riske. Nõue, et VASPi asukoht, tegevuskoht, juhatuse asukoht ja kontaktisik(ud) peavad asuma Eestis, maandab riski, et VASPidel pole reaalset seost Eestiga. Erinevalt eelnevast olukorrast, kus enamik Eesti VASPide tegevuskoht, juhatus, töötajad ja kliendid asusid välismaal, on nüüd VASPid Eestiga tugevamalt seotud ning RABil on võimalik teostada nende üle tõhusamat järelevalvet. Nõuded, mille kohaselt tuleb RABile anda lisateavet VASPi juhatuse liikmete tausta, planeeritava äritegevuse ja tehniliste süsteemide toimivuse jm kohta aitab teha informeeritud otsuseid tegevusloamenetluses ehk maandab riski, et tegevusloa saavad isikud, kel puuduvad võimalused, vahendid ja teadmised nõuetekohaseks teenuse pakkumiseks. Nagu eelnevalt välja toodud, siis aastal 2019. väljastas RAB rekordilised 1304 VASPi tegevusluba. Majandustegevuse registrist[141] nähtub, et aastal 2022 on väljastatud kolm ja 2023. aasta aprilli seisuga kaks VASPi tegevusluba. See tähendab, et karmistunud nõuded on turule sisenemise teinud keerulisemaks, mis täidab eesmärki, et VASPi tegevusluba ei anta isikutele, kes ei suuda täita rahapesu ja terrorismi rahastamise tõkestamise nõudeid. Samuti lisati juurde tegevusloa kehtetuks tunnistamise aluseid, mistõttu on hakatud maandama riski, et turul tegutsevad jätkuvalt RahaPTS-is sätestatud nõudeid mittejärgivad VASPid. Näiteks aastal 2020 tunnistas RAB kehtetuks 1808 tegevusluba, aastal 2021

[139] Tammer, S. Sobivusest sobimatuseni finatntssektoris. – Juridica 2015/5, lk 318.
[140] Moneyval. Anti-money laundering and counter-terrorist financing measures – Estonia: Fifth Round Mutual Evaluation Report. (2022, lk 8) – https://rm.coe.int/moneyval-2022-11-mer-estonia/1680a9dd96 (16.03.2023).
[141] Tarbijakaitse ja Tehnilise Järelevalve Amet. Majandustegevuse register. – https://mtr.ttja.ee/taotluse_tulemus (12.04.2023).

veel 331 tegevusluba ja aastal 2022 lisaks 182 VASPi tegevusluba.[142] Eelkirjeldatust nähtub, et tegevusloa nõuete karmistamine ja lisamine on rahapesu ja terrorismi rahastamise riskide maandamisele kaasa aidanud. Küll aga ei ole see piisav, kuna eelnevast analüüsist selgus, et riskid seoses tehingu vastaspoole tuvastamise ja VASPide kohustuste mittenõuetekohase täitmisega on veel maandamata.

Heites pilgu tulevikku, siis VASPidel tuleb MiCA jõustumisel oma tegevuse jätkamiseks taotleda uus tegevusluba. Nagu eelnevalt selgitatud, siis KrÜSi eelnõu kohaselt hakkab tegevusloa väljastamisega tegelema Finantsinspektsioon. Eelnõu järgi tuleb uue tegevusloa saamiseks edastada Finantsinspektsioonile kirjalik taotlus ja kõik tegevusloa saamiseks vajalikud andmed ja dokumendid. MiCA jõustumisel on vastavad andmed ja dokumendid nimetatud krüptovaraturgude määruses. Autori hinnangul on ebaproportsionaalne nõuda VASPidelt täismahus tegevusloa taotlemise läbimist ja kõikide andmete uuesti esitamist, kui nad on sisuliselt sama teenuse osutamiseks juba tegevusloa saanud. Näiteks juhul, kui VASP on tegelenud virtuaalvääringu vahetamise teenusega ning muutub üksnes teenuse nimetus – krüptovara vahetamise teenuseks. Seda enam, et 2022. aasta märtsis jõustunud RahaPTS-i redaktsiooniga on MiCA nõuded suures osas üle võetud. Seega kehtivate VASPi tegevuslubade omajad on enamus MiCA nõuetele vastavust juba tõestanud.

Autori hinnangul tuleb VASPidele kehtestada lihtsustatud MiCA tegevusloa taotlemise menetlus. Nimelt ei peaks VASP esitama uuesti andmeid, mis on juba majandustegevuse registrisse VASPi tegevusloa taotlemisel esitatud või mis on kättesaadavad e-äriregistrist või teistest avalikest andmebaasidest. Näiteks ei peaks esitama uuesti äriühingu põhikirja, organisatsioonilise ülesehituse ja juhtimisstruktuuri kirjeldust, sobivuse hindamiseks esitatud dokumente, mis sisaldavad juhtorgani liikmete haridustaset, töö- ja ametikohtade loetelu ning dokumente, mis tõendavad juhtorgani liikmete usaldusväärsust ja korrektset ärialast mainet, kui asjaolud pole muutunud. Olemasolevate andmete kasutamiseks tuleb Finantsinspektsioonile tagada juurdepääs majandustegevus registris sisalduvatele andmetele. Alternatiivselt saab RAB saata Finantsinspektsioonile vajalikku teavet ja dokumente X-tee ehk tehnilise keskkonna kaudu, mis võimaldab turvalist andmevahetust nii riigiasutuste vahel kui ka erasektoriga. Andmete töötlemisel

[142] Rahapesu Andmebüroo. Rahapesu Andmebüroo aastaraamat 2020. (2020, lk 7) – https://fiu.ee/aastaraamatud-ja-uuringud/aastaraamatud (19.02.2023); Rahapesu Andmebüroo aastaraamat 2021, lk 30; Rahapesu Andmebüroo aastaraamat 2022, lk 46.

tuleb lähtuda nii isikuandmete kaitse üldmäärusest[143] kui ka isikuandmete kaitse seadusest[144]. Lisaks on avalike andmete topelt küsimine vastuolus avaliku teabe seaduse § 43[1] lg-s 3 sätestatud andmete ühekordse küsimise põhimõttega. VASPid peaksid esitama üksnes neid dokumente ja andmeid, mis on ajakohastatud ja mida on tulenevalt MiCA nõuetest juurde vaja. Olemasolevate ning jätkuvalt aktuaalsete andmete ja dokumentide puhul tuleks VASPidel lisada üksnes viide asjakohasele andmekogule, kus andmed ja dokumendid on kättesaadavad. Lihtsustatud tegevusloa taotlemise menetluse kehtestamisel väheneks ettevõtja halduskoormus ning see oleks kooskõlas andmete ühekordse küsimise põhimõttega.

Kokkuvõttes on autori hinnangul tehtud ettevõtja perspektiivist ebasoodsaid seadusemuudatusi, mis riivavad ettevõtlusvabadust ja õiguskeskkonna stabiilsuse puudumise tõttu ka õiguspärast ootust. Kuna seadusemuudatuste tegemisel on lähtutud kaalukast avalikust huvist ehk eesmärgist maandada rahapesu ja terrorismi rahastamise riske ning seeläbi tagada finantssektori stabiilsus, usaldusväärsus ja läbipaistvus, siis on VASPide õiguspärase ootuse riive põhiseaduspärane. Tegevusloa tingimuste muutmine ja täienemine on erinevate rahapesu ja terrorismi rahastamise riskide maandamist soodustanud, ent eelnevast analüüsist lähtudes on selge, et eksisteerib veel riske, mis vajavad maandamist. Samuti teeb autor lähtuvalt eeltoodud põhjendustest ettepaneku kehtestada lihtsustatud tegevusloa taotlemise protsess eesootava MiCA tegevusloa taotlemiseks. Lihtsustatud protsess täidaks nii andmete ühekordse esitamise eesmärki kui ka vähendaks ettevõtja halduskoormust.

3.2. Riigilõivu suurus ja virtuaalvääringu teenuste riskide maandamine

Eelnevate aastate jooksul on toimunud järsk tõus virtuaalvääringu teenuse tegevusloa taotluse läbivaatamise ja tegevusloa muutmise riigilõivus. Kui 2020. aasta märtsis jõustunud muudatustega tõsteti tegevusloa taotluse läbivaatamise riigilõivu ligi kümnekordselt ehk 325 eurolt 3300 euroni, siis kaks aastat hiljem otsustati riigilõivu tõsta veelgi ligi kolmekordselt ehk kehtiv tegevusloa läbivaatamise riigilõiv on riigilõivuseaduse[145] (edaspidi RLS) § 269 lg 1 p 3 alusel 10 000 eurot. See tähendab, et võrreldes 2020. aasta alguse riigilõivu suurusega on virtuaalvääringu teenuse

[143] Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). ELT L 119/1.
[144] Isikuandmete kaitse seadus. – RT I, 04.01.2019, 11.
[145] Riigilõivuseadus. – RT I, 14.03.2023, 32.

tegevusloa taotluse läbivaatamise riigilõiv tõusnud 30-kordselt. Lisaks kehtestati VASPidele 2022. aastal esmakordselt tegevusloa muutmise taotluse läbivaatamise riigilõiv. Tegevusloa muutmise eest tuleb tasuda RLS § 269 lg 2 alusel 4000 eurot. Seejuures on RLS §-s 51^2 sätestatud erand, mil VASP on riigilõivu tasumisest vabastatud. Riigilõivu ei tule tasuda juhul, kui tegevusloa muutmine hõlmab üksnes ettevõtja asukoha aadressiandmete muutmist Eesti piires. Seega on tegevusloa muutmise riigilõiv alates 2022. aastast tõusnud nullist eurost 4000 euroni. Riigikohtu praktika kohaselt riivab riigilõivu tasumise kohustus nii ettevõtlusvabadust[146] kui ka omandipõhiõigust, kuna selle tasumine vähendab isiku vara ja takistab seeläbi vara vaba kasutamist[147]. Nii PS §-s 31 sätestatud ettevõtlusvabadust kui ka PS §-s 32 sätestatud omandipõhiõigust on võimalik seadusega piirata, ent see peab toimuma põhiseaduspäraselt. Tulenevalt asjaolust, et lühikese aja jooksul on VASPidele kohalduvaid riigilõivusid tõstetud järsult ebasoodsas suunas, hindab autor järgnevalt, kas kehtivad riigilõivu suurused on proportsionaalsed või on tegemist ülemääraste nõuetega ettevõtlusvabaduse ja omandipõhiõiguse suhtes. Samuti uurib autor, kuidas täidab kõrge riigilõivu nõue rahapesu ja terrorismi rahastamise maandamise eesmärki.

PS § 11 kohaselt peavad seadusandja kehtestatud piirangud olema põhiseaduspärased ehk vajalikud ning need ei tohi moonutada piiratavate õiguste ja vabaduste olemust. Nõuete põhiseaduspärasuse kontroll hõlmab nii formaalsete kui materiaalsete nõuete täitmise kontrolli. Kuna seadusandja on järginud riigilõivude kehtestamisel pädevus, menetlus- ja vorminõudeid, siis on vastavad sätted formaalselt põhiseaduspärased. Küll aga on täpsemalt vaja hinnata materiaalsete ehk sisuliste nõuete täitmist. Materiaalse seaduspärasuse kontrollimiseks tuleb kohaldada Riigikohtu praktikas väljakujunenud proportsionaalsuse testi. Selgitamaks välja, kas kehtiv riigilõivu nõue kui ettevõtlusvabaduse ja omandipõhiõiguse riive on proportsionaalne, tuleb hinnata, kas riive on eesmärgi saavutamiseks sobiv, vajalik ja mõõdukas.

Esmalt tuleb välja selgitada riigilõivu kehtestamise eesmärk. Riigilõiv on riigilõivuseaduses sätestatud tasu, millele vastab konkreetne vastusooritus, näiteks taotluse läbivaatamine, haldusakti andmine või dokumendi väljastamine. Riigikohus on sisustanud riigilõivu eesmärgi järgmiselt: „ […] kuna riigilõivumäär kehtestatakse RLS § 4 lõike 1 järgi lähtuvalt toimingu tegemisega kaasnevatest kuludest (kulupõhimõte), on riigilõivu esmaseks eesmärgiks riigi tehtava avalik-õigusliku toimingu kulutuste täielik või osaline hüvitamine toimingu osalise poolt. Lisaks tuleneb

[146] RKÜKo 3-2-1-62-10; RKÜKo 3-3-1-33-11.
[147] RKPJKo 3-4-1-26-13.

RLS § 4 lõikest 2 võimalus kehtestada riigilõivumäär toimingu eesmärgist, toimingust saadavast hüvest ja kaalukast avalikust huvist lähtuvalt kulupõhimõttest erinevalt. Riigilõivu regulatsiooni eesmärgiks peab üldkogu ka menetlusökonoomiat.“[148] RahaPTS 507 SE seletuskirja kohaselt on virtuaalvääringu teenuse tegevusloa taotluse läbivaatamise riigilõivu tõstetud mitmekordselt, et katta toimingutega kaasnevaid kulusid, ennetada tegevusloa andmist isikutele, kelle eesmärgid on seotud kuritegevusega ja tagada menetlusökonoomia ehk vähendada taotluste läbivaatamisega kaasnevat halduskoormust ja kulusid.[149] Virtuaalvääringu teenuse tegevusloa muutmise riigilõiv on määratud eesmärgiga katta muutmise menetlusega kaasnevaid kulusid. Järgnevalt hindab autor, kas 10 000-eurone ja 4000-eurone riigilõiv vastavalt tegevusloa taotluse läbivaatamiseks ja muutmiseks on sobiv, vajalik ja mõõdukas abinõu, et saavutada seadusandja poolt eelkirjeldatud eesmärke.

Sobivuse kriteeriumi kontrollimisel tuleb välja selgitada, kas põhiõiguse piirang soodustab eesmärgi saavutamist. Riigikohus on selgitanud, et põhiõiguse piirang, mis ei soodusta ühelgi juhul eesmärgi saavutamist on selgelt ebaproportsionaalne.[150] Seega sobivuse kriteeriumi täitmiseks piisab, kui määratud riigilõivud aitavad kasvõi osaliselt kaasa eelnimetatud eesmärkide saavutamisele. Ka Saksa Liidukonstitutsioonikohtu praktika kohaselt ei ole sobivuse kriteeriumi täitmiseks vajalik eesmärgi täielik täitmine.[151] Kõrge rahapesu ja terrorismi rahastamise riski maandamiseks virtuaalvääringu teenuse pakkumise tegevusalal on VASPi tegevusloa nõudeid karmistatud ja juurde lisatud. Seega on tõusnud nii tegevusloa menetluse kontrollesemete arv kui ka kontrollimise keerukus, mis on omakorda tinginud suuremad tegevusloa menetluskulud. Kõrge riskiga tegevusala tegevusloa kontrollesemete tõhus ja kvaliteetne kontrollimine vajab suuremat ressurssi, mistõttu on oluline, et riigilõiv kataks toimingutega kaasnevad kulud. Autori hinnangul ei saa väita, et 10 000 euro suurune riigilõiv ei aita katta toimingutega kaasnevaid kulusid. Isegi, kui kulu peaks ületama määratud suuruses riigilõivu, siis täidab see kulude katmise eesmärki osaliselt, mis on sobivuse kriteeriumi täitmiseks piisav. Kõrge riigilõiv täidab samuti (vähemalt osaliselt) eesmärki hoida finantsturgudelt eemal kurjategijaid. Kuna tegevusloa omandamine on Eestis muutunud kulukaks, siis valitakse tegevusloa taotlemiseks, sealhulgas pahatahtlikel eesmärkidel, pigem riik, kus tegevusloa taotlemine on soodsam. Kahanev tegevusloa taotlemiste

[148] RKÜKo 3-3-1-22-11.
[149] RahaPTS 507 SE seletuskiri, lk-d 33-34.
[150] RKPJKo 3-4-1-1-02.
[151] Lübbe-Wolf, G. Proportsionaalsuse põhimõte Saksa Liidukonstitutsioonikohtu praktikas. – Juridica 2021/Riigiõiguse aastaraamat 2021, lk-d 291-292.

arv vähendab ka taotluste läbivaatamisega kaasnevat halduskoormust ja kulusid. Seega soodustab kõrgem riigilõiv ka menetlusökonoomia eesmärki. Kuna kõrge riigilõiv soodustab vähemalt osaliselt nii kulude katmise eesmärgi saavutamist, ennetusfunktsiooni täitmist kui ka menetlusökonoomia tagamist, siis on tegemist sobiva abinõuga. Lisandunud tegevusloa nõuded on tinginud olukorra, kus VASPid peavad tegevuse jätkamiseks taotlema tegevuslubade muutmist. Uutele tegevusloa nõuetele vastamist tuleb põhjalikult kontrollida, et turul ei tegutseks VASPid, kes ei suuda virtuaalvääringu teenuse pakkumisega kaasnevaid riske maandada. Suurenenud halduskoormus on tõstnud tegevusloamenetluse kulusid. Autori hinnangul tuleb ka siinkohal tõdeda, et 4000 euro suurune riigilõiv aitab katta tekkinud kulusid. Seega ka riigilõivu muutmise taotluse riigilõiv on sobiv.

Põhiõiguse piirang on Riigikohtu praktika järgi vajalik, kui„ […] eesmärki ei ole võimalik saavutada mõne teise, kuid isikut vähem koormava abinõuga, mis on vähemalt sama efektiivne kui esimene.“[152] RahaPTS 507 SE seletuskirja kohaselt polnud endine 3300-eurone riigilõiv piisav, et katta tegevusloa läbivaatamisega kaasnevaid kulusid.[153] Samas pole selgitatud, kuidas jõuti seisukohale, et 10 000-eurone riigilõiv on optimaalseim suurus. Näiteks krediidiasutuse tegevusloa taotlemise eest tuleb tasuda menetlustasu 1500 eurot, investeerimisühingu või makse- ja e-raha asutuse tegevusloa taotlemise eest 1000 eurot. Kuna eelloetletud turuosaliste puhul tuleb tegevusloa taotlemisel samuti vastata paljudele keerulistele ja suurt ressurssi vajavatele nõuetele ning tegevusloa nõuetele vastamise kontrollimine on järelevalve asutusele mahukas töö, siis on ebaselge, miks on VASPidele kehtestatud riigilõiv ligi 6-10 korda suurem. Seda enam, et ka eelnimetatud turuosalised on kohustatud isikud RahaPTS-i mõttes ja peavad samuti rakendama rahapesu ja terrorismi rahastamise tõkestamise meetmeid. Ka teistele finantseerimisasutustele, kellele RAB väljastab tegevusloa, on riigilõiv madalam – 3300 eurot. Seega on autori hinnangul tõenäoline, et tegevusloa taotluse läbivaatamiseks ei pruugi 10 000-eurone riigilõiv olla vajalik, vaid kulusid on võimalik katta ka väiksema riigilõivuga.

Teine eesmärk on RahaPTS 507 SE seletuskirja kohaselt kõrgema riigilõivuga ennetada potentsiaalseid kuritegusid: „Liiga madal lävend tegevusloa saamiseks saab rahvusvahelist tähelepanu, mille tulemusel võib kannatada Eesti maine, sest tegevusloa võivad väga kergesti saada

[152] RKPJKo 3-4-1-16-08.
[153] RahaPTS 507 SE seletuskiri, lk 33.

ka isikud, kelle eesmärgid on seotud kuritegevusega.“[154] Autori hinnangul on vastavat eesmärki võimalik saavutada ka väiksem riigilõivuga. Paljudes Euroopa Liidu riikides ei ole üldse tegevusloa taotlemise riigilõivu kehtestatud. Riikides, kus on taotluse eest määratud tasu, on see valdavalt madalam kui 10 000 eurot. Näiteks tuleb Itaalias[155] tasuda 8300 eurot, Belgias[156] 8000 eurot ja Hollandis[157] 5000 eurot. Autor nõustub, et pahatahtlikud isikud võivad taotleda tegevusluba kuritegevuslikel eesmärkidel pigem kohtades, kus tegevusloamenetluse eest peab vähem tasuma, ent tõenäoliselt soodustab ennetamise eesmärki ka madalam riigilõiv kui 10 000 eurot.

Seletuskirjas on välja toodud, et kõrgem riigilõiv maandab ka riske, mis on seotud Eesti valmisettevõtete, millel on virtuaalvääringu tegevusluba, müümist. Nimelt on RAB täheldanud järgnevat tegevusmustrit: „Esialgse tegevusloa taotlemise käigus jäetakse RABile ekslik arusaam, et ettevõte hakkab tegevusloa saamisel teenust osutama. Tegelikkuses aga loobub enamik ettevõtteid tegevusloa saamisel ajutiselt tegevusest kuni ettevõtte müügini. Müügi korral esitatakse RABile tegevusloa muutmise taotlus, mille menetlemisel peab RAB kontrollima kõiki asjaolusid sarnaselt esmase tegevusloataotluse menetlemisega.“[158] Autori hinnangul on valmisettevõtete müügist tulenev risk maandatud juba teiste 2022. märtsis jõustunud muudatustega. Kui varasemalt oli VASPi tegevusloa saamine võrdlemisi lihtne, siis nüüd on tehtud turule sisenemine keeruliseks: kõrged kapitali miinimumnõuded (vähemalt 100 000 eurot), kõrgendatud nõuded tegevuskohale (peab olema Eestis) ja juhatuse liikmetele (kõrgharidusega ja vähemalt 2-aastane erialane töökogemus) ja muudki. Ehk tegevusloa saamine üksnes müümise eesmärgil on muutunud ressursimahukaks ja kulukaks. Samuti on RahaPTS § 70 lg 3^2 p 3 alusel kehtestatud äriplaani esitamise kohustus, mis annab järelevalveasutusele teavet, kas ettevõtja plaanib hakata VASPina tegutsema poole aasta jooksul alates tegevusloa väljastamisest. Kui selgub, et selle aja jooksul virtuaalvääringu teenuseid ei pakuta, on RABil õigus RahaPTS § 75 lg 1 p 3 järgi tunnistada tegevusluba kehtetuks. Lisaks on RahaPTS § 72^6 järgi VASPidele keelatud majandustegevusest

[154] RahaPTS 507 SE seletuskiri, lk 33.
[155] Lexia Avvocati. How to get an Italian VASP licence. (2023) – https://www.lexia.it/en/how-to-get-italian-vasp-license/ (03.03.2023).
[156] Eversheds Sutherland. Virtual asset service providers subject to new registration requirements in Belgium. (2022) – https://www.eversheds-sutherland.com/global/en/what/articles/index.page?ArticleID=en/global/belgium/en/Virtual_Currency_Decree (03.03.2023).
[157] Overheid. Scheme for funding financial supervision for one-off actions. (2020, Wwft.D1.01) – https://wetten.overheid.nl/BWBR0041647/2020-05-21 (03.03.2023).
[158] RahaPTS 507 SE seletuskiri, lk 33.

ajutine loobumine, mistõttu ei saa nad valmisettevõtete puhul jääda kauemaks kui pooleks aastaks ootama ettevõtte müümist ilma ise tegevust alustamata. Autori hinnangul on aga kõige tõhusamaks valmisettevõtete müügist tuleneva riski maandamise meetmeks RahaPTS §70 lg-s 4^1 sätestatu, et VASPi tegevusluba ei saa teisele isikule üle anda. See tähendab, et tegevusluba ei saa anda isikule, kes ei vasta RahaPTS-is sätestatud nõuetele, ettevõtte võõrandamisel peab ka uus ettevõtja vastama kehtestatud tingimustele. Seeläbi maandatakse riski, et tegevusloa saab ettevõtja, kes pole sobiv ja usaldusväärne virtuaalvääringu teenuse pakkumiseks. Eelnevast tulenevalt ei ole autori hinnangul 10 000-eurone riigilõiv vajalik abinõu, et ennetada tegevusloa taotlemist pahatahtlikul eesmärgil või valmisettevõtete müüki, kuna on olemas teised nõuded, mis vastavat eesmärki tõhusamalt täidavad.

Kolmanda eesmärgi ehk menetlusökonoomia kohaselt peaks 10 000-eurone riigilõiv tegevusloa taotluse läbivaatamiseks vähendama eelduslikult taotluste esitamist ja sellega kaasnevat halduskoormust ning kulusid. Puudub avalik info, mitu VASPi tegevusloa taotlust on aastate lõikes esitatud, ent avaldatud on väljastatud tegevuslubade arv. Kui aastal 2020 väljastati 325 tegevusluba ja 2021. aastal 86 tegevusluba[159], siis majandustegevuse registrist[160] nähtub, et virtuaalvääringu teenuse pakkumise tegevuslubasid on aastal 2022 antud kolm ja 2023. aasta aprilli seisuga kaks. See tähendab, et aastate jooksul on väljastatud tegevuslubade arv vähenenud, seejuures tõenäoliselt ka tegevusloa taotluste esitamise arv. Küll aga ei tulene see arvatavasti üksnes kõrgest riigilõivust, vaid ka teistest kõrgendatud nõuetest. Ka RahaPTS 507 SE seletuskirjas on leitud, et kõrgem riigilõiv koos karmistatud tegevusloa nõuetega vähendab eelduslikult uute tegevusloa taotluste esitamist.[161] Kuna menetlusökonoomia eesmärki saavutatakse lisaks riigilõivule ka teiste nõuetega, mis vajavad tunduvalt rohkem ressurssi (nt miinimum 100 000-eurone kapitalinõue, tööjõukulu, IT-tehnoloogiate välja arendamine), kui 10 000 euro suurune riigilõiv, siis tõenäoliselt oleks eesmärk täidetud ka väiksema riigilõivuga.

Autor on eeltoodud argumentidest lähtudes seisukohal, et kulude katmise, ennetamise ja menetlusökonoomia eesmärgi suhtes ei ole 10 000 euro suurune riigilõiv vajalik. Tõenäoliselt on eelnimetatud eesmärke võimalik saavutada ka väiksema summaga. Täpse summa välja arvutamine

[159] Rahapesu Andmebüroo uuring 2022, lk 14.
[160] Tarbijakaitse ja Tehnilise Järelevalve Amet. Majandustegevuse register. – https://mtr.ttja.ee/taotluse_tulemus (12.04.2023).
[161] RahaPTS 507 SE seletuskiri, lk 37.

vajab eraldi analüüsi, mis ei kuulu käesoleva töö käsitlusalasse. Küll aga tuleks autori hinnangul riigilõivu määramisel võtta arvesse ka teistes riikides kehtestatud tasude summasid, et ühtlustada tegevusloa menetlustasude taset ja vältida olukorda, kus Eestis on kõrgema riigilõivu tõttu äritegevuse alustamine põhjendamatult ebasoodsam.

Vajalikkust tuleb hinnata ka tegevusloa muutmise riigilõivu kontekstis. Tegevusloa andmisel hinnatakse, kas tegevusloa taotleja vastab kõikidele RahaPTS §-s 72 sätestatud kontrolliesemetele. Kui tegevusluba on saadud, aga kontrollesemetest midagi hiljem muutub, näiteks vahetub kontaktisik, tuleb RABile esitada tegevusloa muutmise taotlus ning tasuta selle eest riigilõivu 4000 eurot. Nagu eelnevalt mainitud, siis on kehtestatud erand, et riigilõivu ei pea tasuma, kui muuta on vaja üksnes ettevõtja asukoha aadressiandmeid Eesti piires. Vastasel juhul oleks tegemist selgelt ülemäärase nõudega, kuna tegevusloas aadressiandmete muutmine ei too kaasa erinevalt ettevõtja esitatud sise-eeskirjade hindamisest või hoolsusmenetluse läbiviimisest märkimisväärset ajalist ega rahalist kulu. Seadusandja on leidnud, et vastava muudatuse tegemiseks on ressursikulu nii väike, et ettevõtjad on sellest sootuks vabastatud. Sama lähenemist tuleks autori hinnangul kohaldada ka RahaPTS §-s 72 lg 1 p 5-s kehtestatud VASPi maksekontole nõudele. Nimelt peab VASPi tegevusloa ettevõtjal olema maksekonto, mis on avatud krediidiasutuses, e-raha asutuses või makseasutuses, mis on asutatud Eestis või Euroopa Majanduspiirkonna lepinguriigis ja osutab Eestis teenuseid piiriüleselt või mis on asutanud Eestis filiaali. Sarnaselt aadressile tuleb autori hinnangul riigilõivust vabastamise erand kehtestad ka maksekonto muutumisel, kuna tegemist on üksnes formaalse muudatusega, mis ei too kaasa 4000 euro suurust kulu. Seega 4000 euro suurune riigilõiv ei ole vajalik olukordades, kus muudatused on üksnes formaalsed ja vajavad väga vähe ressurssi.

Mõõdukuse kriteeriumi hindamisel tuleb väljakujunenud kohtupraktika järgi: „ […] kaaluda ühelt poolt põhiõigusse sekkumise ulatust ja intensiivsust ning teiselt poolt eesmärgi tähtsust. Mida intensiivsem on põhiõiguse riive, seda kaalukamad peavad olema seda õigustavad põhjused.“[162] Nagu eelnevalt kirjeldatud, siis riigilõiv riivab nii ettevõtja ettevõtlusvabadust kui ka omandipõhiõigust. PS § 11 kohaselt ei tohi põhiõigusi riivata rohkem, kui see on normi legitiimse eesmärgiga põhjendatav. Tuginedes eeltoodud argumentidele leiab autor, et 10 000 euro suurune riigilõiv on kulutuste katmise, menetlusökonoomia ja ennetusfunktsiooni täitmiseks sobiv ehk see soodustab vähemalt osaliselt nimetatud eesmärkide saavutamist, aga tegemist pole vajaliku

[162] RKÜKo 5-18-8/19.

abinõuga. Erinevalt VASPidest on Eesti krediidi- ja finantseerimisasutustele, kelle tegevusloa menetlus on sarnaselt VASPi omale ressursimahukas, kehtestatud kordades madalamad tegevusloa menetlemise tasud. Valdavalt on ka teistes Euroopa Liidu liikmesriikides kehtestatud madalamad tasud kui Eestis. Seadusandja on selgitanud, et 3300 euro suurune riigilõiv ei kata tegevusloamenetluse kulusid, ent põhjendamata on jäänud 10 000 euro suuruse riigilõivu vajalikkus ja mõõdukus. Samuti leidis autor eelnevalt, et seadusandja kirjeldatud eesmärgid nagu ennetus, et tegevuslubasid ei taotletaks pahatahtlikel või müügi eesmärgil, ning halduskoormuse vähendamine, on juba teiste kehtestatud nõuete kaudu saavutatavad.

Kuna ennetamise ja menetlusökonoomia eesmärgid on täidetavad teiste kehtivate nõuetega ehk vastavad põhjendused 10 000 euro suuruse riigilõivu sätestamiseks ei ole arvestatavad ning seadusandja ei ole põhjendanud, kuidas jõuti järeldusele, et just 10 000 eurot on vaja, et katta tegevusloa menetlusega kaasnevad kulud, siis on autori hinnangul võimalik, et tegemist pole mõõduka abinõuga. Seda enam, et välisriigis asuvate VASPide ja Eestis asuvate teiste krediidi- ja finantseerimisasutuste tegevusloa taotlemise tasude näitel on võimalik järeldada, et tegevusloa menetlust on võimalik läbi viia väiksemate kuludega. Tegevusloa karmistatud nõuded on ettevõtjatele niigi VASPi tegevusloa taotlemise muutnud keerulisemaks, mida tõestab eelkirjeldatud vähene tegevuslubade väljastamine. Riigilõivu küsimine osas, mis ületab tegelikke kulusid, ei ole eesmärgipärane ehk takistaks põhjendamatult ettevõtjatel virtuaalvääringu teenuse sektorisse sisenemist ehk ettevõtlusvabadust ja vara vaba kasutamist ehk omandipõhiõigust. Riigilõivu suurus, mis piirab rohkem põhiõigusi, kui see on normi eesmärgiga põhjendatav, on ebaproportsionaalne meede. Autori hinnangul tuleb välja selgitada mõõdukas riigilõiv, mis kataks tegevusloamenetluse kulud, aga ei riivaks liigselt ettevõtja ettevõtlusvabadust ja omandipõhiõigust.

Tulenevalt eeltoodud käsitlusest, on autori hinnangul 4000 euro suurune riigilõiv sobiv abinõu, et katta tegevusloa muutmisega kaasnevaid kulusid, ent tegemist ei ole igas situatsioonis vajaliku abinõuga. Olukordades, kus tegevusloa muutmine piirdub vähest ressurssi nõudva formaalse muudatusega, on 4000 euro suurune riigilõiv ülemäärane, kuna vastav summa ületab selgelt tegelikku tekkinud kulu. Näiteks on põhjendamatu maksta kehtivas määras riigilõivu, kui tegevusloa taotluse muutmine piirdub üksnes ettevõtja maksekonto muutmisega. Kordades suuremas ulatuses riigilõivu tasumine kui see on vajalik tulude katmiseks, ei ole autori hinnangul mõõdukas abinõu. Riigikohtu sõnul ei saa riigilõivu eesmärk olla eelarvesse lisatulude leidmine.[163]

[163] RKÜKo 3-2-1-62-10.

Kuna kulude katmisest ülejääva osa tasumine ei ole legitiimselt põhjendatud, siis on alusetult riivatud ettevõtja vaba vara kasutamist ehk omandipõhiõigust. Seega pole 4000 euro suurune riigilõiv proportsionaalne abinõu situatsioonides, kus tegevusloa muutmine piirdub vähest ressurssi nõudva formaalse muudatusega. Autori hinnangul tuleb riigilõivu tasumisest vabastamise erandeid RLS §-s 51^2 juurde lisada. Sarnaselt aadressi muutmise erandile, peab proportsionaalsuse tagamiseks olema ettevõtjad vabastatud riigilõivu tasumise kohustusest ka näiteks siis, kui tegevusloa muutmine piirdub üksnes ettevõtja maksekonto muutmisega.

KOKKUVÕTE

Magistritöös uuriti virtuaalvääringu teenuste pakkumisega seonduvate rahapesu ja terrorismi rahastamise riskide maandamise problemaatikat. Eesti seadusandja on korduvalt karmistanud VASPidele kohalduvaid nõudeid, saavutamaks VASPi sektori kõrge rahapesu ja terrorismi rahastamise riski üle kontroll. Hoolimata korduvatest seaduse muutmistest, on praktikas näha, et VASPidega seotud rahapesu ja terrorismi rahastamise riskide realiseerumine jätkub. Magistritöö eesmärk oli välja selgitada, millises ulatuses täidavad kehtivad rahapesu ja terrorismi rahastamise tõkestamisele suunatud meetmed eesmärki maandada virtuaalvääringute teenuse pakkumisega seotud rahapesu ja terrorismi rahastamise riske ja pakkuda lahendusi, mis võimaldaks ilmnenud puudusi vähendada.

Eesmärgist lähtuvalt püstitati järgmised uurimisküsimused:

1) Millised on virtuaalvääringutega seotud rahapesu ja terrorismi rahastamise riskid ja kas kehtiva RahaPTS-iga on võimalik neid maandada?

2) Millised on virtuaalvääringu teenuse pakkuja hoolsusmeetmete ja teatamiskohustuse mittenõuetekohase täitmisega seotud rahapesu ja terrorismi rahastamise riskid ja kuidas on neid võimalik maandada?

3) Kuidas on tegevusloa nõuete muutmine mõjutanud rahapesu ja terrorismi rahastamise riske ja VASPide õiguspärast ootust ning kas kehtiv riigilõivu suurus täidab riski maandamise eesmärki?

Magistritöö esimeses peatükis selgitas autor välja, et virtuaalvääringutega seonduvad rahapesu ja terrorismi rahastamise riskid on seotud peamiselt kolme riskiteguriga: anonüümsus, piiriülene levik ja kohustatud isiku puudumine.

Selgus, et anonüümsusest tulenevad riskid väljenduvad osaliselt anonüümsete virtuaalvääringute, suurendatud anonüümsusega virtuaalvääringute ning segamisteenuse kasutamises. Töös jõuti seisukohale, et virtuaalvääringu anonüümsusest tulenevad riskid on maandatud, kui isikud kasutavad VASPide kui RahaPTS-is sätestatud kohustatud isikute teenuseid, sest anonüümsus kõrvaldatakse kliendi isikusamasuse tuvastamisel ja kontrollimisel ning isiku seostamisel tema virtuaalvääringu rahakotiga. Ka segamisteenusega kaasnev anonüümsuse risk on maandatud, kuna töös selgus, et tegemist on virtuaalvääringu teenuse pakkumisega, kus klientide suhtes tuleb

kohaldada anonüümsust kõrvaldavaid hoolsusmeetmeid. Küll aga tuleb anonüümsust suurendavate virtuaalvääringute puhul täiendada RahaPTS-is kliendiandmete kogumise nõuet nn vaatamise võtme kogumisega, kuna see võimaldab kliendi virtuaalvääringu rahakotiga seotud tehingud teha plokiahelas nähtavaks, mis tagab VASPile võimaluse teostada ärisuhte seiret. Juhul, kui klienti pole võimalik tuvastada, on rahapesu ja terrorismi rahastamise riskid maandatud tehingu tegemise ja ärisuhte loomise keeluga.

Piiriülese leviku puhul tuvastas autor, et riskid esinevad juhul, kui klient või tehingu vastaspool elab teises riigis. Veelgi enam, kui tegu on kõrge riskiga piirkonnaga ehk jurisdiktsiooniga, kus rahapesu ja terrorismi rahastamise tõkestamise meetmed on puudulikud. Samuti tuleneb piiriülesest levikust risk, et rahapesijatel ja terrorismi rahastajatel on võimalik kasutada virtuaalvääringu teenuseid, mille osutajad asuvad jurisdiktsioonis, kus rahapesu ja terrorismi rahastamise tõkestamise regulatsioon ja järelevalve on nõrk ning kus puudub suutlikkus teha rahvusvahelist koostööd. Töös leiti, et riskid, mis seonduvad kliendi või tehingu vastaspoole asumisega teises riigis, sealhulgas kõrge riskiga piirkonnas, on maandatud RahaPTS-is kehtestatud ärisuhte seire teostamise kohustusega ning kaugtuvastamisele esitatud nõuetega.

Küll aga vajab maandamist risk, et Eesti seadusandja ei ole Financial Action Task Force (edaspidi FATF) standardist „travel rule“ nõuet täielikult üle võtnud. Lihtsustatult tuleb „travel rule“ nõude järgi virtuaalvääringu vahetamise ja ülekandeteenuse puhul koguda ja talletada andmeid nii virtuaalvääringu ülekande algataja kui ka saaja kohta ning jagada seda teavet ülekande saaja kohustatud isikuga. Kehtivas RahaPTS-is on eelkõige puudulik ülekande saaja kohta kogutava teabe koosseis ja kehtestamata ülekande saaja VASPi kohustused. Kuna RahaPTS-i järgi tuleb VASPil koguda ülekande saaja kohta üksnes tehingu kordumatu tunnus ja virtuaalvääringu rahakoti aadress, mis ei hõlma ülekande saaja isikut tuvastavaid andmeid, siis on kehtiva regulatsiooni kohaselt võimalik teha tehinguid tuvastamata isikutega, sealhulgas sanktsioneeritud isikutega, rahapesijate ja terrorismi rahastajatega. Vastava riski maandamiseks ehk vastaspoole tuvastamiseks tuleb täiendada RahaPTSi osas, mis puudutab ülekande saaja täisnime kogumist ja edastamist ning vastaspoole VASPi kohustust kontrollida ja kinnitada edastatud teabe õigsus. Samuti tuleb nii andmekaitse kui ka rahapesu ja terrorismi rahastamise eesmärgil täiendada kehtivat RahaPTS-i ülekande algataja VASPi kohustusega tuvastada ja kohaldada ülekande saaja VASPile hoolsuskontrolli.

Töös leiti, et kohustatud isiku puudumisest tulenevad riskid väljenduvad detsentraliseeritud virtuaalvääringu teenuse kasutamises ning selle käigus isikult isikule tehingute tegemises. Samuti on riskiks *unhosted walleti* kasutamine. Kuigi detsentraliseeritud teenuste puhul on isikult isikule tehingute tegemine programmeerimiskoodi abil täiesti automatiseeritud, ehk tundub, et puudub kohustatud isik, kellelt nõuda klientide suhtes rahapesu ja terrorismi rahastamise tõkestamise meetmete rakendamist, siis käesolevas töös selgus, et praktikas on siiski võimalik keskne isik tuvastada. Näiteks detsentraliseeritud teenuse loojad, kes omavad mõju või kontrolli teenuse tingimuste või muude parameetrite üle. Kohustatud isik puudub aga juhul, kui isik loob ilma teenusepakkujata virtuaalvääringu rahakoti ehk *unhosted wallet*'i. *Unhosted wallet*'i loomisel ei tule läbida hoolsusmeetmete protsessi, mistõttu on isikul võimalik teha tehinguid anonüümse rahakotiga. Eksisteerib risk, et vastavaid rahakotte kasutatakse rahapesuks ja terrorismi rahastamiseks. Töös leiti, et riski maandamiseks tuleb RahaPTS-i üle võtta erisustega FATFi „travel rule". Täpsemalt tuleb RahaPTS-i täiendada osas, mis puudutab kliendilt vastaspoole täisnime ja kontaktandmete kogumist ning *unhosted wallet*'i omaniku tuvastamist.

Teises peatükis selgus, et suuremal osal VASPidest esineb puudujääke teatamiskohustuse ja hoolsusmeetmete, eelkõige isikusamasuse tuvastamise ja ärisuhte seire kohustuse täitmisega. VASPide poolt kohustuste täitmata jätmise ja mittekohase täitmise korral on risk, et vastavate ettevõtete kaudu on võimalik tegeleda rahapesu ja terrorismi rahastamisega ilma, et VASP seda tuvastaks, RABile teavitaks ja ebaseaduslikku tegevust tõkestaks. Selgus, et mittenõuetekohasel kohustuste täitmisel on kolm põhjust: VASPi töötajate madal teadmiste tase, tõhusate ja tegevusala spetsiifikat arvestavate skriinimis- ja monitoorimissüsteemide puudumine ja hooletus.

Madalast teadmiste tasemest tuleneva riski maandamiseks leidis autor, et RABil tuleb korraldada VASPi sektorile suunatud seminare, koolitusi või töötubasid, mis käsitlevad eelkõige isikusamasuse tuvastamist ja selle kontrollimisel kasutatavate dokumentide analüüsi, samuti teemat, kuidas virtuaalvääringu tehinguid analüüsida plokiahelas kajastuva teabe põhjal. Eesmärk on aidata turuosalistel mõista neile kohalduvaid rahapesu ja terrorismi rahastamise tõkestamise nõudeid ja selgeks teha, kuidas neid äritegevuses nõuetekohaselt järgida. Kuna töös selgus, et märkimisväärsed puudujäägid esinevad ka kontaktisikute teadmistes, kes tegelevad teatamiskohustuse täitmisega, siis tuleb esmalt luua kontaktisiku kutsestandard ja RahaPTS-i täiendada osas, mis puudutab vastava kvalifikatsiooni nõude kehtestamist kontaktisikule. See tagab ühelt poolt ettevõtjale kindluse, et kontaktisik on pädev oma tööülesandeid nõuetekohaselt täitma

ja teiselt poolt kindluse RABile ja laiemalt kogu finantsturule, et VASPidele kehtestatud teatamiskohustus ei jää kontaktisiku teadmiste ja/või oskuste ebapiisavuse tõttu täitmata.

Tõhusate ja tegevusala spetsiifikat arvestavate seire- ja monitooringusüsteemide puudumisest tuleneva riski maandamiseks tuleb riigil välja töötada ja kasutusele võtta skriinimis- ja monitoorimissüsteemi standard ning kehtestada RahaPTS-is vastava sertifikaadi omamine VASPi tegevusloa saamise kohustusliku tingimusena. Samuti tuleks riski maandamiseks täiendada RahaPTS-i RABi kohustusega keelduda tegevusloa andmisest, kui VASPil puudub sertifikaat, mis tõendab IT-süsteemide ja tehniliste lahenduste vastamist standardile. Standardi väljatöötamine ja vastava sertifikaadi kehtestamine tegevusloa nõudena annaks ühelt poolt ettevõtjale selged juhised nõuetekohaste süsteemide väljatöötamiseks, ning teiselt poolt RABile kindluse, et VASPide tehnilised lahendused on nõuetekohased, kvaliteetsed ja tõhusad rahapesu ja terrorismi rahastamise tõkestamiseks.

Töös selgus, et VASPidele, kes pahatahtlikult rikuvad rahapesu ja terrorismi rahastamise tõkestamise kohustust, on RABil olemas õiguslikud meetmed, mille abil mõjutada VASPi oma tegevus nõuetega kooskõlla viima ning vajadusel ka ettevõttelt VASPina tegutsemine õigus ära võtta. Kuna VASPi sektori puhul on tegemist kõrge riskiga valdkonnaga, tuleb RABil rakendada VASPide osas kõrgendatud tähelepanu, suurendada järelevalvekontrollide läbiviimist, teha vajadusel ettekirjutusi ja rakendada ettenähtud sanktsioone VASPide osas, kelle tegevus ei ole kooskõlas neile kehtestatud nõuetega.

Kolmandas peatüki esimeses alaosas selgus, et tegevusloa nõuete muutmine on soodustanud rahapesu ja terrorismi rahastamise riskide maandamist. Lähtuvalt töös eelnenud analüüsist, on aga VASPi sektoris veel riske, mis vajavad maandamist. Samuti selgus, et kuigi tegevusloa nõuete muutumine lühikese aja jooksul on riivanud VASPide õiguspärast ootust stabiilsele õiguskeskkonnale, siis on tegemist õigustatud riivega, kuna muudatused olid tingitud avalikust huvist maandada VASPi sektoris kõrgeid rahapesu ja terrorismi rahastamise riske, et tagada finantssektori stabiilsus, usaldusväärsus ja läbipaistvus.

Peatüki teises alaosas selgus, et kõrge riigilõivu eesmärk rahapesu ja terrorismi rahastamise tõkestamisel väljendub kahel viisil. Esiteks aitab kõrge riigilõiv ära hoida olukorda, kus madal riigilõiv tekitab rahvusvahelist tähelepanu ja huvi isikutes, kes soovivad kergelt ja odavalt taotleda VASPi tegevusluba, et tegutseda VASPina rahapesu või terrorismi rahastamise eesmärgil või

tegevusluba valmisettevõtete kaudu edasi müüa isikutele, kes ei vasta tegevusloa taotlemise nõuetele. Teiseks, VASPide tegevusloa menetluse kontrollesemete arv on kõrge ning nende kontrollimine keeruline. Kõrge riskiga tegevusala tegevusloa kontrollesemete tõhusaks ja kvaliteetseks kontrollimiseks on vaja ressurssi, mistõttu on oluline, et riigilõiv kataks toimingutega kaasnevad kulud.

Analüüsi tulemusel leiti, et 10 000 euro suurune virtuaalvääringu teenuse tegevusloa taotluse läbivaatamise riigilõiv on sobiv meede eelnimetatud eesmärkide täitmiseks, aga ei vasta vajalikkuse ja mõõdukuse kriteeriumitele. Nimelt selgus, et ennetamise eesmärki täidavad teised tegevusloa nõuded tõhusamalt, nt kõrged kapitali miinimumnõuded, kõrgendatud nõuded tegevuskohale ja juhatuse liikmetele, tegevusloa teisele isikule üleandmise keeld jm. Samuti on välisriigis asuvate VASPide ja Eestis asuvate teiste krediidi- ja finantseerimisasutuste näitel võimalik järeldada, et tegevusloa menetlust saab läbi viia väiksemate kuludega kui 10 000 eurot. Töös leiti, et riigilõivu küsimine osas, mis ületab tegelikke kulusid, ei ole eesmärgipärane ning takistab põhjendamatult ettevõtjatel virtuaalvääringu teenuse sektorisse sisenemist ja vara vaba kasutamist. Seega on tegu ebaproportsionaalse meetmega riigilõivu eesmärkide saavutamiseks.

Samuti leiti analüüsi tulemusel, et 4000 euro suurune riigilõiv on sobiv abinõu, et katta tegevusloa muutmisega kaasnevaid kulusid, ent tegemist ei ole igas situatsioonis vajaliku ja mõõduka meetmega. Olukordades, kus tegevusloa muutmine piirdub vähest ressurssi nõudva formaalse muudatusega, on 4000 euro suurune riigilõiv ülemäärane, kuna vastav summa ületab selgelt tegelikku tekkinud kulu. Näiteks on põhjendamatu maksta kehtivas määras riigilõivu, kui tegevusloa taotluse muutmine piirdub üksnes ettevõtja maksekonto muutmisega. Sellest tulenevalt leiti töös, et riigilõivu seadust tuleb täiendada riigilõivu tasumisest vabastamise eranditega olukordade jaoks, mil tegevusloa muutmine piirdub vähest ressurssi nõudva formaalse muudatusega, nt ettevõtja maksekonto muutmisega.

Kokkuvõttes on rahapesu ja terrorismi rahastamise riskid maandatud osas, mil isikud kasutavad VASPide teenuseid, kuna VASPidel on kohustus rakendada kliendisuhte loomisel ja selle käigus rahapesu ja terrorismi rahastamise tõkestamise meetmeid. Küll aga tuleb RahaPTS-i täiendada nõudega tuvastada ja kontrollida virtuaalvääringu tehingu vastaspoolt ning olemasolul ka tema VASPi. Samuti on oluline RahaPTS-i täiendada nii, et tagatud oleks VASPide nõuetekohane hoolsusmeetmete ja teatamiskohustuse täitmine. Riigilõivude osas tuleb välja selgitada proportsionaalne riigilõivu summa, mis täidab rahapesu ja terrorismi rahastamise tõkestamise

eesmärki ja katab tegevusloa taotluse või tegevusloa muutmise taotluse läbivaatamise kulusid, ent ei oleks VASPidele põhjendamatult koormav.

MITIGATING THE RISKS OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE PROVISION OF VIRTUAL CURRENCY SERVICES (Abstract)

According to the Money Laundering and Terrorist Financing Prevention Act (hereinafter referred to as MLTFPA), a virtual currency is a value represented in digital form, which is digitally transferable, preservable or tradable and is accepted as a means of payment by natural or legal persons, but which is not legal tender in any country. The use of virtual currencies offers a number of advantages. Compared to traditional international fiat money transfers, it is faster, cheaper and safer to carry out international transactions with virtual currencies. Virtual currencies also offer new investment opportunities.

While virtual currencies have brought innovation to the financial market, they have also become an attractive tool for money laundering and terrorist financing. The money laundering and terrorist financing risk they entail has been assessed as high at both the European and Estonian level. Estonia has been at the forefront of issuing licenses for virtual asset service providers (hereinafter VASP). As the initially established licensing requirements and supervisory options did not ensure the objective of money laundering and terrorist financing, the legislator has repeatedly tightened up the requirements applicable to VASPs in order to gain control over the high risk in the VASP sector. Despite repeated amendments to the law, in practice it can be seen that the money laundering and terrorist financing risks associated with VASPs continue to materialise. Consequently, the aim of the master's thesis was to find out to what extent the measures in place aimed at preventing money laundering and terrorist financing fulfil the objective of mitigating the money laundering and terrorist financing risks related to the provision of virtual currency services, and to offer solutions that would reduce the shortcomings that have appeared.

In order to achieve the aim, the following research questions were set:

1) What are the money laundering and terrorist financing risks associated with virtual currencies and is it possible to mitigate them with the current MLTFPA?

2) What are the risks of money laundering and terrorist financing associated with the non-compliance of VASPs with their due diligence and reporting obligations and how can they be mitigated?

3) How has the change in the licensing requirements affected the risks of money laundering and terrorist financing and the principle of legitimate expectation of VASPs, and does the current state fee rate serve the purpose of mitigating the risk?

According to the set research questions, the master's thesis was divided into three chapters. In the first chapter, the author identified that the money laundering and terrorist financing risks associated with virtual currencies are mainly linked to three risk factors: anonymity, cross-border spread and the absence of an obliged entity.

It turned out that the risks arising from anonymity are reflected in the use of partly anonymous virtual currencies, virtual currencies with increased anonymity and mixing services. In order to carry out transactions with virtual currencies, it is necessary to create a virtual currency wallet. Transactions with a virtual currency wallet address can be tracked on the blockchain, but since the wallet address is a combination of dozens of letters and numbers, it is not identifiable from the blockchain who the user of the virtual currency wallet is. In the thesis, the author concluded that the risks arising from the anonymity of the virtual currency are mitigated when persons use the services of obliged entities set out in the MLTFPA, as anonymity is eliminated by identifying and verifying the identity of the client and associating the person with their virtual currency wallet. The risk of anonymity associated with a mixing service has also been mitigated, as the study revealed that it is a virtual currency service, where customers must be subject to due diligence measures that remove anonymity. However, in the case of virtual currencies with increased anonymity, the requirement to collect customer data must be supplemented in the MLTFPA by the collection of a so-called view key as this allows transactions related to the client's virtual currency wallet to be made visible on the blockchain, which ensures that VASPs can monitor their business relationship. If it is not possible to identify the client, the risks of money laundering and terrorist financing are mitigated by the prohibition on making a transaction and establishing a business relationship.

In the case of cross-border distribution, the author identified that there are risks if the client or counterparty of the transaction lives in another country. Moreover, when it comes to a high-risk area, i.e. a jurisdiction where anti-money laundering and countering the financing of terrorism (AML/CFT) measures are deficient. The cross-border spread also poses a risk that money launderers and terrorist financiers will be able to use virtual currency services with providers located in jurisdictions where AML/CFT regulation and supervision are weak and where there is a lack of capacity to cooperate internationally. The study identified that the risks associated with the

location of a client or counterparty in another country, including a high-risk area, have been mitigated by the obligation to monitor the business relationship established in the MLTFPA and the requirements for remote identification.

However, the risk that the Estonian legislator has not fully adopted the 'travel rule' requirement from the Financial Action Task Force (hereinafter FATF) standard needs to be mitigated. In simple terms, the 'travel rule' requirement for the exchange of virtual currencies and the transfer service requires the collection and storage of data of both the originator and the recipient of the virtual currency transfer and the sharing of this information with the obliged entity of the recipient of the transfer. In particular, the composition of the information collected about the recipient of the transfer and the obligations of the recipient's VASP are still undetermined in the current MLTFPA. As according to the MLTFPA, a VASP is only required to collect a unique transaction identifier and the virtual currency wallet address of the recipient of the transfer, which does not include the identity of the recipient of the transfer, it is possible under the current regulation to make transactions with unidentified persons, including sanctioned persons, money launderers and terrorist financiers. In the opinion of the author, in order to mitigate the respective risk, i.e. to identify the counterparty, the MLTFPA must be supplemented with regard to the collection and transmission of the full name of the recipient of the transfer and the obligation of the counterparty VASP to verify and confirm the correctness of the information transmitted. In addition, for the purpose of both data protection and the prevention of money laundering and terrorist financing, the current MLTFPA transfer initiator VASP needs to be supplemented with an obligation to identify and apply due diligence to the VASP of the recipient of the transfer.

The study found that the risks arising from the absence of an obliged entity are expressed in the use of a decentralised virtual currency service and the execution of peer-to-peer transactions in the process. Using unhosted wallets also poses a risk. Although in the case of decentralised services, peer-to-peer transactions using a programming code are fully automated, i.e. there seems to be no obliged entity required to apply anti-money laundering and countering the financing of terrorism measures to clients, it was identified in the thesis that in practice it is still possible to identify the central person. For example, decentralised service creators who have influence or control over the terms of service or other parameters. However, there is no obliged entity if a person creates a virtual currency wallet without a service provider i.e. an unhosted wallet. When creating an unhosted wallet, it is not necessary to go through the due diligence process, which is why it is possible for a

person to make transactions with an anonymous wallet. There is a risk that these wallets will be used for money laundering and terrorist financing. The thesis ascertained that in order to mitigate the risk, the FATF 'travel rule' will be incorporated in the MLTFPA. More specifically, the MLTFPA needs to be supplemented in terms of collecting the full name and contact details of the counterparty from the client and identifying the owner of the unhosted wallet.

The second chapter of the thesis determined that the majority of VASPs have shortcomings in due diligence measures, in particular, in the identification and monitoring of business relationships, and in compliance with the obligation to report. In the event of non-compliance and improper performance of their obligations by VASPs, there is a risk that through the respective companies money laundering and terrorist financing can be carried out without the VASP effectively identifying, preventing and reporting it to the Financial Intelligence Unit (FIU). It turned out that there are three reasons for improper performance of duties: low level of knowledge of VASP staff, lack of effective screening and monitoring systems that take into account the specifics of the field of activity, and negligence.

In order to mitigate the risk arising from a low level of knowledge, the author proposed that the FIU needs to organise seminars, trainings or workshops aimed at the VASP sector, in particular on identification and analysis of the documents used for verification, as well as on how to analyse virtual currency transactions based on the information reflected on the blockchain. The aim is to help market participants understand the AML/CFT requirements that apply to them and to clarify how to properly comply with them in their business activities. As the thesis identified that there are also significant gaps in the knowledge of compliance officers who are engaged in fulfilling the reporting obligation, then in the opinion of the author, it is necessary to first establish a professional standard for compliance officers and to supplement the MLTFPA in regards to the introduction of a corresponding qualification requirement for compliance officers. This ensures, on the one hand, the economic confidence for the entrepreneur that the compliance officer is competent to perform their duties and on the other hand, it gives reassurance for the FIU and, more broadly, the financial market as a whole, that the reporting obligation imposed on VASPs will not be fulfilled due to insufficient knowledge and/or skills of the compliance officer.

In order to mitigate the risk arising from the lack of effective screening and monitoring systems that take into account the specifics of the field, the author believes that the state must develop and introduce a standard for screening and monitoring systems and establish the requirement to obtain

a corresponding certificate in the MLTFPA as a mandatory condition for obtaining a VASP license. Also, in order to mitigate the risk, the MLTFPA should be supplemented by the obligation of the FIU to refuse to grant an authorisation if a VASP does not have a certificate certifying that their IT systems and technical solutions meet the standard. The development of a standard and the establishment of a corresponding certificate as a requirement for a licence would, on the one hand, provide clear guidance to the undertaking to develop proper systems and on the other hand give assurance to the FIU and, more broadly, to the financial market as a whole, that the technical solutions of VASPs are meeting the standard, they are of high quality and effective in preventing money laundering and terrorist financing.

In the thesis the author ascertained that for VASPs who maliciously violate their duty to prevent money laundering and terrorist financing, the FIU has legal measures in place to influence the VASPs to bring their activities into compliance and, if necessary, to withdraw the company's right to act as a VASP. As the VASP sector is a high-risk sector, the FIU needs to pay increased attention to VASPs, increase the number of supervisory inspections, issue prescriptions where necessary and impose the prescribed sanctions on VASPs whose activities do not comply with the requirements imposed on them.

The third chapter of the thesis analysed two measures which, in the opinion of the author, have proved to be too burdensome for VASPs following repeated changes in the regulation applicable to VASPs. Firstly, the obligation to obtain a licence and secondly, the state fee for applying for and amending an activity licence. In the first sub-section of the chapter, it became clear that, although changes in the licensing requirements over a short period of time have infringed the legitimate expectation of VASPs, this is a justified interference, since the changes were due to the public interest in mitigating the high risks of money laundering and terrorist financing in the VASP sector.

The second subsection of the chapter revealed that the purpose of a high state fee in the prevention of money laundering and terrorist financing is expressed in two ways. Firstly, a high state fee helps to prevent a situation where a low state fee generates international attention and interest among persons who wish to easily and cheaply apply for a VASP license to act as a VASP for the purpose of money laundering or terrorist financing, or to resell the license through ready-made companies to persons who do not meet the requirements for obtaining a license. Secondly, the number of items to control in the authorisation procedure for VASPs is high and it is difficult to verify them. In order to effectively control the necessary items of the licence of such a high-risk activity and ensure

the high quality of the control procedures, a resource is needed, which is why it is important that the state fee covers the costs associated with these operations.

As a result of the analysis, it was found that the state fee of 10,000 euros for the examination of an application for a licence to operate a virtual currency service is an appropriate measure to achieve the above objectives, but does not meet the criteria of necessity and moderation. Namely, it turned out that the purpose of prevention is fulfilled more effectively by other requirements for the activity licence, e.g. high minimum capital requirements, heightened requirements for the place of business and members of the management board, prohibition on transferring the activity licence to another person etc. It is also possible to conclude from the example of VASPs located abroad and other credit and financial institutions located in Estonia that the activity licence procedure can be carried out at a cost lower than 10,000 euros. In the thesis it was concluded that charging a state fee in excess of the actual costs is not fit for purpose and unduly prevents companies from entering the virtual currency service sector and from using assets freely. The amount of the state fee, which restricts fundamental rights more than is justified by the purpose of the rule, is a disproportionate measure.

The analysis also revealed that a state fee of 4,000 euros is an appropriate measure to cover the costs of changing the activity licence, but it is not a necessary and moderate measure in every situation. In situations where the amendment of the activity licence is limited to a formal change requiring little resources, the state fee of 4,000 euros is excessive, since the corresponding amount clearly exceeds the actual cost incurred. For example, it is unreasonable to pay a state fee at the current rate if the amendment of the application for an activity licence is limited to changing the payment account of an undertaking. Consequently, the study determined that the State Fees Act must be supplemented with exemptions from the payment of state fees in situations where the amendment of the activity licence is limited to a formal change that requires little resources, e.g. changing the payment account of an entrepreneur.

In conclusion, in order to mitigate the risks involved in the provision of virtual currency services, the MLTFPA must be supplemented with regard to the identification and verification of the recipient of the transfer and, if applicable, their VASP. It is also necessary to supplement the MLTFPA with regard to the risks arising from the improper performance of due diligence and reporting obligations by VASPs, in particular to address the low level of knowledge of the staff of a VASP and the lack of adequate screening and monitoring systems. In order to mitigate the high

risk in the VASPs sector, it is necessary to pay close attention to the fulfilment of the obligations of VASPs and to apply the prescribed sanctions in the event of violations. It is also necessary to identify the proportionate amount of the state fee that serves the purpose of preventing money laundering and terrorist financing and covers the costs of examining an application for an operating licence or an application for amendment of a licence, but would not be unduly burdensome for VASPs.

LÜHENDID

1. AMLD5 – Euroopa Parlamendi ja nõukogu viies rahapesuvastane direktiiv (ingl *Anti-Money Laundering Directive V*)
2. AutÕS – autoriõiguse seadus
3. DeFi – detsentraliseeritud rahandus (ingl *decentralized finance*)
4. FATF – rahapesuvastane töökond (ingl k *Financial Action Task Force*)
5. KarS – karistusseadustik
6. KrÜS – krüptovara ja ühisrahastuse seadus
7. MiCA – Euroopa krüptovaraturgude määrus (ingl k *Markets in Cryptoassets regulation*)
8. RAB – Rahapesu Andmebüroo
9. RahaPTS – rahapesu ja terrorismi rahastamise tõkestamise seadus
10. RLS – riigilõivuseadus
11. SE – seletuskiri
12. SNRA –Euroopa Komisjoni riikideülene riskihinnang (ingl k *supranational risk assessment*)
13. TsÜS – tsiviilseadustiku üldosa seadus
14. VASP – virtuaalvääringu teenuse pakkuja (ingl k *virtual asset service provider*)
15. ÜMIVS – ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seadus

KASUTATUD MATERJALID

Kasutatud kirjandus

1. Alexy, R. Põhiõigused Eesti põhiseaduses. – Juridica 2001/eriväljaanne.
2. Allen, J. G., Lastra, R. M. Virtual currencies in the Eurosystem: challenges ahead. (2018) –https://www.europarl.europa.eu/cmsdata/150541/DIW_FINAL%20publication.pdf (03.03.2023).
3. Amiram, D., Jørgensen, B.N, Rabetti, D. Coins for Bombs: The Predictive Ability of On-Chain Transfers for Terrorist Attacks. – Journal of Accounting Research 2022/60, No.2.
4. Cotoc, C-N. jt. Efficiency of Money Laundering Countermeasures: Case Studies from European Union Member States. – Risks 2021/09 No 120.
5. Eesti Vabariigi põhiseadus. Komm vlj. 5. vlj. Tartu: Sihtasutus Iuridicum 2020.
6. Euroopa Liidu Nõukogu. Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. (2022). – https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf (27.03.2023).
7. Ikkonen, K. Avalik huvi kui määratlemata õigusmõiste. – Juridica 2005/3.
8. Ivan, K. Rahapesu virtuaalvääringutega ja selle tõkestamise meetmed. Magistritöö. Juhendaja Indrek Tibar. Tartu: Tartu Ülikool 2022.
9. Kim, S. H., Taylor, S., jt. A comprehensive forensic preservation methodology for crypto wallets. – Forensic Science International: Digital Investigation 2022/42-43.
10. Krüptovara ja ühisrahastuse seadus. Eelnõu. – https://advokatuur.ee/uploads/files/Kr%C3%9CS%20EN.pdf (07.04.2023).
11. Krüptovara ja ühisrahastuse seadus. Seletuskiri. – https://advokatuur.ee/uploads/files/Kr%C3%9CS%20SK.pdf (07.04.2023).
12. Lübbe-Wolf, G. Proportsionaalsuse põhimõte Saksa Liidukonstitutsioonikohtu praktikas. – Juridica 2021/Riigiõiguse aastaraamat 2021.
13. Mbiyavanga, S. Cryptolaundering: Anti-Money Laundering Regulation of Virtual Currency Exchanges. – Journal of Anti-Corruption Law 2019/3, No 1.
14. Mäeker, M., Nõmm, A. Pangasaladuse hoidjast politseinikuks: valikud rahapesu tõkestamisel. – Juridica 2020/8.
15. Narits, R. Õiguse entsüklopeedia. Tallinn: Juura 2002.

16. Oengo, O. F., Virtuaalvääringu teenuse regulatiivsed eripärad, senine areng ja perspektiiv. – Juridica 2020/8.
17. Pikamäe, P. Ootused-lootused ehk õiguspärase ootuse põhimõte põhiseaduslikkuse järelevalve praktikas. – Juridica 2019/9.
18. Pikamäe, P., Sootak, J (koost). Karistusseadustik. Komm vlj. 5. vlj. Tallinn: Juura 2021.
19. Rahapesu ja terrorismi rahastamise tõkestamise seaduse ja teiste seaduste muutmise seadus 507 SE. Eelnõu. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/ffe848a6-7b78-43cf-b106-720915882205/rahapesu-ja-terrorismi-rahastamise-tokestamise-seaduse-ja-teiste-seaduste-muutmise-seadus (25.03.2023).
20. Rahapesu ja terrorismi rahastamise tõkestamise seaduse ja teiste seaduste muutmise seadus 507 SE. Seletuskiri. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/ffe848a6-7b78-43cf-b106-720915882205/rahapesu-ja-terrorismi-rahastamise-tokestamise-seaduse-ja-teiste-seaduste-muutmise-seadus (25.03.2023).
21. Rahapesu ja terrorismi rahastamise tõkestamise seaduse ning riigilõivuseaduse muutmise seadus 8 SE. Eelnõu. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/24832445-95e0-4ffc-adbe-ec44d87d5eb1/rahapesu-ja-terrorismi-rahastamise-tokestamise-seaduse-ning-riigiloivuseaduse-muutmise-seadus (25.03.2023).
22. Rahapesu ja terrorismi rahastamise tõkestamise seaduse ning riigilõivuseaduse muutmise seadus 8 SE. Seletuskiri. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/24832445-95e0-4ffc-adbe-ec44d87d5eb1/rahapesu-ja-terrorismi-rahastamise-tokestamise-seaduse-ning-riigiloivuseaduse-muutmise-seadus (25.03.2023).
23. Tammer, S. Sobivusest sobimatuseni finatntssektoris. – Juridica 2015/5.
24. Valdmann, F. Rahapesu tõkestamise kohaldumine krüptovaluutadele Eestis. Magistritöö. Juhendaja Kaido Künnapas. Tallinn: Tallinna Tehnikaülikool 2018.
25. Varul, P. jt (koost). Tsiviilseadustiku üldosa seadus. Komm vlj. Tallinn: Juura 2010.
26. Wronka, C. Money laundering through cryptocurrecies - analysis of the phenomenon and appropriate prevention measures. – Journal of Money Laundering Control 2022/25 No 1.
27. Ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seadus. Eelnõu. – https://eelnoud.valitsus.ee/main#lfDlLOyf (07.04.2023).
28. Ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seadus. Seletuskiri. – https://eelnoud.valitsus.ee/main#lfDlLOyf (07.04.2023).

Raportid ja juhendid

30. Chainanalysis. The 2023 Crypto Crime Report (2023) – https://blockbr.com.br/wp-content/uploads/2022/06/2022-crypto-crime-report.pdf (03.03.2023).
31. Eesti rahapesu ja terrorismi rahastamise tõkestamise siseriiklik riskihinnang 2020. 13. Virtuaalvääringute teenuste pakkujate riskide analüüs 2020-2021. (2021) – https://www.fin.ee/finantspoliitika-valissuhted/rahapesu-ja-terrorismi-rahastamise-tokestamine/riskihinnangud (16.02.2023).
32. Euroopa Komisjon. Supra-National Risk Assessment (SNRA). (2022) – https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0344&from=EN (02.02.2023).
33. Euroopa Parlament. Virtual currencies and terrorist financing: assessing the risks and evaluating responses. (2018) – https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf (24.02.2023).
34. Financial Action Task Force. FATF report: Virtual Currencies Key Definitions and Potential AML/CFT Risks. (2014) – https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (24.02.2023).
35. Financial Action Task Force. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. (2012, updated 2023) – https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html (01.03.2023).
36. Financial Action Task Force. Terrorist Financing Risk Assessment Guidance. (2019, lk 29) – https://www.fatf-gafi.org/en/publications/Methodsandtrends/Terrorist-financing-risk-assessment-guidance.html (16.02.2023).
37. Financial Action Task Force. Updated Guidance: A Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. (2021) – https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (02.02.2023).
38. Monetary Authority of Singapore. Guidelines to MAS Notice PS-N02 on Prevention of Money Laundering and Countering the Financing of Terrorism. (2020, lk-d 41-42) – https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-

Terrorism/Guidelines--to--Notice-PSN02-on-Prevention-of-ML-and-Countering-the-Financing-of-Terrorism.pdf (24.03.2023).

39. Moneyval. Anti-money laundering and counter-terrorist financing measures – Estonia: Fifth Round Mutual Evaluation Report. (2022) – https://rm.coe.int/moneyval-2022-11-mer-estonia/1680a9dd96 (16.03.2023).
40. Rahapesu Andmebüroo. Juhend kahtlaste tehingute tunnuste kohta. (2022) – https://fiu.ee/oigusaktid-ja-juhendid/juhendid#juhend-kahtlaste-teh (04.03.2023).
41. Rahapesu Andmebüroo. Rahapesu Andmebüroo aastaraamat 2020. (2020) – https://fiu.ee/aastaraamatud-ja-uuringud/aastaraamatud (19.02.2023).
42. Rahapesu Andmebüroo. Rahapesu Andmebüroo aastaraamat 2021. (2021) – https://fiu.ee/aastaraamatud-ja-uuringud/aastaraamatud#item-2 (19.02.2023).
43. Rahapesu Andmebüroo. Rahapesu Andmebüroo aastaraamat 2022. (2022) – https://fiu.ee/aastaraamatud-ja-uuringud/aastaraamatud#item-1 (01.04.2023).
44. Rahapesu Andmebüroo. Rahapesu ja terrorismi rahastamise riskide juhtimine ning hoolsusmeetmete kohaldamine Rahapesu Andmebüroo järelevalvatavatele kohustatud isikutele. (2022) – https://fiu.ee/oigusaktid-ja-juhendid/juhendid#rahapesu-ja-terroris (26.02.2023).
45. Rahapesu Andmebüroo. Tagasiside 2022. aastale. Rahapesu Andmebüroo tagasiside virtuaalvääringu teenuse pakkujatele. (2023) – https://fiu.ee/aastaraamatud-ja-uuringud/tagasiside-teatajatele#tagasiside-virtuaalv (06.04.2023).
46. Rahapesu Andmebüroo. Täpsustav juhis teate esitamiseks Rahapesu Andmebüroole. (2020) – https://fiu.ee/oigusaktid-ja-juhendid/juhendid#esitatava-teate-tait (23.03.2020).
    Rahapesu Andmebüroo. Virtuaalvääringu teenuse pakkujate uuring. (2020) – https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#virtuaalvaaringu-tee--2 (02.02.2023).
47. Rahapesu Andmebüroo. Virtuaalvääringu teenuse pakkujatega seonduvad riskid Eestis. (2022) – https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#virtuaalvaaringu-tee (02.02.2023).

Kasutatud õigusaktid

48. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/848, 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 141/73, pp 44; RahaPTS 507 SE seletuskiri, lk 18.
49. 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 156/43.
50. Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). ELT L 119/1.
51. Infotehnoloogiliste vahendite abil isikusamasuse tuvastamise ja andmete kontrollimise tehnilised nõuded ja kord. RaMm 23.05.2018 nr 25. – RT I, 04.12.2020, 9.
52. Isikuandmete kaitse seadus. – RT I, 04.01.2019, 11.
53. Karistusseadustik. – RT I, 06.01.2023, 4.
54. Rahapesu ja terrorismi rahastamise tõkestamise seadus. – RT I, 10.02.2023, 29.
55. Rahvusvahelise sanktsiooni seadus – RT I, 08.03.2022, 3.
56. Riigilõivuseadus. – RT I, 14.03.2023, 32.
57. Verordnung über verstärkte Sorgfaltspflichten bei dem Transfer von Kryptowerten (Kryptowertetransferverordnung –KryptoWTransferV). Bundesgesetzblatt Jahrgang 2021 Teil I Nr. 69, ausgegeben zu Bonn am 29. September 2021. – https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-09-29-KryptoWTransferV/3-Verkuendete-Verordnung.pdf?__blob=publicationFile&v=4 (24.03.2023).

Kasutatud kohtupraktika

58. RKPJKo 3-4-1-27-13.
59. RKPJKo 3-4-1-1-02.
60. RKPJKo 3-4-1-16-08.
61. RKPJKo 3-4-1-20-04.
62. RKPJKo 3-4-1-24-11.
63. RKPJKo 3-4-1-26-13.
64. RKPJKo 3-4-1-6-00.
65. RKPKJo 3-4-1-20-04.
66. RKÜKo 3-2-1-62-10.
67. RKÜKo 3-3-1-22-11.
68. RKÜKo 3-3-1-33-11.
69. RKÜKo 3-4-1-1-14.
70. RKÜKo 5-18-8/19.

Muud allikad

71. Bundesanstalt für Finanzdienstleistungsaufsicht. Veranstaltungen der BaFin. (2023) – https://www.bafin.de/DE/DieBaFin/Service/Veranstaltungen/veranstaltungen_node.html#ID_13385960 (27.03.2023).
72. De Nederlandsche Bank. InnovationHub and Regulatory Sandbox. (2023) – https://www.dnb.nl/en/sector-information/supervision-stages/prior-to-supervision/innovationhub-and-regulatory-sandbox/ (27.03.2023).
73. D'Aversa, A. A Record $3.6 Billion Seizure and the Twisting Paths of Money Laundering in the Digital World. (2022) – https://www.moneylaunderingnews.com/2022/02/a-record-3-6-billion-seizure-and-the-twisting-paths-of-money-laundering-in-the-digital-world/ (03.03.2023).
74. Electric Coin Company. Explaining viewing keys. (2020) – https://electriccoin.co/blog/explaining-viewing-keys/ (11.02.2023).
75. Euroopa Nõukogu. At a glance. (2023) – https://www.coe.int/en/web/moneyval/home (06.04.2023).
76. Euroopa Parlament. Digital finance package. (2020) – https://finance.ec.europa.eu/publications/digital-finance-package_en (17.03.2023).
77. Europol. Multi-million euro cryptocurrency laundering service Bestmixer.io taken down. (2019) – https://www.europol.europa.eu/media-press/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down (26.02.2023).
78. Eversheds Sutherland. Virtual asset service providers subject to new registration requirements in Belgium. (2022) – https://www.eversheds-sutherland.com/global/en/what/articles/index.page?ArticleID=en/global/belgium/en/Virtual_Currency_Decree (03.03.2023).
79. FinanceEstonia. FinanceEstonia esitas ettepanekud krüptovara ja ühisrahastuse seaduse eelnõule. (2022) – http://www.financeestonia.eu/news/financeestonia-esitas-ettepanekud-kruptovara-ja-uhisrahastuse-seaduse-eelnoule/ (14.03.2023).
80. Financial Action Task Force. "Black and grey" lists. (2023) – https://www.fatf-gafi.org/en/countries/black-and-grey-lis<ts.html (17.02.2023).
81. Financial Action Task Force. Who we are. (2023) – https://www.fatf-gafi.org/en/the-fatf/who-we-are.html (17.02.2023).

82. Finantsinspektsioon. DeFi. (2022) – https://www.fi.ee/et/finantsinspektsioon/innovatsioonikeskus/defi (09.03.2023).
83. Fruhlinger, J. WannaCry explained: A perfect ransomware storm. (2022) – https://www.csoonline.com/article/3227906/wannacry-explained-a-perfect-ransomware-storm.html (11.02.2023).
84. Landeiro, I. Vahistatud Eesti ettevõtjaid kahtlustatakse 575 miljoni dollari krüptorahakelmuses – Postimees 21.11.2022.
85. Lexia Avvocati. How to get an Italian VASP licence. (2023) – https://www.lexia.it/en/how-to-get-italian-vasp-license/ (03.03.2023).
86. NotaBene. Due Diligence Questionnaire for Travel Rule Data Sharing. (2022) – https://app.hubspot.com/documents/7222759/view/277011207?accessId=877505 (01.03.2023).
87. Overheid. Scheme for funding financial supervision for one-off actions. (2020) – https://wetten.overheid.nl/BWBR0041647/2020-05-21 (03.03.2023).
88. Rahapesu Andmebüroo. Rahapesu Andmebüroo kahtlaste tehingute tunnuste juhendi lisa: Kõrgema terrorismi rahastamise riskiga riikide nimekiri. (2022) – https://fiu.ee/oigusaktid-ja-juhendid/juhendid#juhend-kahtlaste-teh (23.03.2023).
89. Rahapesu Andmebüroo. Rahapesu Andmebüroole esitatava teate vorm. (2020) – https://fiu.ee/oigusaktid-ja-juhendid/juhendid#esitatava-teate-vorm (23.03.2020).
90. Statista. Daily number of DeFi users worldwide up until January 9, 2023. (2023) – https://www.statista.com/statistics/1297745/defi-user-number/ (03.03.2023).
91. Suberg, W. Bitcoin Exchange ShapeShift Helps Police As WannaCry Attacker Converts To Monero. (2017) – https://cointelegraph.com/news/bitcoin-exchange-shapeshift-helps-police-as-wannacry-attacker-converts-to-monero (11.02.2023).
92. Tarbijakaitse ja Tehnilise Järelevalve Amet. Majandustegevuse register. – https://mtr.ttja.ee/taotluse_tulemus (12.04.2023).