7. Finantstehnoloogia sektori haavatavus

7.1. Sektori üldkirjeldus

Sektori kirjeldus:
Eesti on üks arenenumaid digiühiskondasid[1] ja eestlasi peetakse tehnikateadlikeks, seda veendumust toetab ka OECD asjaomane uuring[2]. Digitaliseerimine võimaldab tõhusust, suuremat konkurentsi ja uudseid teenuseid. Samal ajal loovad uusi haavatavusi ja riske tuginemine digitaalsetele infrastruktuuridele, milles on keerulised väärtusahelad ja erinevad teenuseosutajad, kiire innovatsioon ning kasvav surve kulude vähendamiseks.

Käesoleva riskihindamise (NRA) raames analüüsiti Eesti finantstehnoloogia (FinTech) sektori all virtuaalvääringu teenuse (virtuaalvääringu rahakotiteenus ja virtuaalvääringu vahetamise teenus) ning ühisrahastusteenuse osutamisega seotud ohtusid. NRA läbiviimise metoodika nägi ette FinTech sektori puhul üksnes virtuaalvääringutega seonduvate riskide hindamise, kuid FinTech töörühma juhi ettepanekul ja juhtrühma heakskiidul võeti hindamisse ka ühisrahastus.

FinTech sektori töörühm näeb selget vajadust tulevasel riskihindamisel analüüsida põhjalikumalt FinTech sektori alamsektoreid. Kindlasti on vaja edaspidi hinnata peale virtuaalvääringute ka teisi krüptovarasid, nii eraldi tokeni liikide kui ka krüptovaradega seotud teenuste osas. Turul on ka palju teenuseosutajaid, kes ei ole ise finantsjärelevalve all, kuid kes pakuvad erinevaid finantstehnoloogia-alaseid või sellega seotud teenuseid finantsjärelevalve subjektidele. Ka viidatud ettevõtjatega seotud ohtusid tuleks edaspidi analüüsida, kuna nendega seotud ohuvektoritest ei ole käesoleval ajal ülevaadet. Tulevase riskihindamise puhul tuleb läbi mõelda ka viidatud ettevõtjate hindamiseks kasutatav metoodika.

Tabel 34. Finantstehnoloogia sektori kirjeldus.

Turuosalised	Turuosaliste arv[3] seisuga 31.12.2019	Turuosaliste arv seisuga 31.12.2020	Kohustatud isikute arv	Erialaliidu või katusorganisatsiooni olemasolu
Virtuaalvääringu teenuse osutajad[4]	1201[5]	419[6]	100%	Eesti Krüptoraha Liit
Ühisrahastusteenuse osutajad	NA	34[7]	17,6%	Pole üldist katusorganisatsiooni, kuid osad teenuseosutajad on koondunud FinanceEstonia MTÜ alla

NRA raames läbiviidud küsitlus toimus ajavahemikus, mille jooksul suur hulk eelnevalt virtuaalvääringu teenuse tegevusloa ettevõtetest jäid tegevusloast ilma. Seetõttu on ka virtuaalvääringute osas laekunud tagasiside algselt eeldatust tunduvalt väiksem. Ühisrahastuse alamsektori aktiivsus oli kõrge.

[1] TalTech, FinTech Report Estonia 2019, lk 13, https://old.taltech.ee/public/m/majandusanaluusi-ja-rahanduse-instituut/FinTech_Report_Estonia_2019_final.pdf.
[2] Measuring the Digital Transformation, https://www.oecd.org/publications/measuring-the-digital-transformation-9789264311992-en.htm.
[3] Virtuaalvääringute puhul on arvestatud ka majandustegevusest ajutise loobumise teate esitanud isikuid.
[4] MTRi andmed.
[5] Nende hulgas 1188 virtuaalvääringu raha vastu vahetamise teenuse ja 1083 virtuaalvääringu rahakotiteenuse osutajat, kellest erinevaid äriühinguid.
[6] Arv saadud 383+36; st 383 virtuaalvääringu teenus, 31 virtuaalvääringu raha vastu vahetamise teenus ja 29 virtuaalvääringu rahakotiteenus (viimasel kahel erinvaid äriühinguid kokku 36)).
[7] Hinnanguline arv. Teenuseosutajate nimekiri on kokku pandud avalikest allikatest saadud info põhjal.

Tabel 35. Finantstehnoloogia sektoris läbiviidud küsitluse andmed.

Alamsektor	Turuosaliste arv	Valimi maht	Valimi suurus/ nõutud vastuste arv	Väljasaadetud kutsete arv	Saadud vastuste arv	Vastamise määr
Virtuaalvääringute teenuse pakkujad	951	valim	274	951	100	47%
Ühisrahastus	34	valim	30	34	14	36%

Virtuaalvääringud

Krüptovarad on Eesti õiguses defineerimata mõiste, kuid krüptovarade alla võib tinglikult liigitada kõiki instrumente, mis on esitatud krüptograafilisel kujul. Krüptovarasid on võimalik jagada kolmeks lähtuvalt nende peamisest funktsioonist ja kasutusotstarbest. Nendeks on maksetokenid ehk virtuaalvääringud, investeerimislaadsed tokenid ja kasutustokenid.[8]

Maailmas on ringluses enam kui 9000 erinevat virtuaalvääringut[9]. Enamik virtuaalvääringutest kasutab plokiahela tehnoloogiat. Virtuaalvääringute alustalaks olev plokiahel kujutab endast jagatud digitaalset andmebaasi, mis salvestab tehinguid ning mida ei ole võimalik muuta, tehes andmed võltsimiskindlaks ja kestvaks. Tehingute detailid on avalikud ja lõpuni jälgitavad[10],[11] välja arvatud aga isikutega seotud detailid.

Eristatakse tsentraliseerituid ja detsentraliseerituid virtuaalvääringuid. Tsentraliseeritud virtuaalvääringutel on keskne administraator, kes virtuaalvääringuid väljastab, nende kasutamist haldab ja käibest kõrvaldab. Sageli leiab neid veebikeskkondadest, mis pakuvad alternatiivseid maksevõrgustikke või *online*-mänge. Detsentraliseeritud virtuaalvääringutel, nt bitcoin, puudub selline keskne administraator.[12]

Kitsamalt saab virtuaalvääringute all eristada krüptoraha. See on krüptograafilistel alustel üles ehitatud rahasüsteem, mis tavaliselt on detsentraliseeritud ja isereguleeruv. Kasutaja jaoks on krüptoraha küllaltki läbipaistev, sest tehingud on avalikult jälgitavad, teisalt aga anonüümsust võimaldav. Krüptorahade kategooriasse liigitub enamik tuntumaid virtuaalvääringuid nagu bitcoin ja ethereum[13].[14]

Virtuaalvääringute alla liigituvad ka nn stabiilsed mündid (*stablecoins*), mille hind seotakse mingi konkreetse vara väärtusega, kõige levinumalt 1:1 USA dollariga (nt Tether, USD Coin, Paxos). Samuti on hetkel väljatöötamisel mitut valuutat ühendav stabiilne münt Libra, mis töötab kui digitaalne komposiit Libra üksikvaluuta (USD, EUR, GBP) stabiilsetest müntidest. Kuigi oma olemuselt ei kaasne stabiilsete müntidega kuidagi kõrgemad riskid kui virtuaalvääringutega üldiselt, on mõnevõrra alarmeeriv nende suurem potentsiaal massiliseks kasutuselevõtuks, mille tagajärgi ei osata praegusel ajal täpselt hinnata[15].[16]

[8] Seletuskiri ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu juurde, lk 10.
[9] Veebiportaali CoinMarketCap andmetel seisuga aprill 2021.a. Kättesaadav: https://coinmarketcap.com/.
[10] Ärileht. Plokiahela tehnoloogia. 14.01.2019.
[11] Rahapesu andmebüroo, virtuaalvääringu teenuse pakkujate uuring, lk 3, 22.09.2020. Kättesaadav: https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b.
[12] Keatinge, T., Carlisle, D., Keen, F. (2018). Virtual currencies and terrorist financing: assessing the risks and evaluating responses. European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs. Rahapesu andmebüroo, virtuaalvääringu teenuse pakkujate uuring, lk 3.
[13] Vt https://www.kryptoraha.ee/tehnoloogia/.
[14] Rahapesu andmebüroo, virtuaalvääringu teenuse pakkujate uuring, lk 3, 22.09.2020. Kättesaadav: https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b.
[15] FATF. (2020). Virtual Assets – Draft FATF Report to G20 on so-called Stablecoins.
[16] Rahapesu andmebüroo, virtuaalvääringu teenuse pakkujate uuring, lk 3, 22.09.2020. Kättesaadav: https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b.

Virtuaalvääring on Eesti õiguses defineeritud 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 ega rahaline vahend /…/ ega makseinstrument või maksetehing /…/ (RahaPTS § 3 p 9). Virtuaalvääringu teenus jaguneb omakorda virtuaalvääringu rahakotiteenuseks ja virtuaalvääringu vahetamise teenuseks (vt täpsemalt allpool sektori õigusraamistiku kohta kirjutatut).[17]

Kõige hilisema ülevaate Eesti virtuaalvääringu teenuse osutajate kohta on võimalik leida Rahapesu Andmebüroo 22.09.2020 avalikustatud uuringust.[18]

Eesti turul tegutsevate virtuaalvääringute teenuste pakkujate vahendatud teenuste teadaolev kogukäive on kiiresti kasvanud. Kui 2018. aastal oli see suurusjärgus 590 miljonit eurot, siis 2019. a esimesel poolaastal juba kaks korda kõrgem – 1,2 miljardit eurot.[19] Virtuaalvääringu teenuse vahendamise käibed varieeruvad ettevõtete puhul väga suurtes piirides. Mõlemal perioodil kuulus suurim käive ühele ettevõttele, vastavalt 420 miljonit eurot 2018. aastal ja 820 miljonit eurot 2019. a esimesel poolaastal. Teenuse pakkumisega alustanud ettevõtete seas oli vahendatud tehingute mediaankäive 2018. aastal 94 tuhat eurot ja 2019. aasta esimeses pooles 50 tuhat eurot. 83 ehk ligikaudu kolmandik virtuaalvääringu ettevõtet olid 2018. aastal teenuseid vahendanud; 2019. aasta I poolaasta kohta tegi seda juba 188 ettevõtet.[20]

Virtuaalvääringu sektori eripära

Virtuaalvääring on digitaalsel kujul esinev ülekantav, säilitatav või kaubeldav väärtus, mis ei ole küll üheski jurisdiktsioonis seaduslik makse- ega rahaline vahend, kuid mida füüsilised või juriidilised isikud kasutavad maksevahendina (vt AMLD V ja RahaPTS[21]).[22] Eestis käsitletakse virtuaalvääringuid tulumaksuseaduse (TuMS) § 15 lõike 1 tähenduses varana ja nendest saadud tulu (kasu vara võõrandamisest, palgatulu, ettevõtlustulu kaevandamisest) maksustatakse sarnastel põhimõtetel traditsioonilises valuutas saadud tuluga[23].[24] Tehingud on digitaalsed ning ei vaja ilmtingimata teostamiseks kolmandat isikut, mis teeb nende liikumise kiiremaks kui tavapärased finantstehingud. Sel põhjusel on vajadusel nende peatamine raskendatud.

Ühisrahastus

Ühisrahastus on finantseerimisviis, mis võimaldab projektide ja ettevõtete finantseerimiseks koguda rahastust paljudelt isikutelt selleks loodud keskkonna (nt ühisrahastusplatvormi) kaudu.[25] Ühisrahastus on üha enam populaarsust koguv ettevõtlusvorm, mis ühelt poolt on kasulik väikestele ja keskmise suurusega ettevõtetele, võimaldades ühisrahastusplatvormi kaudu kaasata kapitali, ja teiselt poolt jaeinvestoritele, kellel on võimalik teenida tulu ka väiksemate investeeringutega. Ühisrahastus pakub alternatiivseid võimalusi klassikalistele finantsteenustele ja aitab tugevdada konkurentsi finantsteenuste

[17] Seletuskiri ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu juurde, lk 11.
[18] Virtuaalvääringu teenuse pakkujate uuring, kättesaadav: https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b.
[19] Andmed põhinevad RABi virtuaalvääringu teenuse pakkujate uuringust ja on hinnangulised, kuivõrd kõik subjektid viidatud uuringule ei vastanud ja arvutused on tehtud saadud vastuste pinnalt.
[20] Allikas: https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b. Seletuskiri ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu juurde, lk 17.
[21] RahaPTS § 3 p 9: Virtuaalvääring on digitaalsel kujul esitatud väärtus, mis on digitaalselt ülekantav, säilitatav või kaubeldav ja mida füüsilised või juriidilised isikud aktsepteerivad maksevahendina, kuid mis ei ole ühegi riigi seaduslik maksevahend ega rahaline vahend Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/2366 makseteenuste kohta siseturul, direktiivide 2002/65/EÜ, 2009/110/EÜ ning 2013/36/EL ja määruse (EL) nr 1093/2010 muutmise ning direktiivi 2007/64/EÜ kehtetuks tunnistamise kohta (ELT L 337, 23.12.2015, lk 35–127) artikli 4 punkti 25 tähenduses ega makseinstrument või maksetehing sama direktiivi artikli 3 punktide k ja l tähenduses.
[22] Rahapesu andmebüroo, virtuaalvääringu teenuse pakkujate uuring, lk 4.
[23] Allikas: https://www.emta.ee/et/eraklient/tulu-deklareerimine/muu-tulu/eraisiku-virtuaalses-valuutaskruptovaluutassaadud-tulu.
[24] Rahapesu andmebüroo, virtuaalvääringu teenuse pakkujate uuring, lk 4.
[25] European Commission. Crowdfunding explained. 29.09.2015, p. 6. Arvutivõrgus: https://ec.europa.eu/growth/content/crowdfunding-explained-0_en.

turul. Ühisrahastusteenuse osutajate ülesanne on leida projektid ja projektidele rahastajad ehk investorid ning pakkuda rahastuse taotlejate ja investorite huvide kokkuviimiseks tehnilist lahendust, mida on soodustanud ka tehnoloogia areng.[26]

Suures plaanis võib ühisrahastust jaotada laenupõhiseks ühisrahastuseks (ingl *peer-to-peer lending*), investeerimispõhiseks ühisrahastuseks (ingl *equity crowdfunding*) ning ühissponsorlusel põhinevaks ühisrahastuseks (ingl *rewards-based crowdfunding*).[27] Euroopa Komisjon jagab ühisrahastuse viide peamisesse kategooriasse, kusjuures ettevõtja ärimudelist tulenevalt võivad platvormid moodustada ka hübriidvorme, mis koosnevad mitmest kategooriast:

1. ***investeerimispõhine ühisrahastus*** - ettevõtted emiteerivad omakapitali (nn osaluspõhine ühisrahastus) või võlainstrumente (nn ühisvõlakirjad) investoritele platvormi kaudu;
2. ***laenupõhine ühisrahastus*** - ettevõtted või eraisikud taotlevad avalikuselt platvormide kaudu laenu;
3. ***arvete kauplemine ühisrahastamise teel*** - varapõhise finantseerimise vorm, mille puhul ettevõtted müüvad tasumata arveid või nõudeid eraldi või kogumina platvormi kaudu investoritele;
4. ***preemiapõhine ühisrahastus*** - isikud annetavad projektile või ettevõttele, saades hiljem mitterahalist tasu oma panuse eest (näiteks kaupu või teenuseid);
5. ***annetuspõhine ühisrahastus*** - isikud panustavad summasid konkreetse heategevusprojekti suurema rahastamise eesmärgi saavutamiseks, saamata samal ajal rahalist ega materiaalset tulu.[28]

Tabel 36. Ühisrahastuse mahud Eestis (mln eur)[29]

Aasta	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020***
Vahendatud rahastuse maht	29	41	66	95	168	313	196
Rahastuse jääk perioodi lõpus	29	50	93	144	235	370	414

Ühisrahastussektori eripära

Ühisrahastuse sektor eristub teistest teenusepakkujatest finantssektoris selle poolest, et käesoleval ajal ei ole ühisrahastusteenuse osutajatel ei loa- ega registreerimise kohustust. Sellest tulenevalt puudub täpne ülevaade ühisrahastusteenuse pakkujate tegelikust hulgast Eestis ja konkreetseid mahtusid seega hinnata ei ole võimalik.[30] FinTech sektori raames küsitletud ühisrahastusteenuse pakkujate arv on 34, kellest enamus (82,4 %) ei ole kohustatud isikud rahapesu ja terrorismi rahastamise tõkestamise seaduse mõttes. RahaPTSi kohaseid kohustatud isikuid on ühisrahastusteenuste osutajate hulgas 6. Nimetatud ühisrahastusteenuse osutajad on kas allutatud finantsjärelevalve alla ja neil on tegutsemiseks tegevusluba (krediidiandja või -vahendaja (4); investeerimisteenuse pakkuja (1)) või on tegevusloata väikefondi valitseja (1). Nimetatud isikutega seotud riske on hinnatud finantsteenuste sektori all. Annetuspõhised ühisrahastusteenuse osutajad on üldjuhul mittetulundusühingud (MTÜ) ja MTÜ-dega seotud ohtusid on käsitletud ka NRA mittetulundusühingute sektori töörühmas.

Finantstehnoloogia sektori õigusraamistik

2021. aasta 15. jaanuaril avalikustati ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalväärtingute seaduse eelnõu (*ÜMIVS*, esimene kooskõlastusring)[31]. Viidatud eelnõuga soovitakse

[26] Eesti Pank, Finantssektori struktuuri ülevaade, 2019, lk 20.

[27] Allikas: https://ec.europa.eu/growth/tools-databases/crowdfunding-guide/types_en, https://www.fi.ee/et/finantsinspektsioon/finantsinnovatsioon/uhisrahastus.

[28] SNRA 2017 ja 2019. NRA Finantstehnoloogia sektori dokumendianalüüs. Vt ka Eesti finantstehnoloogia sektori haavatavused, dokumendianalüüs, lk 26.

[29] Allikas: Eesti Pank, avalikud andmeallikad; Seletuskiri ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalväärtingute seaduse eelnõu juurde, lk 15.

[30] Eesti finantstehnoloogia sektori haavatavused, dokumendianalüüs, lk 5.

[31] Eelnõu on kättesaadav eelnõude infosüsteemis, https://eelnoud.valitsus.ee/main/mount/docList/f4deaf4f-7351-4384-b3ae-aaa9621bf050 (dokumendi nr 21-0050/01, toimiku nr 21-0050). Vt ka asjaomast pressiteadet https://www.rahandusministeerium.ee/et/uudised/rahandusministeerium-asub-uhisrahastuse-ja-kruptovarade-valdkonda-reguleerima.

reguleeritakse uudseid ja innovaatilisi kapitali kaasamise viise eelkõige sooviga tagada senisest suurem investorite kaitse.[32] Viidatud eelnõuga on tehtud ettepanek kehtestada tegevusnõuded ja järelevalve Eestis tegutsevatele:

- ühisrahastusplatvormidele;
- krüptovarasid pakkuvatele ettevõtjatele, sh virtuaalvääringu teenuse osutajatele;
- muudele ettevõtjatele, kes pakuvad nö alternatiivseid investeerimisvõimalusi, kuid ei ole seni järelevalvele allutatud.[33]

Kuivõrd 2021. a esimeses pooles toimub eelnõu avalik konsultatsioon, siis ei ole hetkel teada, milline saab olema vastuvõetava seaduse lõpptekst.

Seoses eelnevaga on käesoleva hindamise raames analüüsitud teenuseosutajatega seotud õigusraamistik muutumisel ja tõhustamisel.

Virtuaalvääringu sektori õigusraamistik

Eesti on üks esimesi riike maailmas, kus asuti reguleerima virtuaalvääringu teenusepakkujate tegevust. Kuna leiti, et infotehnoloogilised arengud võimaldavad uusi, regulatsioonidele mittealluvaid praktikaid rahapesuks, allutati 2008. aastal alternatiivsete maksevahendite teenuse pakkujad RahaPTS regulatsioonile.[34]

Rahapesu Andmebüroo väljastab alates 27.11.2017 tegevuslubasid Eestis virtuaalvääringu teenuse pakkumiseks.[35] Virtuaalvääring on defineeritud rahapesu ja terrorismi rahastamise tõkestamise seaduse (edaspidi RahaPTS) § 3 punktis 9, mille kohaselt virtuaalvääring on digitaalsel kujul esitatud väärtus, mis on digitaalselt ülekantav, säilitatav või kaubeldav ja mida füüsilised või juriidilised isikud aktsepteerivad maksevahendina, kuid mis ei ole ühegi riigi seaduslik maksevahend ega rahaline vahend Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/2366 makseteenuste kohta siseturul, direktiivide 2002/65/EÜ, 2009/110/EÜ ning 2013/36/EL ja määruse (EL) nr 1093/2010 muutmise ning direktiivi 2007/64/EÜ kehtetuks tunnistamise kohta (ELT L 337, 23.12.2015, lk 35–127) artikli 4 punkti 25 tähenduses ega makseinstrument või maksetehing sama direktiivi artikli 3 punktide k ja l tähenduses.[36]

Virtuaalvääringu teenus on kehtiva RahaPTS järgi virtuaalvääringu rahakotiteenus ja virtuaalvääringu vahetamise teenus. Rahakotiteenuse puhul klientidele luuakse või hoitakse nende krüpteeritud võtmeid, mida kasutatakse virtuaalvääringute hoidmiseks, säilitamiseks ja ülekandmiseks. Virtuaalvääringu vahetamise teenus jaguneb omakorda kaheks: virtuaalvääringu vahetamine raha vastu või raha vahetamine virtuaalvääringu vastu ja ühe virtuaalvääringu vahetamine teise vastu.[37]

Rahapesu ja terrorismi rahastamise tõkestamise seaduse ning riigilõivuseaduse muutmise seaduse eelnõuga, mis võeti vastu 11.12.2019. a, tehti RahaPTSis mitmeid olulisi muudatusi.[38] Peamised muudatused jõustusid 2020. aasta 10. märtsil. Muudatustega koondati virtuaalvääringu raha vastu vahetamise teenuse pakkujad ja virtuaalvääringu rahakotiteenuse pakkujad ühe mõiste alla – virtuaalvääringu teenuse pakkujad. Muudatuste kohaselt võib tegevusluba anda üksnes virtuaalvääringu teenuse pakkujale, kelle registrijärgne asukoht, juhatuse asukoht ja tegevuskoht on Eestis või välisriigi äriühingule, kes tegutseb Eestis äriregistrisse kantud filiaali kaudu, mille tegevuskoht ja juhataja asukoht on Eestis. Täiendavalt kehtestati juhtorgani liikmele, prokuristile, tegelikule kasusaajale ja omanikule korrektse ärialase maine nõue. Lisaks peab loa taotlejal olema avatud maksekonto krediidiasutuses, e-raha asutuses või makseasutuses mis on asutatud Eestis või Euroopa Majanduspiirkonna lepinguriigis ja

[32] Seletuskiri ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu juurde, lk 1.
[33] Seletuskiri ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu juurde, lk 1.
[34] Rahapesu andmebüroo, virtuaalvääringu teenuse pakkujate uuring, lk 4, kättesaadav: https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b.
[35] Rahapesu andmebüroo, majandustegevuse luba. Kättesaadav: https://www.politsei.ee/et/juhend/majandustegevuse-luba.
[36] Seletuskiri ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu juurde, lk 11.
[37] Seletuskiri ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu juurde, lk 11.
[38] Seaduse eelnõu on kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/24832445-95e0-4ffc-adbe-ec44d87d5eb1/Rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20seaduse%20ning%20riigil%C3%B5ivuseaduse%20muutmise%20seadus.

osutab Eestis teenuseid piiriüleselt või mis on asutanud Eestis filiaali. Kehtestati nõue, et tegevusluba taotleval ettevõtjal peab olema aktsia- või osakapital vähemalt 12 000 eurot, mis on täies ulatuses rahaliselt sissemakstud. Tegevusloa taotluse läbivaatamise riigilõiv tõsteti 345 eurolt 3300 euroni. Enne muudatusi väljastatud tegevusload jäid kehtima, kuid tegevusloaga isikud pidid oma tegevuse viima kooskõlla tegevusloa andmise tingimustele, kuna vastasel juhul on RAB-il õigus tegevusluba kehtetuks tunnistada. Üheks läbivaks muudatuseks oli, et virtuaalvääringu teenuse pakkujatele hakati kohaldama finantseerimisasutustele kohaldatavaid RahaPTS nõudeid. Seetõttu pidid virtuaalvääringu teenuse pakkujad uuendama sisekontrollieeskirju, protseduurireegleid ja riskiisu dokumente. Pärast muudatusi peavad virtuaalvääringu teenusepakkujad väiksemat või suuremat riski iseloomustavate asjaolude tuvastamisel ja lihtsustatud või täiendavate hoolsusmeetmete valikul arvestama Euroopa järelevalveasutuste suunistest riskitegurite kohta. Lisaks hakkasid kohalduma RABi kontaktisiku määramise kohustus ning virtuaalvääringu teenuse pakkujate jaoks karmistusid nõuded isikusamasuse tuvastamisele, sh kaugtuvastamisele ja korduvate rikkumiste osas hakkasid kohalduma kõrgemad sunniraha ülemmäärad.

Ühisrahastussektori õigusraamistik

Kehtivast regulatsioonist tulenevalt jagunevad ühisrahastusteenuse osutajad reguleeritud ja reguleerimata teenuseosutajateks, kus esimestele kohaldub mõni finantsteenuse eriseadus (nt KAVS, VPTS). Ühisrahastusteenuse osutajale kohalduv regulatsioon sõltub seega käesoleval ajal ettevõtte ärimudelist ja rahastusprojekti struktuurist. Muuhulgas peab ettevõtja hindama, kas tema tegevuses võivad esineda sellised tunnused, milleks on vaja taotleda tegevusluba või registreerida oma tegevus Finantsinspektsioonis.[39]

Laenupõhise ühisrahastuse liigi puhul tuleb eristada juriidilistele (enamasti äriühingutele) ja füüsilistele isikutele (tarbijatele) suunatud ühisrahastamist. Kui ühisrahastusteenuse osutaja soovib vahendada tarbijale krediiti, peavad nii laenulepingud kui ka teenuseosutaja kui tarbijakrediidi vahendaja tegevus vastama tarbijakrediidilepingu sätetele krediidiandjate ja -vahendajate seaduse (KAVS) § 2 lõike 2 kohaselt. See tähendab muu hulgas, et nimetatud ettevõtja peab taotlema Finantsinspektsioonilt krediidivahendaja tegevusloa.[40] Eeltoodust tulenevalt käsitletakse tarbijakrediiti vahendavate ühisrahastusteenuse osutajate tegevust krediidiandjate ja -vahendajate tegevusena riikliku riskihinnangu koostamise raames, mistõttu on nendega seonduvad rahapesu ja terrorismi rahastamise riskid hinnatud finantsteenuste sektori alamsektori all. Sarnane on olukord käesoleval ajal ka investeerimispõhise ühisrahastuse puhul, kuna sõltuvalt tegevusmudelist võib olla vajalik investeerimisühingu või fondivalitseja tegevusluba. Nimetatud tegevuslubasid omavate teenusepakkujatega seotud riskid on samuti hinnatud finantsteenuste sektori riskihinnangu raames.

2016. aastal esitas Finantsinspektsioon algatuse ühisrahastuse reguleerimiseks.[41] FinanceEstonia MTÜ eestvedamisel loodi samal aastal ühisrahastuse hea tava[42], mille eesmärk on muuta ühisrahastusteenuse osutajate tegevus klientidele (rahastuse taotlejad ja investorid) arusaadavaks ja läbipaistvaks. Soovitusliku iseloomuga juhise täitmise eest said 2019. aastal märgise 4 ettevõtjat[43].

7.10.2020 võeti vastu Euroopa Parlamendi ja nõukogu määrus (EL) 2020/1503 (edaspidi nimetatud ka EL ühisrahastuse määrus)[44] ning Euroopa Parlamendi ja nõukogu direktiiv (EL) 2020/1504, millega

[39] Eesti finantstehnoloogia sektori haavatavused, dokumendianalüüs, lk 6.
[40] Allikas: Seletuskiri krediidiandjate ja -vahendajate seaduse eelnõu juurde, lk 12. Eelnõu seletuskiri on leitav Riigikogu veebileheküljelt: Krediidiandjate ja -vahendajate seadus 795 SE, https://www.riigikogu.ee/tegevus/eelnoud/eelnou/950bdd45-ccf9-468c-b66e511edb1d6e3f/Krediidiandjate%20ja%20–vahendajate%20seadus. TMKo 2-17-11472 lk 2, HMKo 2-18-104070 p 23.
[41] Kättesaadav https://www.fi.ee/sites/default/files/2016_09_Uhisrahastuse_seaduse_eelnou.pdf.
[42] Kättesaadav: http://financeestonia.eu/wp-content/uploads/2017/07/hisrahastuse-Hea-Tava-.pdf.
[43] Vt http://www.financeestonia.eu/priority_niche/crowdfunding/.
[44] https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32020R1503&from=EN.

muudetakse direktiivi 2014/65/EL ehk MiFID II direktiivi.[45] Õigusakte hakatakse rakendama vastavalt 10.11.2021 ja 10.05.2021.

15.01.2021. a esitati esimesele kooskõlastusringile ÜMIVS eelnõu, mis tulevikus ühisrahastuse valdkonna õigusmaastikku oluliselt muudab.[46] Nimetatud eelnõuga kehtestatakse muu hulgas normid, mis rakendavad määrust (EL) 2020/1503 ja normid, millega võetakse üle direktiiv (EL) 2020/1504 ning kehtestatakse vastutus ja järelevalve viidatud EL õigusaktide kohaldamisalas olevate ühisrahastusteenuse osutajate üle.[47]

7.2. Riskide tüpoloogiate kirjeldus

Finantstehnoloogia sektoris üldlevinud riskid ja nende tüpoloogiad

Riigi või geograafilise asukohaga seotud riskid

- **piiriülene tegevus ja globaalne haare** (sh tehingud kõrge riski piirkondades)[48]
- **rahaliste vahendite tuvastamise keerukus** (vahendid liiguvad kiiresti üle riigipiiride)

Teenuste, toodete omaduste ning transaktsioonide ja jaotuskanalitega seotud riskid

- **internetipõhine teenuseosutamine** (sh tehingud tumeveebis)
- **anonüümsust võimaldavate sularaha ja virtuaalvääringute kasutamine**
- **tehingute kiirus** (tehingud toimuvad kiiresti, mh üle riigipiiride, mis raskendab kuritegeliku raha liikumise kindlaksmääramist)
- **probleemid monitoorimise süsteemidega** (teenuseosutajate monitoorimise süsteemid ei suuda piisava efektiivsusega tuvastada kuritegeliku päritoluga rahavooge)

Klientidega seotud riskid

- **isikutuvastusega seotud problemaatika** (sh tehingud kõrge riskiga kliendiga; teenuseosutaja ei suuda tuvastada tehingut, mille vastaspooleks on riikliku taustaga isik, kas skriinimise süsteemi või riikliku taustaga isikute nimekirjade puudulikkuse tõttu)
- **tegeliku kasusaaja kindlakstegemise keerukus** (teenuseosutaja ei suuda tuvastada tegelikku kasusaajat kliendi või tehingu vastaspoole keerulise omandistruktuuri või tegelike kasusaajate info puudulikkuse tõttu registris)
- **mitteresidentidest või e-residentidest** kliendid (teenuseosutaja ei suuda rakendada vastavaid hoolsusmeetmeid mitteresidentidest klientide või e-residentidest klientide suhtes nende tegeliku riskitaseme tuvastamise keerukuse tõttu)

Regulatiivse keskkonnaga, sh järelevalve teostamisega seotud riskid

- **valdkonna alareguleeritus** (valdkonna kiire areng käib regulatiivsest keskkonnast sammu ees, tehnoloogia kiire areng võimaldab pidevalt turule tuua uusi teenuseid)
- **valdkonna regulatsioonide killustatus globaalselt** (erinevad nõuded, definitsioonid jne)
- **koostöö teiste riikide järelevalveasutustega võib olla problemaatiline** (eriti kolmandate riikide pädevate asutustega)
- **koostöö teenuseosutajate ja pädevate asutuste vahel** (teenuseosutajad sooviksid suuremat koostööd pädevate asutustega ja tõhusamaid koolitusi)
- **valdkonnaspetsiifiliste suuniste ja juhendite puudus** (teenuseosutaja ei suuda tuvastada terrorismi rahastamisele suunatud või massihävitusrelvade levikut soodustatavaid tehinguid)

[45] https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32020L1504&qid=1606384145932&from=EN.
[46] Vt ülal ÜMIVS eelnõu kohta kirjutatut.
[47] Seletuskiri ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu juurde, lk 9-10.
[48] Vt ka http://www.fatf-gafi.org/countries/#high-risk.

Kuritegevus

- **pettused** (sh kelmused, nt investeerimiskelmused; teenuseosutaja ei suuda tuvastada fiktiivset tehingut (tehinguga seotud fiktiivsed dokumendid) või isikut (fiktiivsed isiku tuvastamise dokumendid))
- **küberkuritegevus** (sh internetikelmused, virtuaalsed väljapressimised, rünnakud arvutisüsteemidele, andmete kompromiteerimine (sh info vargused, manipulatsioonid), rünnakud teenuseosutajate süsteemidele, veebilehtede nakatamised viirusega, krüptokaevandamised, ründed mobiilsete rahakottide vastu))
- **tehingud tumeveebis**
- **narkootikumidega seotud süüteod**

Kirjanduse[49] andmetel finantstehnoloogia valdkonnas üldised riskid suurenevad seoses digitaalsete finantsteenuste osutamisega ja kaasnevate probleemidega, nt isikutuvastus. Elektroonilise identifitseerimise kasutamine ja usaldusväärsus muutuvad tulevikus veelgi olulisemaks.[50] Virtuaalvääringu ja virtuaalvara rahapesu ja terrorismi rahastamise riske peetakse üldjuhul kas kõrgeks või väga kõrgeks.[51]

7.3. Ohud

7.3.1. Rahapesu ohud

Üldlevinud ohud

Käesoleva riskihinnangu raames hinnati[52] finantstehnoloogia sektori **ohutaset** järgmiselt:

Tabel 37. FinTech sektori ohutasemed

Finantstehnoloogia sektor	**Rahapesu ohu tase sektori tasandil**		**Terrorismi rahastamise ohu tase sektori tasandil**	
Virtuaalvääringud	**3**	keskmine	**5**	kõrge
Ühisrahastus	**2,45**	keskmine/madal	**2,3**	keskmine/madal

Virtuaalvääringutega seotud võimalikud ohud

Riigi või geograafilise asukohaga seotud ohud

- Tehingute piiriülesus võimaldab teha tehinguid kõrge riski piirkonnast või kõrge riskiga klientidega, keda ei ole võimalik tuvastada.
- Virtuaalvarasid on lihtne üle kanda erinevatesse riikidesse ning puuduvad ühesugused kontrolli ja ennetamise meetmed globaalsel tasandil. Kurjategijad kasutavad virtuaalvarade, sh -vääringute süsteeme väärtuse ülekandmiseks või toodete ostmiseks anonüümselt.
- Virtuaalvääringute detsentraliseeritus (rahvusvahelisus ja riigipiire ületav tegevus) ei võimalda tõhusat järelevalvet ja varade konfiskeerimist.
- Rahvusvahelise koostöö keerukus.
- Puudulik siseriiklik koostöö.

[49] Vt nt 2019 SNRA.
[50] COM SNRA 2017 (Euroopa Komisjoni poolt läbi viidud üle-Euroopaline TF/ML riskide hindamine).
[51] COM SNRA 2019 (Euroopa Komisjoni poolt läbi viidud üle-Euroopaline TF/ML riskide hindamine, parandatud ja täiendatud versioon.
[52] NRA ohtude töörühma poolt antud hinnangud, mis põhinevad riskihinnangu läbiviimise metoodikal.

Võimaliku ohu realiseerumise tõenäosuse analüüs Eestis

Rahvusvahelisus on üheks suurimaks ohuks Eesti virtuaalvääringu sektoris. RABi koostatud virtuaalvääringu teenuse pakkujate uuringu[53] kohaselt märkimisväärsel osal ettevõtjatest, kes omavad virtuaalvääringu teenuse osutamiseks Eesti tegevusluba, on tegelik äritegevus välismaal ja seos Eestiga puudub.[54] Ka andmed virtuaalvääringu teenuseosutajate arvelduskontode paiknemise kohta viitavad ettevõtete vähesele seotusele Eestiga. Ligi 40%-l ettevõtetest oli küsitlusele vastamise hetkel arvelduskonto Leedus, 25%-l Suurbritannias ja 10%-l Eestis. Eestist on pärit vaid ligikaudu 0,15% kõikidest Eesti tegevusloaga virtuaalvääringute teenusepakkujate klientidest.

Virtuaalvääringu globaalne mõõde teeb raskeks keskse järelevalve teostamise ja korrakaitseasutuste uurimise. Tehinguid tehakse riigipiiride üleselt ja mitmeid erinevates jurisdiktsioonides asuvaid teenusepakkujaid kasutades. Seega on raske kindlaks määrata, kelle jurisdiktsiooni tehtud tehingud kuuluvad ja kuidas tagada vastava informatsiooni kättesaadavus.

RAB uuringu kohaselt on Eestis jätkuvalt ohuks rahvusvahelise koostöö raskus. Teatud riikidega koostöö ei toimi, see muudab skeemide avastamise ja kuritegude tõkestamise keeruliseks, kuna peaaegu kõik juhtumid on rahvusvahelise haardega.

Võimalus kasutada kiiret finantstehnoloogiat „vahepeatusena“, rikastab kuritegeliku või ebaselge päritoluga raha kihistamise võimalusi. Kiired ja piiriülesed rahavood riikidest, mis ei tee efektiivselt rahvusvahelist koostööd, annavad kurjategijatele võimaluse vahendid legaalsesse ärisse suunata.

Tulenevalt Eesti heast ettevõtluskeskkonnast ja e-riigi võimalustest on Eestis äriühinguid kerge ja soodne luua ka mitteresidentidel või e-residentidel. Samuti tegutsevad turul nö riiulifirmade müüjad, kes loovad äriühinguid, mis müüakse edasi kas mitteresidentidele või e-residentidele, pakkudes ka postkasti(skeemi)teenust (ingl *letterbox*), luues selliselt näilise sideme Eestiga. Kolmandatest riikidest pärit mitteresidentide ja e-residentide puhul on probleemiks ka taustakontrolli tegemise keerukus. Näiteks tuvastas riigikontroll 2020. aastal, et Politsei- ja Piirivalveamet (PPA) on e-residendi digi-ID välja andnud välismaalastele, kellel on välisriigis kehtiv kriminaalkaristus.[55] Lähtudes eeltoodust võib **mitteresidentidest ja e-residentidest omanikega äriühingutega kaasnevat ohtu pidada „madalaks keskmiseks“.**

Lähtuvalt eeltoodust ning RahaPTS § 2 lg 5 ja § 31 lg 1 p 2 koostoimest, st virtuaalvääringu teenusepakkuja kui finantseerimisasutuse kohustusest tuvastada ja kontrollida isiku isikusamasus kas samas kohas viibides või kasutades infotehnoloogilisi vahendeid, võib **riigi või geograafilise asukohaga seotud ohte pidada „keskmiseks/kõrgeks“.**

Teenuste, toodete olemuse ning transaktsioonide ja jaotuskanalitega seotud ohud

- Plokiahela (ingl *blockchain*) tehnoloogia ei võimalda efektiivselt tehinguid monitoorida ja kahtlaseid tehinguid tuvastada, mis vähendab korrakaitseametite võimet jälitada kriminaalset tulu. Tehingud on IT-alaselt keerukad.
- Tehingute pseudo-anonüümsus, läbipaistmatus ja kiirus, sh ilma vara omanikku paljastamata.
- Hägustamistehingud, st hägustada seos kuriteo ja sellest saadud vara vahel, soovides jätta muljet, et tegemist on seaduslikult teenitud rahaga.
- Internetis ja piiriülese teenusena pakutult omavad suuremat riski (sh tumeveebi tehingud, virtuaalvarades või sularahas teostatavad tehingud).
- Virtuaalvääringute „segamise“ teenused (ingl *mixing services*) võimaldavad suuremat privaatsust (nt ebaseaduslikul teel saadud virtuaalvääring segatakse legitiimsega, mis teeb vara liikumise jälgimise oluliselt keerulisemaks, kui mitte võimatuks), kiiremaid ülekandeid, madalamaid ülekandetasusid ja väiksemat hinnakõikumist.

[53] Kättesaadav: https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b.
[54] 2020. aastal jõustunud RahaPTSi muudatused on olukorda parandanud.
[55] Allikas: https://www.riigikontroll.ee/Suhtedavalikkusega/Pressiteated/tabid/168/ItemId/1294/amid/557/language/et-EE/Default.aspx.

- Virtuaalvääringuid on võimalik soetada sularahas või kolmandate osapoolte ülekantud rahaga, mistõttu raha päritolu ei ole võimalik korralikult kindlaks teha.
- Virtuaalvarad, sh -vääringud võimaldavad pääseda rahale ligi anonüümselt, varjata ülekannete ajalugu, omada privaatvõtmeid, võtta sularaha välja sularahaautomaatidest.
- Detsentraliseeritud teenuse osutamise kanalid (sh sularahaautomaadid).
- Detsentraliseeritud platvormid, mis ei saa sekkuda kliendi tehingutesse.
- Ohuks on ka sellised virtuaalvääringu teenuse osutajad, kes klientide nimel privaatvõtmeid ei hoiusta, vaid pakuvad nn tööriistasid, mis võimaldavad kliendil enda privaatvõtmeid hoiustada ja sellest tulenevalt võib teenuseosutajal endal puududa ligipääs rahakotile.

Võimaliku ohu realiseerumise tõenäosuse analüüs Eestis
Kuigi virtuaalvääringud ja asjaomane sektor pärineb juba 2008. aastast, siis varasemalt võeti see omaks reeglina entusiastide ja nn virtuaalvääringute ekstremistide poolt, kelle prioriteediks on anonüümsus ja privaatsus. Kuigi virtuaalvääringud muutuvad üha populaarsemaks ka tavakasutajate seas, eeskätt investeerimis- või spekuleerimisinstrumendina, siis suur hulk kasutajaid on jätkanud nn ekstremistlikku suhtumist, rõhudes oma privaatsuse olulisusele. Sellest tulenevalt on virtuaalvääringute sektoris (võrreldes teiste käesolevas raportis käsitletus sektoritega levinud, et vaatamata kohustatud isiku nõudmisele keeldub klient hoolsusmeetmete rakendamisel asjaomase teabe esitamisest ja seda eeskätt kartusest, et tema privaatsust rikutakse ja asjaomased andmed saadetakse kohe maksuametile.

Anonüümsus ja tehingute läbipaistmatus paelub ka kurjategijad, kes näevad võimalust oma raha legaliseerimiseks läbi virtuaalvääringute. Virtuaalvääringu rahakottide omanike osas on vähem läbipaistvust ja kuigi tehingute tegemine on tehniliselt küll avalik, siis selle taga olevad isikud võivad jääda ja suuresti jäävadki siiski anonüümseteks. Tehingute peitmiseks kasutatakse nt hägustamismeetmeid, mis ei võimalda varade liikumist jälgida. Kui krüptovara muundub fiat rahaks, siis selle makse tegija on enamasti vahendaja, mistõttu ei pruugi nähtuda, kes on tegelikkuses vara omanik. Teenuseosutajatel on raske kontrollida vara päritolu kui virtuaalvääringute vahendusteenuse osutaja ei ole hoolsusmeetmeid korralikult täitnud.

Tehingute läbipaistmatus aitab kurjategijatel kiirelt liigutada rahalisi väärtusi ja seda eeskätt reguleerimata finantssektori teenusepakkujate kaudu. Ka virtuaalvääringu teenused on nende huviorbiidis. Kontrolli puudumine annab võimaluse kuritegelikul teel saadud raha „puhtaks pesta“. Eelnevat hõlbustavad ka keerulised omandistruktuurid ja tehingud seotud isikute vahel. Väiksemate teenuseosutajate puhul võivad taolised tehingud jääda vastava tähelepanuta, mh kompetentse inimressursi puudumise tõttu.

Virtuaalvääringuid on võimalik omandada ka sularaha eest, mis on oma olemuselt anonüümne ja seetõttu on oht finantssüsteemi ärakasutamiseks. Kuritegelikul teel saadud tulu võidakse välja võtta ka sularahas, et kaotada seos kuritegeliku tulu ja selle kasutaja vahel.

Kuna arveldus- või maksekonto omamine on virtuaalvääringu teenuse pakkujatel seadusest tulenev kohustus – RahaPTS § 72 lg 1 p 5, siis reguleeritud makseteenuse osutajate kasutamine võib ohtusid mõnevõrra maandada.

Lähtuvalt eelnevast võib teenuste, toodete olemuse ning transaktsioonide ja jaotuskanalitega seotud ohtu pidada „keskmiseks/kõrgeks“.

Klientidega seotud ohud
- **Isikutuvastusega seotud problemaatika** (sh tehingud kõrge riskiga kliendiga; teenuseosutaja ei suuda tuvastada tehingut, mille vastaspooleks on riikliku taustaga isik, kas skriinimise süsteemi või riikliku taustaga isikute nimekirjade puudulikkuse tõttu).

- **Tegeliku kasusaaja kindlakstegemine** (nt tehingute anonüümsus või pseudo-anonüümsus, kus teatud tehnoloogia kasutamisel on võimalik tegelik kasutaja[56] isik tuvastada; teenuseosutaja ei suuda tuvastada tegelikku kasusaajat kliendi või tehingu vastaspoole keerulise omandistruktuuri või tegelike kasusaajate info puudulikkuse tõttu registris).
- **Mitteresidentidest või e-residentidest kliendid** (teenuseosutaja ei suuda rakendada vastavaid hoolsusmeetmeid mitteresidentidest klientide või e-residentidest klientide suhtes nende tegeliku riskitaseme tuvastamise keerukuse tõttu).

Võimaliku ohu realiseerumise tõenäosuse analüüs Eestis

Eesti klientide puhul ei ole isikute tuvastamisega teadaolevalt probleeme. Kuna sektor on rahvusvaheline, siis globaalselt võib klientide tuvastamine olla problemaatiline (nt isikutuvastamise tehnoloogia tõhusus või kättesaadavus). Klientide osas sobilike hoolsusmeetmete rakendamisega on võimalik finantstehnoloogia sektorist eemale hoida isikuid, kes seda võiksid kuritarvitada. Vastasel juhul võivad kurjategijad rahalisi väärtusi liigutada läbi variisikute või ettevõtjate, mistõttu on keeruline tegeliku kasusaaja tuvastamine. Ohud eksisteerivad ka kliendisuhete loomisel internetis, kus on probleemiks isikut tõendavate dokumentide suurem väärkasutus. Väiksematel finantseerimisasutustel võib olla probleeme mitte-residentidest klientide vajalikul määral tuvastamisega ja seetõttu võib sattuda finantstehnoloogia sektorisse rahalisi vahendeid, mille omaniku või päritolu osas puudub selgus.

Sektoris on tuvastatud probleeme ka tunne-oma-klienti printsiibi ehk KYC põhimõtte rakendamisega. Nimelt on levinud väärarusaam, et KYC põhimõtte rakendamine tähendab üksnes isikusamasuse tuvastamist RahaPTS § 21 kohaselt (eeskätt rakendades kahe allika põhimõtet RahaPTS § 21 lg 4 järgi), mitte rahapesu ja terrorismi rahastamise hoolsusmeetmeid tervikuna RahaPTS § 20 järgi. Sellest tulenevalt tekitab kohustatud isik, kes lisaks isikusamasuse tuvastamisele kohaldab täiendavaid ning tugevdatud hoolsusmeetmeid, pahameelt klientide seas, mille tagajärjeks on informatsiooni ja dokumentide esitamata jätmine ja hoolsusmeetmete kohaldamise võimatus.

Lähtudes eeltoodust võib klientidega seotud ohtu pidada „keskmiseks/kõrgeks".

Regulatiivse keskkonnaga seotud ohud

- **Virtuaalvaradega seotud valdkonna alareguleeritus**.
- **Virtuaalvarade konfiskeerimise problemaatika**.
- **Erinevad nõuded, sh erineva tasemega regulatsioonid, EL liikmesriikides ja globaalsel tasandil**.
- Kuivõrd virtuaalvääringud ja -varad on väga uuenduslikud ja pidevas muutumises, on ohuks ka erinevate **regulatsioonides olevad definitsioonid**, mis võivad teatud teenused/tooted regulatsioonide rakendamisest välistada.
- **Koostöö teiste riikide järelevalveasutustega võib olla problemaatiline** (eriti kolmandate riikide pädevate asutustega).
- **Koostöö teenuseosutajate ja pädevate asutuste vahel** (teenuseosutajad sooviksid suuremat koostööd pädevate asutustega ja tõhusamaid koolitusi).
- **Valdkonnaspetsiifiliste suuniste ja juhendite puudus** (teenuseosutaja ei suuda tuvastada terrorismi rahastamisele suunatud või massihävitusrelvade levikut soodustatavaid tehinguid).
- **Spetsialiseerunud kohtunike ja pädevate järelevalveametnike puudus**.

Võimaliku ohu realiseerumise tõenäosuse analüüs Eestis

Finantstehnoloogia sektori kiire areng käib regulatiivsest keskkonnast sammu ees, võimaldades turule tuua uusi teenuseid, mis olemasoleva õigusraamistiku alt välja jäävad.

RAB uuringu kohaselt on probleemiks ebaselgus ka seadusandluses ja PPA sisemistes regulatsioonides seoses virtuaalvääringute arestimisega. Hetkel on see lihtsalt kokkuleppeline, menetlusalustele isikutele

[56] Tegelik kasusaaja on rahapesu ja terrorismi tõkestamise seaduse (edaspidi *RahaPTS*) § 9 lg 1 kohaselt füüsiline isik, kellel on lõplik valitsev mõju füüsilise või juriidilise isiku üle või kelle huvides, kasuks või nimel tehing või toiming tehakse. Lõplik valitsev mõju tuleneb omandisuhtest või muul viisil teise isiku kontrollimise kaudu.

pakutakse võimalust vääringud PPA krüptovaluuta kontole hoiule võtta või konverteerida need eurodeks. Analüüsimist vajab, kas kohtuotsuse resolutsioonides välja toodud virtuaalvääringute väärtus eurodes (mitte kogus krüptovääringus) on asjakohane, arvestades nimetatud vääringute väga suurt volatiilsust. Ka kohtunikud võivad vajada virtuaalvarade osas teatud küsimustes täiendavaid teadmisi (nt asjaomaseid koolitusi).

Lisaks piiriülesusele ja kasutaja võimalusele valida virtuaalvääringute teenuse kättesaadavus ükskõik milliselt teenusepakkujalt, tõstab sektori riski ka ühtsete normide puudumine ja õiguslik arbitraaž. ELi üleselt on ühtsete normide ja definitsioonide kokkuleppimine keeruline (siiani puudub asjaomane regulatiivne raamistik)[57], globaalses mastaabis on probleem veelgi suurem. Käesoleval ajal on EL tasemel läbirääkimistel Euroopa Parlamendi ja nõukogu määruse ettepanek, mis käsitleb krüptovaraturge, kuid selle menetlus võib võtta aastaid enne õigusakti jõustumist ja kohaldamist.

Kuna virtuaalvääringute regulatsioon on riigiti erinev, puudub riikidel sektorist ühesugune ülevaade või kontrollimise võimekus. Näiteks asub üks tehingu osapool riigis, kus tehingus osalejaid ei identifitseerita ega verifitseerita ning tehingute ajalugu, mis oleks seotud konkreetse isikuga, ei ole võimalik esitada või on regulatsioon nõrk, informatsioon RAB-le kättesaamatu ja raha liikumise jälgimine muutub võimatuks. Olukorras, kus vastavuskontrolliprogramm on kliendi vaatest liigselt koormav võrreldes konkurentide poolt kohaldatavate meetmetega, ei ole teenusepakkuja äri jätkusuutlik ega kasumlik, mille tulemusena lõpetatakse äritegevus või kohaldatakse rahapesu ja terrorismi rahastamise tõkestamise meetmeid vähemal määral.

Lisaks sobivustestidele (ingl *fit&proper*) ja muudele menetlustoimingutele, on oluline, et järelevalvel oleks ka ressurssi sügavuti analüüsida tegevusloa taotleja RahaPTS hoolsusmeetmeid, sh protseduurireegleid ja nende rakendamist, kuna käesoleval ajahetkel hetkel ei vasta osade tegevusluba omavate teenusepakkujate asjaomane vastavuskontrolliprogramm seadusest tulenevatele nõuetele ning seadusandja ja järelevalve ootustele. Niisamuti on oluline aru saada, kas tegevusloa taotleja vastavuskontrollifunktsiooni, eeskätt kontaktisiku funktsiooni täidab ametlik töölepingujärgne töötaja või vastavuskontrolli teenusepakkuja, milliste maht on Eestis märkimisväärne. Kui kontaktisiku funktsiooni täidab kolmas osapool, siis on ootuspärane, et vastavuskontrolli tase ega ajakohasus ei vasta teenusepakkujale omastele spetsiifilistele riskidele, ning sellises koostöövormis tegutseva kontaktisiku motivatsioon ei ole suunitletud tegelike riskide juhtimisele ega teenusepakkuja maine ega jätkusuutlikkuse tagamisele. Tagamaks seadusandja ja järelevalve ootuste täitmine ning nendest arusaam, on mh relevantne rõhuda ja julgustada riigi ja teenusepakkujate harmoniseeritud koostööle, et vastavad ootused oleksid täidetavad ja proportsionaalsed spetsiifilise sektoriga ja kaasnevate ohtudega. Leitud on ka, et pädevate asutuste infovahetus on keeruline, eeskätt suhtlus kolmandate riikide järelevalvetega.

Tulenevalt sellest, et Eestis on plaanis 2021. aastal tõhustada virtuaalvaradega seonduvat õiguskeskkonda, maandab see mitmeid ülalkirjeldatud ohtude realiseerumise võimalusi. Samuti on EL tasemel esitatud krüptovaraturgude reguleerimise ettepanek, mis parendab tulevikus õiguskeskkonda ka Euroopas tervikuna.

Lähtudes eeltoodust võib regulatiivse keskkonnaga seotud ohtu pidada „keskmiseks".

<u>Kuritegevus</u>

- Eestis RAB poolt välja antud virtuaalvääringu teenuse pakkuja tegevusluba on kasutatud välisriikides muude finantsteenuste osutamiseks, mis nõuavad vastavat tegevusluba ning selle eesmärgiks on olnud klientide eksitamine.
- Virtuaalvääringuid kasutatakse nii ebaseaduslike toimingute eest tasumiseks kui ka „musta" raha vahetamiseks.

[57] Euroopa Parlamendi ja nõukogu määruse, mis käsitleb krüptovaraturge ja millega muudetakse direktiivi (EL) 2019/1937, ettepanek, kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52020PC0593&from=EN.

- Probleemiks on virtuaalvääringute disainivigade ärakasutamine ja virtuaalvarade kasutamist lunarahanõuete (nn virtuaalsed väljapressimised) puhul (ingl ransomware).
- Digitaalsed tarneahelad võimaldavad hõlpsasti toime panna identiteedivargusi.
- Virtuaalvääringu rahakottide loomine ja suurte summade jagamine mitmete osapoolte vahel on lihtne, mistõttu on rahapesuskeemide tuvastamine virtuaalvääringute kasutamisel keeruline. Virtuaalvääringud võimaldavad kurjategijatel vara hoiustada formaalsest finantssüsteemist väljaspool ja digitaalselt, et selle päritolu ja lõpliku omandajat peita.
- Virtuaalvääringud ja -varad on populaarsed maksevahendid kurjategijate vahelistes tehingutes tumeveebis (ingl dark web).
- Arvutikelmused.
- Narkokaubandus.

Kurjategijad kasutavad finantstehnoloogia sektorit oma kuritegelikul teel teenitud vara liigutamiseks vähemalt ühes rahapesu faasis (paigutamine, laotamine, integratsioon). Majandustehingute eesmärk on peita kuritegeliku päritoluga vahendeid ja varjata nende tegelikku omanikku. Kiired piiriülesed rahavood riikidest, mis ei tee efektiivselt rahvusvahelist koostööd, annavad kurjategijatele võimaluse oma tulu legaalsesse ärisse suunata.

Rahapesu on kuritegu, millele eelnevad materiaalset tulu toovad kuriteod (eelkuriteod). Kui aastakümneid tagasi käsitleti eelkuritegudena ainult uimastikuritegusid, kus kuritegelik tulu oli eriti suur, siis nüüd on põhimõtteliselt iga kuritegu, millest kuritegelikku tulu saadakse, võimalik käsitleda rahapesu eelkuriteona.[58] Kuivõrd sularaha on oma olemuselt anonüümne, on oht, et finantssektorisse paigutatakse illegaalsel teel saadud sularaha.

Eesti majanduses on sularaha käive pigem väike. Maksudest kõrvalehoidumine, (küber)kelmustega ning narko- ja salakaubandusega teenitud tulu on sularaha mõistes Eestis ohukohtadeks, kus finantsteenuse osutajad võivad kokku puutuda suures koguses ebaselge päritoluga sularahaga, mida soovitakse peita või legaalsesse majandusse suunata.
Virtuaalvääringu teenuse osutajad võivad teenuseid pakkuda ka kurjategijatele või regulatsioonidega mittevastavuses olevatele juriidilistele isikutele, kui jäetakse piisaval määral rakendamata hoolsusmeetmed. Kuivõrd virtuaalvääringu sektor ja tehnoloogia on kiiresti arenev, on keeruline tagada piisavat riskiteadlikkust ja kõikide riskide maandamine.

RABi uuringu kohaselt on virtuaalvääringute kasutamine Eestis levinud kuritegelikes skeemides ning suur osa n-ö kuritegeliku keskkonna arveldamistest toimub virtuaalvääringutes. Samuti kasutatakse virtuaalvääringuid kuritegude ettevalmistamise faasis. Virtuaalvääringuid kasutatakse nii arvutikelmuste kaudu omandatud vara käitlemiseks kui ka narkootikumide kauplemisel.[59]

2018. aasta lõpus moodustas illegaalsete tehingute maht globaalselt 76 miljardit USD, s.o 46% kõikidest bitcoini tehingutest, mille turuosa sellel ajahetkel oli üle 63%, mis on peaaegu võrreldav USA ja ELi narkootiliste ainete turumahuga. Niisamuti leiti, et ligikaudu 26% kõikidest kasutajatest ja 23% kõikide virtuaalvääringu tehingute väärtusest võisid olla seotud ebaseadusliku tegevusega, eeskätt tumeveebiga. 2017. aasta aprilli seisuga eeldati, et 27 miljonit turuosalist kasutab bitcoini ebaseaduslikel eesmärkidel, tehes aastas ligikaudu 37 miljonit tehingut ja kollektiivselt kontrollides ligikaudu 7 miljardi USD väärtuses bitcoine. On täheldatud, et illegaalse tegevusega seotud bitcoini kasutajate maksetavad ja kasutusharjumused on erinevad kui seaduslikel eesmärkidel tegutsevatel kasutajatel. Näiteks, kui tavakasutajad omavad suuremat kogust bitcoini, kasutavad nad seda peamiselt investeerimise eesmärgil. Kurjategijad kasutavad tulenevalt varade külmutamise riskist bitcoine reeglina maksevahendina ja võivad teha rohkem tehinguid väiksemates summades ning suurema tõenäosusega teevad tehinguid

[58] Allikas: Pangaliit, https://pangaliit.ee/rahapesu-tokestamine.
[59] RAB, Virtuaalvääringu teenuse pakkujate uuring, lk 19.

tumbler'ite või *mixer*'itega ja samade tehingupartneritega. Nt bitcoini tehingute võrgustik illegaalide vahel on 3 kuni 4 korda tihedam kui tavakasutajate vaheline.[60]

Samuti on oluline märkida, et kuigi üksnes 5% aktiivsetest virtuaalvääringu teenusepakkujatest täitis 2019. aastal RahaPTS-s sätestatud teavitamiskohustust ning kõikidest virtuaalvääringu sektori teadetest 93% oli esitatud vaid 3 turuosalise poolt, siis ülalkirjeldatud uuringu järeldus kurjategijate bitcoinide kasutamise kohta väljendub ka RAB teadete esitamise statistikas. Kui ebahariliku tehingu (UTR) osakaal virtuaalvääringu sektori teadetest oli olematu, siis teated ebahariliku tegevuse kohta (UAR) moodustasid kõikidest teadetest 14,1%. Lähtudes virtuaalvääringu teenusepakkujate allutamisest finantseerimisasutustega võrdväärsetele RahaPTS nõuetele, võib eeldada, et nii rahapesu kui ka terrorismi rahastamise tuvastamise vahendid, meetodid, hoolsusmeetmed ja RAB-le esitatavate teadete kvantiteet ja kvaliteet on edaspidi paranenud. Eelnevat väljendab ilmekalt ka asjaolu, et erinevalt sularahast või pangaülekannetest on virtuaalvääringu tehingud plokiahelas avalikult kättesaadavad ning kasutades skriinimis- ja monitoorimissüsteeme ja erinevaid tehingute analüüsimismeetodeid on võimalik tuvastada virtuaalvääringute tegelik päritolu ja sihtpunkt.

Lähtudes eeltoodust võib kuritegevusega seotud ohtu pidada „keskmiseks/kõrgeks".

<u>Järeldus</u>
Virtuaalvääringu sektor
Kuigi virtuaalvääringud on rahapesijate hulgas populaarseks maksevahendiks, siis on virtuaalvääringu teenusepakkujatel asjakohaste investeeringute ja mehhanismide rakendamisel võimalik sellised isikud ja tehingud tuvastada ning sellest järelevalvele teada anda. Seetõttu leiame, et siiani on üleüldine virtuaalvääringu sektori rahapesu oht olemas, kuna asjakohased investeeringud, kompetents ja motivatsioon, jättes arvestamata üksikud teenusepakkujad, on tervikuna sektoris veel madal. Samuti esineb puudujääke regulatiivsel tasandil, seda nii riigisiseselt kui ka globaalselt.

Lähtudes eeltoodust võib virtuaalvääringutega seotud ohtusid pidada „keskmiseks/kõrgeks".

7.3.2. Üldlevinud ohud

<u>Ühisrahastusega seotud võimalikud ohud:</u>

Riigi või geograafilise asukohaga seotud ohud

- Ka ühisrahastussektor on rahvusvaheline, võimaldades viia kokku investoreid ja rahastuse taotlejaid üle kogu maailma. Teenuseosutajal on globaalne haare, viies kokku investorite ja projektiomanike huvisid, kes asuvad erinevates jurisdiktsioonides. Projekti omanik, investor või nende asjakohased tegelikud kasusaajad võivad asuda jurisdiktsioonis, mis on seotud kõrgemate rahapesu/terrorismi rahastamise riskidega või ilma tõhusate rahapesuvastaste vahendite või terrorismi rahastamise tõkestamise alase järelevalveta. Ühisrahastusteenuse osutaja klient võib asuda kus iganes maailmas, sh kõrge riskiga piirkonnas[61].
- Rahalised vahendid saadakse isiklikest või ärilistest sidemetest jurisdiktsiooniga, mille usaldusväärsed allikad on tuvastanud olulise seose korruptsiooniga või muu kuritegeliku tegevusega nagu terrorism, rahapesu, ebaseaduslike uimastite tootmine ja tarnimine või muud eelkuriteod.

<u>Võimaliku ohu realiseerumise tõenäosuse analüüs Eestis:</u>

[60] S. FOLEY, J. R. KARLSEN and T. J. PUTNIŅŠ, "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?", December 2018, 26, lk-d 1-3. Arvutivõrgus kättesaadav sellelt lingilt.
R. HOUBEN., A. SNYERS. European Parliament. „Crypto-assets. Key developments, regulatory concerns and responses.", April 2020, lk 25. Arvutivõrgus kättesaadav sellelt lingilt.
[61] Sectoral guideline for regulated crowdfunding platforms (Guideline 17), https://eba.europa.eu/calendar/draft-guidelines-under-articles-17-and-184-directive-eu-2015849-customer.

Ligikaudu 60% Eesti ühisrahastusettevõtjate poolt vahendatavate projektide rahastusest toimub Eestis ja 40% välismaal. Eesti osakaal ajas väheneb, sest ettevõtjad laienevad välismaale, seda soodustab ka EL ühisrahastusmääruse rakendamine alates 10.11.2021, mis annab võimaluse teenuseosutajatel tegutseda ELis ühtsete nõuete alusel ja ühe tegevusloaga.

Lähtudes eeltoodust võib riigi või geograafilise asukohaga seotud ohtu pidada „keskmiseks".

Teenuste, toodete olemuse ning tehingute ja jaotuskanalitega seotud ohud

- Ühisrahastusteenuste osutamine internetis, veebiplatvormide kaudu.[62]
- Investeerimis- ja krediidipõhise ühisrahastuse puhul on võimalik kaasata suuremaid summasid (kõrgem risk kui annetuspõhistel ärimudelitel), kuigi üldjuhul on sellised platvormid reguleeritud (sh avalikustamise nõuded ja krediidiasutuste kasutamine).
- Ühisrahastusteenuse osutaja aktsepteerib platvormil sularahainvesteeringuid või lubab sularaha platvormilt välja võtta.[63] Mõned ühisrahastusteenuse osutajad võimaldavad investeerimist ka krüptovaradesse või nimetatud vahenditega ühisrahastusplatvormi kaudu makseid teha.[64]
- Ühisrahastusteenuse osutaja võimaldab platvormil teha ülekandeid investorite või projektiomanike vahel või teha investoritel platvormi kaudu projekti omanikule makse instrumentidega, mis ei ole reguleeritud või mille suhtes kehtivad vähem ranged rahapesu tõkestamise/CFT nõuded kui direktiivis (EL) 2015/849.
- Ühisrahastusteenuse osutaja ei piira ühisrahastusplatvormi kaudu töödeldud tehingute suurust, mahtu ega väärtust, ühisrahastusplatvormi kaudu töödeldud laadimist ega tagasivõtmist (ingl *loading or redemption*) ega üksikute investorite kontodel hoitavate vahendite hulka.
- Ühisrahastusteenuse osutaja võimaldab investeeringute ennetähtaegset lunastamist, laenude ennetähtaegset tagasimaksmist või investeeringute või laenude edasimüüki järelturgude kaudu, samuti finantsvõimendust või privilegeeritud lunastamist või garanteeritud tootlust.
- Krediidipõhise ühisrahastuse puhul ei ole arusaadavalt esitatud nominaalset intressimäära, intressi maksmise kuupäeva, intressimaksete tähtpäevi, tähtaega ja rakendatavat tootlust.
- Ühisrahastusteenuse osutaja võimaldab investoritel ja projektiomanikel hoida ühisrahastusplatvormil mitut kasutajakontot.
- Ühisrahastusteenuse osutaja haldab ühisrahastusplatvormi täielikult veebis ilma piisavate kaitsemeetmeteta, näiteks isiku elektrooniline tuvastamine, kasutades selleks elektroonilisi allkirju või elektroonilisi isikut tõendavaid dokumente, mis vastavad määrusele (EL) nr 910/2014. Kliendid on aktsepteeritud või vastu võetud (*on-boarded*) ilma näost näkku isikusamasuse kontrollimiseta ja kaitsemeetmed ei ole pagas.
- Ühisrahastusteenuse osutaja pakub oma teenuseid väljaspool mis tahes regulatiivset režiimi ja seetõttu ei pruugi olla rakendatud meetmeid, mis tuvastaksid või maandaksid riske seoses ühisrahastusteenuse osutaja kasutamisega rahapesu või terrorismi rahastamise eesmärgil.

[62] ACAMS, Crowdfunding: The New Face of Financial Crimes?, http://files.acams.org/pdfs/2017/Crowdfunding_The_New_Face_of_Financial_Crimes_S.Sessoms.pdf. Eesti finantstehnoloogia sektori haavatavused dokumendianalüüs, lk 39.

[63] Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (''The Risk Factors Guidelines''), amending Guidelines JC/2017/37, Guidline 17, lk 125, https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2020/Draft%20Guidelines%20under%20Articles%2017%20and%2018%284%29%20of%20Directive%20%28EU%29%202015/849%20on%20customer/JC%202019%2087%20CP%20on%20draft%20GL%20on%20MLTF%20risk%20factors.pdf.

[64] Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (''The Risk Factors Guidelines''), amending Guidelines JC/2017/37, Guidline 17, lk 126.

- Ühisrahastusteenuse osutajate puhul on riskifaktoriteks, kui platvorm võimaldab raha hiljem edasi kanda (näiteks teadmata projekti jaoks raha kogumine või raha tagastamine investoritele), investeeringute edasimüümise võimekus, platvorm ei sea ülekannetele limiite, makseid on võimalik teha vääringutega, mida ei reguleerita või mis on nõrgalt reguleeritud, platvorm võimaldab sularaha sisse/väljamakseid, platvorm ei võimalda tagasiostmist, platvormi makseid saab teha virtuaalvääringutes, võimaldab klientidel hallata mitut kontot, mis ei ole omavahel seotud.[65]

Võimaliku ohu realiseerumise tõenäosuse analüüs Eestis

Ühisrahastusteenuse osutajad peavad teenuste osutamiseks kasutama üldjuhul maksekontot, mida pakuvad näiteks krediidi- ja makseasutused. Kuivõrd krediidiasutused on tugevalt reguleeritud isikud, siis nende teenuste kasutamine aitab teatud ohtusid maandada. Teenuseosutajad on seega huvitatud, et neil oleksid paigas korrektsed protsessid, mis aitavad toime tulla finantstehnoloogia sektoris esinevate ohtudega, et vastata maksekonto teenust osutava isiku poolt seatavatele nõuetele.

Eeltoodust lähtuvalt võib teenuste, toodete olemuse ning transaktsioonide ja jaotuskanalitega seotud ohtusid pidada „madalaks/keskmiseks".

Klientidega seotud ohud

- Isikutuvastusega ja tegeliku kasusaaja kindlakstegemisega seotud problemaatika (teenuseosutaja ei suuda tuvastada tehingut, mille vastaspooleks on riikliku taustaga isik, kas skriinimise süsteemi või riikliku taustaga isikute nimekirjade puudulikkuse tõttu; teenuseosutaja ei suuda tuvastada tegelikku kasusaajat kliendi või tehingu vastaspoole keerulise omandistruktuuri või tegelike kasusaajate info puudulikkuse tõttu registris).
- Mitteresidentidest või e-residentidest kliendid (teenuseosutaja ei suuda rakendada kohaseid hoolsusmeetmeid mitteresidentidest klientide või e-residentidest klientide osas).
- Investor küsib privilegeeritud tingimusi või fikseeritud investeeringutasuvust või palub investeeringu tagasi osta lühikese aja jooksul pärast alginvesteeringut või kannab platvormile vahendeid, mis ületavad projekti jaoks nõutavaid summasid, ja palub seejärel ülejäävad summad tagasi maksta. Investeerimiseks mõeldud vahendite allikas on ebaselge ja investor ei soovi seda teavet nõudmisel esitada. Investeeritud varade aste ületab hinnanguliselt investori likviidsete varade mahtu. Investeeritud vahendid on laenatud. Investor keeldub nõutava teabe esitamisest, mis on vajalik teenuseosutajale kliendi nõuetekohase hoolsuse menetluse läbiviimiseks.
- Rahastuse taotleja äriplaanil (investeerimisprojektil) puudub ilmne strateegia või majanduslik eesmärk. Rahastuse taotleja kiirendab ootamatult või mõistliku selgituseta kokkulepitud lunastamis- või tagasimaksegraafikut, kas ühekordse väljamakse või ennetähtaegse lõpetamise abil. Rahastuse taotleja näib olevat vastumeelne projekti või selle omaniku kohta teabe esitamisel.

Võimaliku ohu realiseerumise tõenäosuse analüüs Eestis

Eesti klientide puhul ei ole isikute tuvastamisega teadaolevalt probleeme. Kuna sektor on rahvusvaheline, siis globaalselt võib klientide tuvastamine olla problemaatiline. Puudujääke on nii kasutatavas isikutuvastamise tehnoloogias kui mujal. Samas tehakse siiani enamus tehinguid Eestis, mistõttu on oht kindlasti väiksem kui virtuaalvääringu teenuse osutajate puhul. Ohud eksisteerivad ka kliendisuhete loomisel internetis, kus on probleemiks isikut tõendavate dokumentide suurem väärkasutus. Väiksematel teenuseosutajatel võib olla probleeme mitte-residentidest klientide soovitud määral tuvastamisega ja seetõttu võib sattuda finantstehnoloogia sektorisse rahalisi vahendeid, mille omaniku või päritolu osas puudub selgus. Klientide osas sobilike hoolsusmeetmete rakendamisega on võimalik finantstehnoloogia sektorist eemale hoida isikuid, kes seda võiksid kuritarvitada.

Eeltoodust lähtuvalt võib klientidega seotud ohtusid pidada „madalaks/keskmiseks".

[65] EBA acts to improve AML/CFT supervision in Europe, https://eba.europa.eu/eba-consults-revised-guidelines-money-laundering-and-terroristfinancing-risk-factors.

Regulatiivse keskkonnaga seotud ohud

- Valdkonnapõhised regulatsioonid on alles arengujärgus, mis võimaldab teenusepakkujatel tegutseda limiteeritud või puuduva järelevalve all. Riski nähakse ka selles, et uued regulatsioonid on kehtestatud peamiselt omakapitalipõhistele platvormidele (investoritelt rahastuse kaasamine läbi ettevõtete osaluse müügi) ning jättes seeläbi finantstööstuse avatuks riskidele, mis seonduvad pettuste, rahapesu ja terrorismi rahastamisega.[66]
- Ühisrahastusteenuse osutamine ei pruugi olla käesoleval ajal finantsjärelevalve all ning nimetatud teenuseosutajad ega rahastuse taotlejad ei pea esitama kohustuslikke aruandeid ega teavet. Projekti kohta saadav informatsioon võib seetõttu olla piiratud.[67] Mitmetes EL liikmesriikides ei ole ühisrahastusteenuse osutajad reguleeritud või on reguleeritud üksnes teatud kategooriad.
- Ühisrahastusteenuse osutajaid ei käsitleta rahapesu ja terrorismi rahastamise tõkestamise regulatsioonide osas kui kohustatud isikuid.

Võimaliku ohu realiseerumise tõenäosuse analüüs Eestis

2021. aastal on plaanis reguleerida Eesti ühisrahastussektor, sh kehtestada asjaomased tegevusnõuded, tegevusloa kohustus ja järelevalve. Vt täpsemalt ühisrahastussektori õigusraamistiku alapunktis kirjutatut.

Eeltoodust lähtuvalt võib regulatiivse keskkonnaga seotud ohtusid pidada „madalaks/keskmiseks".

Kuritegevus

- Eestis on asutatud ühisrahastusettevõtteid sooviga panna toime investeerimiskelmust, kuna regulatsioon on olnud ebapiisav ning ettevõtte loomine lihtne/kiire ja suhteliselt odav.[68] Aktuaalsed on pettused ja investorite usalduse kuritarvitamine (nt fiktiivsed projektid, mille eesmärgid ei realiseeru).
- Ohuks võib olla ka organiseeritud kuritegevuse poolt loodud ühisrahastusplatvormide risk või variisikute kasutamine.

Võimaliku ohu realiseerumise tõenäosuse analüüs Eestis

Käesoleval ajal võib eelviidatud ohtude realiseerumine olla keskmine/kõrge. Eestis on asutatud ühisrahastusettevõtteid sooviga panna toime investeerimiskelmust, kuna regulatsioon on olnud ebapiisav ning ettevõtte loomine lihtne, kiire ja suhteliselt odav. Näiteks pandi 2019. ja 2020. aastal toime pettusi seoses ühisrahastusteenuste osutamisega. Mitmel juhul oli tegemist e-residendi poolt Eestis asutatud äriühinguga, millel puudus muu seos Eestiga, ka ettevõtte tegevuse juhtimine toimus välismaalt.[69]

Eeltoodust lähtuvalt võib kuritegevusega seotud ohtusid pidada „keskmiseks".

Järeldus

Ühisrahastussektor

Eesti ühisrahastussektoris on rahapesuga seotud ohtude esinemise tõenäosus pigem madal. Sektor on väike ja vahendatavate tehingute mahud on endiselt marginaalsed. Siiani ei ole Eestis tuvastatud ühtegi rahapesu juhtumit, mis oleks seotud ühisrahastusteenuste osutamisega.

Eeltoodust lähtuvalt võib klientidega seotud ohtusid pidada „madalaks/keskmiseks".

7.3.3. Terrorismi rahastamise ohud

[66] ACAMS, Crowdfunding: The New Face of Financial Crimes?, http://files.acams.org/pdfs/2017/Crowdfunding_The_New_Face_of_Financial_Crimes_S.Sessoms.pdf. Eesti finantstehnoloogia sektori haavatavused dokumendianalüüs, lk 39.

[67] Eesti finantstehnoloogia sektori haavatavused, dokumendianalüüs.

[68] Vt https://www.politsei.ee/et/uudised/kas-envestio-ja-kuetzal-puhul-oli-tegemist-pettusega-1151.

[69] Vt nt https://www.politsei.ee/et/uudised/kas-envestio-ja-kuetzal-puhul-oli-tegemist-pettusega-1151. Vt ka ECN reports Kuetzal and Envestio to National Conduct Authority, https://eurocrowd.org/2020/01/22/ecn-reports-kuetzal-and-envestio-to-national-conduct-authority/.

Enamlevinud ohud

Virtuaalvääringute sektoris üldlevinud riskistsenaariumid:

- Virtuaalvarasid on globaalsel tasandil lihtne liigutada.
- Virtuaalvarade olemusega seotud ohud, sealhulgas (pseudo-)anonüümsus[70] ja kiirus, internetis ja piiriülese teenusena kasutamise võimalus, anonüümne ligipääs varale, ülekannete ajaloo varjamise võimalus, privaatvõtmete omamine ja sularahaautomaatide kasutamise võimalus. Terroriorganisatsioonid kutsuvad avalikult oma tegevust toetama kas kombineeritult „makseteenuse osutaja + virtuaalvääring" või ainult virtuaalvääringus, et tagada transaktsioonidel maksimaalne anonüümsus.
- Virtuaalvara „segamise" teenuse (ingl *mixing services*) osutamine võimaldab suuremat privaatsust, kiiremaid ülekandeid, madalamaid ülekandetasusid ja väiksemat hinnakõikumist.
- Teenuseosutajate ebapiisav teadlikkus terrorismi rahastamise osas võib põhjustada terrorismi rahastamise suhtes rakendatavate hoolsusmeetmete ebapiisavust.
- Kuigi alates 10.03.2020 kehtivad virtuaalvääringu teenuse pakkujatele samasugused RahaPTS nõuded nagu finantseerimisasutustele, esineb endiselt probleeme „tunne-oma-klienti" ehk KYC nõuete täitmisega. Seetõttu eksisteerib oht, et teenust osutatakse terrorismi rahastamise tõttu näiteks sanktsioneeritud isikutele. Üldjuhul ei toimu virtuaalvara teenuse osutamisel näost näkku kohtumist, mis omakorda võib võimaldada anonüümselt rahastamise või toodete soetamise (sularaha sissemaksed või maksed kolmandate isikute poolt, milles ei tuvastata vahendite päritolu) olukorras, kus teenusepakkuja jätab kohased hoolsusmeetmed kohaldamata. Samuti on ohuks anonüümsed ülekanded, kui saatjat ja saajat korrektselt ei tuvastata.
- Teadlikkuse probleem riskidest, mh sellest, milliseid meetodeid kasutavad terroristlikud organisatsioonid krüptoraha väärkasutamisel ja sellega seotud tehnilistes vahendites raha kogumiseks, ülekandmiseks või hoidmiseks, esineb kindlasti ka ametkondlikul tasemel, mistõttu ei pruugi regulatiivne keskkond vastata alati reaalelu vajadustele. Seetõttu pakuvad tehnoloogilised arengud sektorile ja ka regulaatoritele uusi väljakutseid terrorismi rahastamise vastases võitluses.
- Kuivõrd virtuaalvääringud ja -varad on populaarsed maksevahendid kurjategijate omavahelistes tehingutes, siis võib eeldada, et on oht, et neid võidakse kasutada ka terrorismi rahastamises. Samas möönab RAB oma uuringus, et terrorismi rahastamise kohta virtuaalvääringute abil on võrdlemisi väike arv kinnitatud juhtumeid. On tuvastatud juhtumeid, kus islami- või paremäärmuslaste rühmitused on virtuaalvääringuid kasutanud tumeveebist ebaseaduslike esemete (nt relvad) soetamiseks, ühisrahastusplatvormidel kapitali kogumiseks või varade rahvusvaheliseks liigutamiseks (P2P ehk isikult isikule kannetega). Seega koguvad virtuaalvääringud populaarsust islamiäärmuslaste seas, kes kasutavad neid rahakogumiskampaaniate korraldamisel, jagades anonüümseid rahakotiaadresse läbi sotsiaalmeedia või suhtlusrakenduste.[71] Kasutades tõhusaid tehingute skriinimis- ja monitoorimismehhanisme, on eelnevale vaatamata virtuaalvääringu teenusepakkujatel võrdlemisi tõhus võimekus sellised aadressid tuvastada, tehingud peatada ning RAB-le asjaomast informatsiooni jagada.

Ühisrahastussektoris üldlevinud riskistsenaariumid:

- Ehkki ühisrahastuse veebisaidid pole täiesti uued, tekitavad nad täiendavat riski, kuna need on spetsiaalselt loodud rahastamise ja annetuste saamiseks. 2015. aastal tõstis Euroopa Väärtpaberiturujärelevalve (ESMA) esile investeeringupõhiste ühisrahastusteenuste ohtu: neid võidakse kuritarvitada terrorismi rahastamiseks, eriti kui platvormid teostavad projektiomanike ja nende projektide osas hoolsuskohustust piiratud ulatuses või üldse mitte.[72]

[70] Anonüümsus ja pseudo-anonüümsus (teatud tehnoloogia kasutamisel on võimalik tegelik kasutaja isik tuvastada).

[71] Vt lisaks ACAMS, New Technologies: The Emerging Terrorist Financing Risk, 03.06.2020, https://www.acamstoday.org/new-technologies-the-emerging-terrorist-financing-risk/.

[72] Questions and Answers: Investment-based crowdfunding: money laundering/terrorist financing, European Securities and Markets Authority, 1 July 2015, https://www.esma.europa.eu/sites/default/files/library/2015/11/esma_2015_1005_qa_crowdfunding_money_laundering_and_terrorist_financing.pdf.

- Üks riskitüpoloogia on annetuspõhise ühisrahastusteenuse kuritarvitamine terrorismi rahastamiseks. Heategevusannetuste väärkasutamine terrorismi rahastamiseks on paljude terroriorganisatsioonide üks peamisi rahastamisvooge. Finantsteenuste rakkerühm (FATF) on avaldanud selle teema kohta konkreetsed juhised soovituses 8.[73] On tuvastatud ühisrahastuse veebisaitide kuritarvitamise juhtumeid väidetavate heategevuslike eesmärkide jaoks, millest said lõpuks kasu terrorirühmitused.[74] Seadusloojate ja pädevate asutuste väljakutseks on teabe puudumine nende platvormide kampaaniatele kaasaaitajate kohta.[75]
- Eriline tähelepanu peaks olema suunatud jurisdiktsioonidele, mis teadaolevalt rahastavad või toetavad terroriakte või kus teatakse, et tegutsevad terroriakte sooritavad rühmad, ning jurisdiktsioonidele, mille suhtes kehtivad rahalised sanktsioonid, embargo või meetmed (välja andnud näiteks EL või ÜRO), mis on seotud terrorismi, terrorismi rahastamise või leviku tõkestamisega.

7.3.4. Järeldus

Eesti ei ole oma geograafilise asukoha ja väikesearvulise moslemikogukonna tõttu terroriaktide toimepanemiseks islamiäärmuslaste jaoks esimene eelistus. Samas on Eesti lähinaabruses Skandinaavias ja Venemaal suured moslemikogukonnad, mistõttu mitmed islamiäärmuslikult meelestatud isikud kasutavad Eestit transiitriigina. Siinne soodne majanduskeskkond ja kinnisvaraturg on äratanud aktiivset ärihuvi ka eelmainitud kogukondades. Muudest allikatest tõusetuv terrorismioht on islamistliku terrorismi kõrval väga väike.

Eesti innovaatiline ja arenenud finantstehnoloogia sektor võib muutuda tulevikus üha atraktiivsemaks islamiäärmuslaste jaoks terrorismi rahastamise ja toetamise seisukohast. Islamiäärmuslikku vaadet omavate isikute ja rühmituste seas on traditsioonilised terrorismi rahastamise kanalid asendumas alternatiivsete finantsteenuse osutajatega. Virtuaalvääringud võivad tagada ka täieliku anonüümsuse.

RAB-le on laekunud virtuaalvääringu teenuse osutajatelt teateid, kus terrorismiga seotud sanktsioneeritud isikud on soovinud luua ärisuhteid, mis on selge viide virtuaalvääringute atraktiivsusele terrorismi rahastamise vaates.

Samuti ei ole tugevdatud hoolsusmeetmete kohaldamine vaid tehingu piirmäärade ületamisel enam asjakohane ega tõhus. Enamik terrorismi rahastamise kahtlusega tehingud on teostatud väikestes summades (ka alla 10 euro). Selliseid summasi võimaldab hõlpsasti investeerida ühisrahastussektor, sh väikestes summades annetada, kasutades annetuspõhiseid ühisrahastusplatvorme.

Eeltoodust lähtuvalt võib virtuaalvääringu teenuse osutamisega seotud terrorismi rahastamise ohtusid pidada pigem „kõrgeks“, ühisrahastusteenuse osutamisega seotud riske „keskmiseks“.

7.4. Haavatavused

7.4.1. Rahapesu tõkestamise haavatavused

Käesoleva riskihinnangu raames hinnati[76] finantstehnoloogia sektori **rahapesu haavatavuse taset** järgmiselt:

[73] Risk of Terrorist Abuse in Non-Profit Organisations, Financial Action Task Force, June 2014, https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf.
[74] APG/MENA FATF Social Media and Terrorism Financing Report, 23 January 2019, Asia/Pacific Group On Money Laundering, http://www.apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=1142.
[75] Alexandra Posadzki, “Hard to identify crowdfunding platforms financing terrorism,” The Star, 18 May 2017, https://www.thestar.com/business/2017/05/18/hard-to-identify-crowdfunding-platforms-financing-terrorism.html.
[76] NRA ohtude töörühma poolt antud hinnangud, mis põhinevad riskihinnangu läbiviimise metoodikal.

Tabel 38. Finantstehnoloogia alamsektorite rahapesu haavatavuse tasemed

Finantstehnoloogia sektor	**Rahapesu haavatavuse tase sektori tasandil**	
Virtuaalvääringud	**3,02**	Keskmine/kõrge
Ühisrahastus	**1,99**	keskmine/madal

Virtuaalvääringu sektor

Virtuaalvääringu sektoris esinevad järgmised haavatavused:

- Järelevalveasutusel pole piisavalt vahendeid (inim-, IT, õiguslikke ja ajalisi ressursse), et sisuliselt teostada kontrolli virtuaalvääringute turule suunduvate äriühingute vastavuse osas. Alles 2019. a sai RAB juurde töötajaid (kokku on 9 inimest, kes tegelevad järelevalve ja tegevuslubade väljastamisega), et paremini toime tulla 2018-2019 virtuaalvääringute loataotlustest tuleneva töö mitmekordse kasvuga. Alles 2020. a märtsist muutus tegevusloa kontrollieseme ulatus, pikenes tegevusloa menetluse tähtaeg 60 päevani, riigilõivu määr suurenes 3300 euroni, osakapitali suurus peab olema vähemalt 12 000 eurot ning määratud peab olema ka kontaktisik. Lisatud meetmed võimaldavad turgu küll korrastada, kuid see on riigis toimunud suure viivitusega. Meetmete tõhustamine peab jätkuma, sest pole mõistetav, et Eesti turule mahuks ära üle 400 virtuaalvääringu teenuse pakkuja nii, et kõiki suudaks järelevalve ja ennetustegevusega seaduse nõuetega kooskõlla viia ja hoida. Samuti tuleb analüüsida, kes võiks olla tulevikus pädev asutus asjaomaste tegevuslubade väljastamiseks. Nimetatud kohustus peab olema kaetud ka piisavate ressurssidega.
- Järelevalveasutusel pole piisavalt ressursse, et läbi viia ka riskipõhist järelevalvet määral, mis annaks teadmist sektoris tegutsevatest äriühingutest ning vajadusel nõuetega kooskõlas mitteolevatelt isikutelt lubade äravõtmist. Samuti pole võimalik teha järelevalvet uute tegevuslubadega ettevõtet osas, et välja selgitada õigeaegselt, kas äriühing on tegevust alustanud või mitte ning vastavalt sellele puhastada turgu äriühingutest, kellel pole oma tegevuseks luba vaja. Läbi selle oleks aga võimalik vähendada ka tegevuslubade väärkasutamise ohtu. Teadlikkuse kasvuks järelevalveasutuses ei ole piisavalt ajalist ressurssi, sest kõik on hõlmatud kas tegevuslubade väljastamisega või kohapealsete kontrollide läbiviimisega. Efektiivse järelevalve puudumisel võib realiseeruda risk, et virtuaalvääringute sektorit kasutatakse rahapesu toimepanemiseks.
- Anonüümsus – alates 10.03.2020 on virtuaalvääringu teenuse pakkujatel anonüümsete teenuste osutamise keeld (RahaPTS § 25 lg 1 ja 2). See tähendab, et juhuti tehingute tegemisel ja ärisuhte loomisel tuleb tuvastada kliendi isikusamasus ja kontrollida esitatud teavet, sõltumata tehingu summast. Sellest hoolimata on oht, et teenusepakkujad ei järgi seaduses sätestatud nõudeid ja teenuse tarbijate isikusamasus jäetakse (korrektselt) tuvastamata.
- Tagasisidest virtuaalvääringu teenuse pakkujatele selgus, et 2019. aastal suunati vaid 8 sektori teadet süvaanalüüsi ja pädevatele Eesti uurimisasutustele edastati 7 teate informatsioon, kuivõrd enamikel teates esitatud isikutel puudub seos Eestiga ja tegemist on välisriigi kodanikega. Haavatavuseks võib olla liiga väheste teadete puhul süvaanalüüsi teostamine, aga ka näiteks olukord, kus teatest ei selgu mingitel põhjustel esitamise tegelik põhjus või ei tooda välja kõiki olulisi põhjuseid. Seetõttu vajaks edaspidi täpsemat analüüsi teadete esitamisega seonduv.
- Segamise teenus (ingl *mixing services*) võimaldab suuremat privaatsust, kiiremaid ülekandeid, madalamaid ülekandetasusid ja väiksemat hinnakõikumist. Samuti võimaldab antud teenus ebaseaduslikul teel saadud virtuaalvääringu segada legitiimsega, mistõttu on raskendatud või koguni võimatu tuvastada vara liikumist.
- Kui sularaha osakaal sektoris on madal, siis arvestatavat riski Eesti finantssektorile mõjutab virtuaalvääringute teenusepakkujate kliendiportfell, millest üksnes 0,15% moodustavad Eestist pärit isikud. Samas pärineb statistika 2019. aasta novembrikuu RABi küsitlusest, mil oli väljastatud 1282 tegevusluba virtuaalvääringu raha vastu vahetamise ja 1165 tegevusluba virtuaalvääringu rahakotiteenuse pakkumiseks, sellest unikaalseid ettevõtteid oli kokku 1308.

Seisuga 01.08.2020 ja tänu virtuaalvääringu teenuseosutajate võrdsustamisele finantseerimisasutustega kehtis erinevaid virtuaalvääringute tegevuslube kokku 611 (295 virtuaalvääringu raha vastu vahetamise teenuse, 261 rahakotiteenuse ja 55 virtuaalvääringu teenuse luba). 2020. aasta lõpu seisuga tegutses Eestis 419 virtuaalvääringu teenuse osutajat. Kuivõrd eelnev seadusemuudatus keelas virtuaalvääringu teenusepakkujatel nii ärisuhte välise teenuse osutamise kui ka allutas neid RahaPTS §-s 31 sätestatud EEA päritolu piirangutele, võib järeldada, et mitteresidentidega, eriti suurema riskiga klientidega, kaasnev risk on märkimisväärses langustrendis ja eestlaste, sh teiste EEA lepinguriikidest pärit isikute osakaal turuosaliste kliendiportfellis suureneb.

- Virtuaalvääringute ostmine ja müümine sularahas läbi ATM-de, mille puhul on isiku tuvastamine puudulik.
- Infovahetus kriminaalmenetlustes erinevate õiguskaitseasutuste ja RAB-i vahel ei ole automaatne, vaid sõltub konkreetse menetleja huvist infot edastada. RAB-il ei ole võimalik teada saada, millistes kriminaalmenetlustes on kuritegeliku tegevuse tulemusel saadud vara konverteeritud virtuaalvääringutesse või millised kuriteod pannakse toime kasutades ainult virtuaalvääringuid. Seetõttu ei ole võimalik ka operatiivselt infot saada RAB-i tegevuslubadega äriühingute osas, kes on RahaPTS-s sätestatud nõudeid rikkunud või kes on kriminaalmenetlustes kahtlustatavad või süüdistatavad. Samuti ei ole automaatne infovahetus rahvusvaheliste õigusabipalvete osas, milles samuti on palutud Eesti tegevuslubadega äriühingute osas informatsiooni. Eelnimetatud info edastamine peaks riigis olema digitaalseid vahendeid kasutades, mitte käsitöö, et kiirendada saadud info analüüsimist.
- Eestis asutatud ja tegevuslube omavad äriühingud panevad toime pettusi väljaspool Eestit, nende poolt kuritegudega hõlmatud rahad ei liigu läbi Eesti finantssüsteemi, kannatanud ei ole enamuses Eesti isikud. See aga on probleemiks nende äriühingute tegevuse osas kriminaalmenetluste läbiviimises, kuna asjaolu, et kurjategijast äriühing või tema juhatuse liige on Eestist, ei ole piisavaks, et Eestis alustada kriminaalmenetlusi. See piirab võimalust kriminaalmenetluslike vahenditega välja selgitada võimalike Eesti enda kuritegelike gruppide seotust kuritegude toimepanemises, sh rahapesu või rahapesu teenuse pakkumist just läbi Eesti juriidiliste kehade.

Ühisrahastussektor

Rahapesu tõkestamise haavatavus on keskmiselt kõrge, sest esinevad järgmised haavatavused:

- Sektor on siiani olnud suuresti reguleerimata ja järelevalveta. 2021. aastal kavandatakse aga mitmeid valdkonda puudutavaid seadusemuudatusi (hakatakse rakendama EL ühisrahastusmäärust, riigisiseselt on plaanis kehtestada täiendavad investorkaitse nõuded tarbijakrediidipõhistele ühisrahastusteenustele ning annetus- ja auhinnapõhistele ühisrahastusteenustele majandustegevuse registreerimise kohustus).
- Vähesed teadmised kaasatud vahendite päritolust, ühisrahastuse ulatusest ja eesmärgist (sh avalikustamise kohustuste puudumine).

7.4.2. Riskiteadlikkus

<u>Üldine riskiteadlikkus</u>

Virtuaalvääringu sektor

Kuivõrd virtuaalvääringu sektor ja tehnoloogia on kiiresti arenev, on keeruline tagada piisavat riskiteadlikkust ja kõikide riskide maandamine. Kuna virtuaalvääringute regulatsioon on riigiti erinev, puudub riikidel sektorist ka ühesugune ülevaade. Virtuaalvääringu globaalne mõõde teeb raskeks keskse järelevalve teostamise ja korrakaitseorganite uurimise. Riskiteadlikkust ei saa seega eeldada, kuivõrd pädev asutus vajab sisuliseks analüüsiks infot nii tehingute, tehingutes kasutatud vara päritolu, rahakottide kui ka tehingute tegelike kasusaajate osas. Kuna tehinguid tehakse riigipiiride üleselt ja mitmeid erinevates jurisdiktsioonides asuvaid teenusepakkujaid kasutades, on raske kindlaks määrata, kelle jurisdiktsiooni tehtud tehingud kuuluvad ja kuidas tagada vastava informatsiooni kättesaadavus. Haavatavuseks on ka sellised virtuaalvääringu administraatorid, kes

asuvad riikides, kus on ebapiisavad rahapesu ja terrorismi rahastamise tõkestamise seadused. Keerukus seisneb ka virtuaalvääringute edasikandmise piiramises ja kohustatud isikult andmete nõudmises. Lisaks suurendatakse virtuaalvääringu teenuse pakkuja registreeringu olemasoluga teenuse tarbijates usaldusväärsust, mis võimaldab läbi viia pettuseid ja omastada isikute vara.

Suurimaks haavatavuseks võib pidada seadusandluse puudumist või selle ebapiisavust. Samuti puudub hetkel laiem regulatsioon, mis reguleeriks laialdasemalt virtuaalvarasid. RahaPTS-s on esitatud virtuaalvääringu mõiste, mis on uuemate virtuaalvarade kontekstis liiga kitsas, kuivõrd uuemad virtuaalvarad seaduses sätestatud mõiste alla ei liigitu ja seetõttu ei allu ka regulatsioonile. Üha enam on levinud *tokenite* kasutamine, mis virtuaalvääringu mõiste alla ei liigitu. Rahandusministeerium on avalikustanud seaduse eelnõu (ÜMIVS)[77], millega soovitakse reguleerida ka selliseid krüptovarasid ja krüptovara teenuseosutajaid, kes tänase RahaPTS regulatsiooni alla ei kuulu. Eelnõuga kavandatakse nõudeid instrumentidele, mis kannavad endas investeerimise eesmärki või mida seostatakse juriidilises isikus osaluse omamisega või muul moel kontrolli teostamisega teises juriidilises isikus. Eelnõu kohaselt soovitakse kehtestada nõuded ka virtuaalvääringutega kauplemise platvormi korraldamise teenuseosutajatele.

Küsitluse tulemused teadlikkuse osas:
NRA raames läbiviidud küsitluse tulemused näitavad seda, et sektori teadlikkus rahapesu tõkestamisest on pigem tagasihoidlik (vt ka alljärgnevalt väljatoodud aspekte). Lisaks, alla poolte teenuseosutajate ei hinda töötajate usaldusväärsust töösuhte keskel, mistõttu puudub tööandjal teadmine, kas jälgitakse kõiki rahapesu tõkestamise põhimõtteid.

Küsitluse tulemused teatamise statistika osas:
Sektor täidab tagasihoidlikult oma teatamiskohustust. Küsitlusele vastanutest 6% ei olnud või ei osanud öelda, kas ettevõttes on välja töötatud metoodika ja/või juhend rahapesu ja terrorismi rahastamise kahtlusest või ebatavalisest tehingust teatamiseks. Samas on teenusepakkujatel kohustuslik kehtestada metoodika ja juhend, kui tekib rahapesu ja terrorismi rahastamise kahtlus või on tegemist ebatavalise tehingu või asjaoluga, ning teatamiskohustuse täitmise juhend. Samuti selgus küsitlusest, et rohkem kui pooltelt teenusepakkujatel ei ole juhendit praktikas vaja läinud. Arvestades küsitlusele vastanute aastakäivete suurust, on kahtlust tekitav, et sedavõrd suurte käivete juures ei ole ettevõtetel ette tulnud tehinguid või asjaolusid, millest tulnuks RAB teavitada. Eelnev viitab sellele, et teenusepakkujad ei järgi seadusega kehtestatud teatamiskohustust ning jätavad mitmed olulised teated ja kahtlused RAB-le edastamata, mistõttu puudub RAB-l vajalik informatsioon sektoris levivate riskide ja skeemide tuvastamiseks.

Metoodika järgi hindas töörühm haavatavusi seoses virtuaalvääringu teenuseosutajate töötajate teadmistega rahapesu tõkestamisest kõrgeks. Arvestades ka eespool kirjeldatut on üldine riskiteadlikkus sektoris esinevatest riskidest madal.

Ühisrahastussektor
Ühisrahastuse valdkonna riskiteadlikkust võib käesoleval ajal pidada keskmiseks. Teadmiste vähesus võib olla tingitud sektori alareguleeritusest, kuid 2021. hakatakse rakendama EL ühisrahastusmäärust ning tõhustatakse ka riigisisest sektorispetsiifilist õiguskeskkonda. Seoses eelnevaga kehtestatakse ka tõhus investorkaitse, mis muudab ettevõtjate tegevust kindlasti läbipaistvamaks. Arvestades, et valdkond on saanud viimastel aastatel ka meedia tähelepanu, siis ühiskonna teadlikkus sektorist on kindlasti tõusuteel. Sellele aitavad kaasa ka investor-blogijad, kes kirjutavad ühisrahastusega seotud teemadel.

Eestis tegutseb mitmeid ühisrahastusteenuse osutajaid, kes on end vabatahtlikult finantssektoris tavapäraste nõuetega vastavusse viinud ja kes teevad seda muuhulgas eesmärgiga taotleda 2021. või sellele järgnevatel aastatel ühisrahastusteenuse osutamiseks asjaomast tegevusluba. Mitmed neist

[77] Ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu, vt õigusraamistiku alapunktis kirjutatut.

täidavad ka MTÜ FinanceEstonia ühisrahastuse hea tava suunist, mis küsitluse tagasiside kohaselt on olnud teenuseosutajatele abiks[78]. Küsitluse kohaselt on umbes pooltele vastanutest viidatud suunisest kasu olnud. Üle poolte vastanutest on kasulikuks pidanud ka RABi antud suunised. Enamus küsitlusele vastanutest on kehtestanud RahaPTS §-s 14 sätestatud sise-eeskirjad, kuigi seadusest neile sellist kohustust ei tulene. Arvatavasti on tegemist ärikultuurist tuleneva survega (nt surve krediidiasutuste poolt).

Küsitluse tulemused teadlikkuse osas:
NRA raames läbiviidud küsitluse tulemused näitavad seda, et sektori teadlikkus rahapesu tõkestamisest on pigem hea.

Küsitluse tulemused teatamise statistika osas:
71,4% vastanutest on arvamusel, et rahapesu kahtlusest teatamine ei too kaasa negatiivseid tagajärgi teate esitanud töötajale. See on positiivne ja näitab, et ollakse teadlikud ka sellest, kuidas jaotub teatamise korral vastutus ühingu tasandil. Samas on 28,4% vastanutest arvamusel, et rahapesu kahtlusest teatamine võib kaasa tuua negatiivseid tagajärgi ettevõttele. Negatiivsete tagajärgede kartuses võivad ettevõtjad loobuda rahapesu kahtluse teavitamisest, mis võib tõsta sektori haavatavuse taset.

Metoodika järgi hindas töörühm haavatavusi seoses ühisrahastusteenuse osutajate töötajate teadmistega rahapesu tõkestamisest madalaks/keskmiseks. Hinnangu andmisel arvestati ka ankeetküsitluste tulemusi, mille kohaselt enamik vastanutest teevad oma töötajatele asjaomaseid koolitusi, pakuvad veebikursuseid ja tõstavad pidevalt üldist teadlikkust. Eeltoodule tuginedes on üldine riskiteadlikkus ühisrahastussektoris esinevatest riskidest keskmine.

Juhtkonna pühendumine ja juhtroll

Virtuaalvääringu sektor

Küsitluse tulemusena selgus, et riskiteadlikkus on virtuaalvääringute sektoris madal ja vajab tõhustamist. Küsitluse tulemusena ei ole Eesti virtuaalvääringu teenuse pakkujad kokku puutunud välismaiste asutuste sunnimeetmetega, mistõttu Eesti teenusepakkujaid need pigem ei mõjuta. Kuigi RahaPTS § 72 lg 1 p 5 loob virtuaalvääringu teenuse pakkujale arveldus- või maksekonto olemasolu kriteeriumi, siis eelduslikult luuakse maksekonto just välisriigi makseteenusepakkuja juures, mis tõstab teenuse osutajate, skriinimise ja järelevalve riski.

Küsitluse kokkuvõttena võib öelda, et programmi „tunne oma töötajat“ kõikehõlmavus on pigem puudulik ning tööandja ei tunne oma töötajat piisaval määral ja see tekitab kõrge riski. Samuti oleks töötajate skriinimisel abiks KAPO koostööst, kuivõrd kohustatud isikul on vajaliku informatsiooni kättesaamine raskendatud. Kuivõrd veidi alla poolte teenusepakkujate ei hinda töötajate usaldusväärsust töösuhte keskel, siis esineb tööandjal rahapesu tõkestamise põhimõtete jälgitavuse osas teadmatus. Samuti rikuvad praktiliselt kõik küsitlusele vastanud konfidentsiaalsuse nõuet. RAB-l on õigus kontrollida tegevusloa menetluse raames kontaktisikukandidaadi sobivust seaduses sätestatud ülesannete täitmiseks. Järelevalve teostamisel kontrollitakse seda, kas kohustatud isik on teenuste osutamisel järginud seaduses sätestatud nõudeid ja kes RahaPTS-st tulenevate nõuete eest vastutas. Samuti leiab küsitlusele vastanutest ligikaudu 80%, et rahapesu kahtlusest teatamine ei too töötajale negatiivseid tagajärgi ning kuigi osades ettevõtetes on kasutusel erinevad mehhanismid, võib eeldada, et need suures osas siiski puuduvad või esinevad olulised puudused ning neile ei pöörata piisavalt tähelepanu.

Juhtkonna pühendumist ja juhtrolli hinnati metoodika järgi kolmes alapunktis, mille haavatavuse hinnangud olid järgmised:

- turu avaldatava surve tase rahapesu tõkestamise standardite järgimiseks – kõrge;
- sisenemiskontrolli olemasolu ja tõhusus – keskmine/madal;
- töötajate ausameelsus - keskmine.

[78] Seda on kasulikuks pidanud ligikaudu pooled vastanutest.

Ühisrahastussektor
Kuivõrd turuosalised teevad üldjuhul koostööd krediidiasutustega, kohaldavad osad turuosalised RahaPTS-st tulenevaid hoolsusmeetmeid (nn ärikultuuri survel). Ilma krediidi- või makseasutuse koostööta ei oleks võimalik omada kontot, mille kaudu rahasid kaasata. Riskiteadlikust võib hinnata keskmiseks.

Enamus vastanutest (78,6%) viib töötajate värbamisel läbi taustakontrolli. See asjaolu vähendab sektori haavatavust. Taustakontrolli puhul kasutatakse enim avalikke registreid (38,1%), Google ja sotsiaalmeediat (217%) ning soovitusi (19%). Vähesemal määral kontrollitakse karistusregistri väljavõtet (9,5%), suheldakse eelmiste tööandjatega (9,5%), kontrollitakse maksekäitumist (4,8%) ning vaadatakse üle CV-d (4,8%). Nende turuosaliste, kes töötajate usaldusväärsuse hindamist töösuhte kestel teostavad (35,7%), põhimõtted hõlmavad töötaja tegevuse jälgimist ja kontrolli (40%) ning vestlusi töötajaga ja küsimustike täimist (20%).

14,3% vastanutest on kinnitanud, et neil ei ole regulaarset koolituskava ja nad ei tee midagi selleks, et rahapesu tõkestamise eest vastutavad töötajad Eestis oleksid regulaarselt koolitatud. Haavatavus on vähene, kuna enamus turuosalisi teevad selleks koolitusi ja veebikursusi (57,1%) ning tõstavad üldiselt teadlikkust (21,4%).

Ainult 3 vastanu puhul ei ole töötajad viimasel kolmel aastal läbinud rahapesu tõkestamise koolitust. Ülejäänud turuosaliste puhul on koolitusi läbinud 1 kuni 3 töötajat ja kahel juhul kõik töötajad. Koolituste läbimine vähendab haavatavust ja tõstab teadlikkust. 46,7% turuosalistest tagavad koolitustega selle, et töötajad oleksid teadlikud rahapesu tõkestamise alastest kohustustest. Ülejäänud kasutavad muid meetmeid. Samas, 57,2% vastanutest kas ei oska öelda (14,3%) või ei kasuta mingeid meetmeid (42,9%) selleks, et kaitsta rahapesu tõkestamise nõuete täitmisega seotud töötajaid selle tegevusega seotud negatiivsete tagajärgede eest. See näitab, et üle poole vastanutest ei mõtle sellele, kuidas rahapesu tõkestamisega tegelevad töötajad saaksid võimalikult objektiivselt ja turvaliselt rahapesu tõkestamisega tegeleda. Kindlasti näitab eeltoodu haavatavust. Siiski, 71,4% vastanute hinnangul ei too rahapesu kahtlusest teatamine kaasa negatiivseid tagajärgi teate esitanud töötajale. See on positiivne ja näitab seda, et ollakse teadlikud, et teavitamisest ei hoiduta põhjusel, et see võiks töötajat kuidagi kahjustada ehk ollakse teadlikud ka sellest, kuidas jaotub vastutus ühingu tasandil. Haavatavus on eelneva osas väga madal. 28,4% vastanute hinnangul võib rahapesu kahtlusest teatamine kaasa tuua negatiivseid tagajärgi ettevõttele. See näitab aga mõningast haavatavust, kuna negatiivsete tagajärgede võimalikkuse korral ettevõttele võidakse teatamisest pigem hoiduda.

Juhtkonna pühendumist ja juhtrolli hinnati metoodika järgi kolmes alapunktis, mille haavatavuse hinnangud olid järgmised:

- turu avaldatava surve tase rahapesu tõkestamise standardite järgimiseks – keskmine/madal;
- sisenemiskontrolli olemasolu ja tõhusus – keskmine/kõrge;
- töötajate ausameelsus – keskmine.

7.4.3. Õigusraamistik ja kontroll

<u>Üldist</u>
Virtuaalvääringu sektor
Enne 10.03.2020 olid virtuaalvääringu teenuse osutaja tegevusload eristatud kahe teenuse järgi: virtuaalvääringu raha vastu vahetamise teenus ja virtuaalvääringu rahakotiteenus. Alates nimetatud kuupäevast loetakse eelnevalt nimetatud kaks tegevusluba samaväärseks virtuaalvääringu teenuse pakkuja tegevusloaga ehk on üks üldine tegevusluba.

Rahapesu ja terrorismi rahastamise tõkestamise seaduse uus redaktsioon, mis jõustus 10.03.2020, muutis põhjalikult nõudeid, mida riik virtuaalvääringu teenuse pakkujatele esitab. Muudatused hõlmasid mh osakapitali ligi viiekordset kasvu ja nõuet, et ettevõtte tegevus- ja asukoht oleksid Eestis. Muudatuste eesmärgiks oli karmistada virtuaalvääringu teenuse ja rahakotiteenuse pakkujate

tegevusloa saamise tingimusi, et vähendada nende teenustega seotud rahapesu ja terrorismi rahastamise riske.

Karmimad nõuded ei puudutanud ainult uusi ettevõtjaid. Üleminekuperioodi jooksul, mis kestis kuni 01.07.2020, pidid oma tegevuse ja dokumendid viima uues redaktsioonis kehtestatud nõuetega kooskõlla ka kõik juba vastavat tegevusluba omavad teenuseosutajad. Kui ettevõtjad ettenähtud tähtajaks RahaPTS § 118^2 lg-s 1 sätestatut ei täitnud, tunnistas Rahapesu Andmebüroo tegevusloa(d) kehtetuks.

Ettevõtjal tuli tegevusloa kooskõlla viimisel arvestada järgnevaga:

- Ettevõtja asukohaga seotud nõuded: Ettevõtja registrijärgne asukoht, juhatuse asukoht ja tegevuskoht peavad olema Eestis. Kui välisriigi äriühing tegutseb Eestis äriregistrisse kantud filiaali kaudu, peab selle tegevuskoht ja juhataja füüsiline asukoht olema Eestis. Statistika kohaselt on suurem osa tegevusloa saanud ettevõtetest mitteresidendid. See tähendab, et välisriigi ettevõtja peab tegevusloa nõuetega kooskõlla viimiseks asutama Eestis filiaali.
- Osakapitali suuruse nõue: Ettevõtja aktsia- või osakapital peab olema vähemalt 12 000 eurot. Osakapital peab olema täies ulatuses rahaliselt sisse makstud.
- Maksekonto nõue: Ettevõtjal peab olema avatud maksekonto krediidiasutuses, e-raha asutuses või makseasutuses, mis on kas asutatud Eestis või Euroopa Majanduspiirkonna lepinguriigis ja osutab Eestis teenuseid piiriüleselt või tegutseb Eestis filiaali kaudu. Ettevõtja peab tegevusloa uue redaktsiooni nõuetega kooskõlla viimiseks esitama rahapesu andmebüroole kõikide oma nimel peetavate maksekontode loetelu koos iga maksekonto kordumatu tunnuse ja kontopidaja nimega.
- Ettevõtja tausta, sobivust ning korrektset laitmatut mainet kinnitavad tõendid: Ettevõtja peab esitama oma juhtorgani liikme ja prokuristi kohta dokumendid, mis sisaldavad haridustaset, töö- ja ametikohtade täielikku loetelu ning juhtorgani liikme puhul ka vastutusvaldkonda. Kuna analoogne nõue sisaldub ka kehtivas seaduses, on paljud ettevõtjad eelviidatud dokumendid koos tegevusloa taotlusega ilmselt juba esitanud. Seega peaks iga ettevõtja üle kontrollima, millised dokumendid on ta tegevusluba taotledes juba esitanud ning seejärel hindama, milliseid täiendavaid dokumente esitada tuleks, kui üldse. Samuti peab ettevõtja esitama muud dokumendid, mida ta peab oluliseks tõendamaks, et tema juhtorgani liikmel, prokuristil, tegelikul kasusaajal ja omanikul on laitmatu ärialane maine.
- Isikut tõendavad dokumendid ja kriminaalkaristuse puudumist tõendavad dokumendid: Juhul kui ettevõtja, tema juhtorgani liige, prokurist, tegelik kasusaaja või füüsilisest isikust omanik on välisriigi kodanik, siis tuleb rahapesu andmebüroole esitada kõikide kodakondsusjärgsete riikide kohta isikut tõendavate dokumentide koopiad. Samuti tuleb sellisel juhul esitada kõikide kodakondsusjärgsete riikide karistusregistri tõend või pädeva kohtu- või haldusorgani väljastatud samaväärne dokument, mis tõendab karistuse puudumist riigivõimuvastase või rahapesualase süüteo või muu tahtlikult toimepandud kuriteo eest. Tõendi väljastamisest ei tohi olla selle esitamise hetkeks möödunud rohkem kui kolm kuud. Tõend peab olema notariaalselt või sellega võrdsustatud korras kinnitatud ja legaliseeritud või kinnitatud legaliseerimist asendava tunnistusega.
- Virtuaalvääringu teenuse pakkujad on kohustatud kajastama rahapesu ja terrorismi rahastamise tõkestamist käsitlevate õigusaktide asjakohaseid sätteid tegevuspõhimõtetes või -korras. Kuigi 85% vastanutest leiab, et protseduurireegleid on viimase aasta jooksul üle vaadatud, on küsitav, kas seda tehakse kogu aeg, kas sellest lähtutakse enda tegevuses ning kas seda tehakse kooskõlas tuvastatud riskidega ja omakorda RP/TR riskihinnanguga.
- Ettevõtjal on kohustus esitada andmed selle kohta, et tal on olemas teenuse pakkumiseks vajalikud teadmised, oskused, kogemused, haridus, kutsealane sobivus ja laitmatu ärialane maine. Samuti peab ettevõtja kontaktisik töötama alaliselt Eestis (RahaPTS § 17 lg 5). Andmed, mis esitatakse isiku sobivuse kohta, peavad olema ammendavad ja piisavad ning peegeldama adekvaatselt isiku sobivust, mida on õigus RAB-l tegevusloa menetluse raames kontrollida.
- 10.09.2020. a jõustunud RahaPTSi muudatuste kohaselt loetakse virtuaalvääringu teenusepakkujaid finantseerimisasutuseks, mistõttu kohalduvad neile RahaPTS § 31 alusel

kehtestatud nõuded isikusamasuse tuvastamisele ja andmete kontrollimisele infotehnoloogiliste vahendite abil.
- 15.01.2021 avalikustas Rahandusministeerium ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu.

Kuigi virtuaalvääringute õigusraamistikuga seotud haavatavusi on hinnatud keskmiseks/kõrgeks, on Eesti asjaomaseid regulatsioone viimastel aastatel korduvalt tõhustatud ja seadusandja on ka lähitulevikus kavandamas seadusemuudatusi, mis antud valdkonna riske veelgi maandavad.

Ühisrahastussektor

Käesoleval ajal ei ole ühisrahastusteenuse osutajatel ei loa- ega registreerimise kohustust ühisrahastusteenuse osutamiseks, v.a teatud ärimudelite puhul, milleks võib olla vajalik krediidiandja või- krediidivahendaja või investeerimisühingu tegevusluba. FinTech sektori raames küsitletud ühisrahastusteenuse pakkujate arv on 34, kellest enamus (82,4 %) ei ole kohustatud isikud rahapesu ja terrorismi rahastamise tõkestamise seaduse mõttes. 10.11.2020 võeti vastu EL ühisrahastusmäärus, mida hakatakse kohaldama alates 10.11.2021. 2021. aasta jaanuaris avalikustati ka ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu, mille jõustumist kavandatakse 2021. aasta 1. juulil. Viidatud eelnõuga reguleeritakse küsimused, milles EL ühisrahastusmäärus annab õiguse või paneb kohustuse ning täpsustatakse nõudeid EL ühisrahastusmääruse kohaldamisalast väljajäävate ühisrahastusmudelite puhul. Näiteks tarbijakrediiti vahendavad ühisrahastusteenuse osutajad peavad ettepaneku kohaselt edaspidi täitma ka investorkaitse nõudeid, annetus- ja auhinnapõhistele ärimudelitele soovitakse kehtestada majandustegevuse registreerimiskohustus. Lisaks peavad ühisrahastusteenuse osutajad hakkama järgima ka RahaPTS nõudeid.

Ühisrahastuse õigusraamistikuga seotud haavatavusi on hinnatud keskmiseks. Haavatavuse hinnangu andmisel on võetud arvesse muuhulgas seda, et EL ühisrahastusmäärust hakatakse rakendama alates 10.11.2021 ja ka riigisiseselt on kavandamisel teatud muudatused (vt ÜMIVS eelnõu kohta varasemalt kirjutatut). Lisaks järgivad käesoleval ajal mitmed teenuseosutajad sektori hea tava ja täidavad vabatahtlikult ka muid nõudeid.

Järelevalve kvaliteet

Virtuaalvääringu sektor

Kuna järelevalve on siiani olnud väga ühekoeline, st seisnenud üksnes andmepäringutes ja tegevuslubade tühistamises, on üleüldine hoolsuskohustus ja juhtkonna pühendumine rahapesu ja terrorismi rahastamise vastases võitluses madal. Kohapealsete kontrollide arv võrreldes teenuseosutajate arvuga on marginaalne ja pigem ebapiisav. Ka kaugkontrollide arv võiks olla suurem.

Tabel 39. Virtuaalvääringute teenuse tegevuslubade arv ja teostatud kontrollide arv aastatel 2018-2020

Väljastatud tegevusload	**31.12.2018 seisuga**	**31.12.2019 seisuga**	**31.12.2020 seisuga**
Virtuaalvääringu raha vastu vahetamise teenus	553	1188	31
Virtuaalvääringu rahakotiteenus	516	1083	29
Virtuaalvääringu teenus	0	0	419

Kontrollide arv	**2018**	**2019**	**2020**
Kohapealsete kontrollide arv	3	5	7
Kaugkontrollide arv	23	29	5

Virtuaalvääringu teenuseosutajate järelevalvega seotud haavatavusi on hinnatud keskmiseks:

- karistuste olemasolu ja rakendamine – keskmine;
- järelevalvekorra ja -tavade tõhusus – keskmine.

Ühisrahastussektor
Järelevalve kvaliteeti ei saa käesoleval ajal hinnata, kuivõrd puudub regulatiivne kontrollmehhanism ja pädev asutus, mistõttu metoodika kohaselt võib järelevalve kvaliteediga seotud haavatavust pidada kõrgeks. 2021. a on kavandamisel asjaomased õiguskeskkonna muudatused.

Vastavuskontrollisüsteemide ja aruandluse tõhusus

Virtuaalvääringu sektor
Turuosalistel tuleks korrapäraselt hinnata vastavuskontrollisüsteemide piisavust. Küsitluse tulemusena selgus, et 89% kontrollib vastavusprogrammi piisavust, sealhulgas sellest ligikaudu 89% vähemalt kord aastas, ning 30% teostab IT süsteemide auditit. Siiski esineb risk, et teatud hulk teenusepakkujaid ei hinda korrapäraselt süsteemide piisavust. Niisamuti on kaheldav, et kontrollitakse kolmandatest isikutest teenusepakkujate süsteeme või vähemalt tasemel, mida on deklareeritud.

Seiresüsteemide automatiseerimiseks on võimalik kasutada erinevaid IT lahendusi, seda eelkõige suure arvu klientide puhul. Erinevate seiresüsteemide (nii kahtlaste tegevuste kui ka finantssanktsiooni skriinimise) vastustest järeldub, et automaatsete süsteemide kasutamine ei ole kuigivõrd levinud. Vaid 16% vastanutest kasutab automaatsüsteemi kahtlaste tehingute tuvastamiseks ja 10% sanktsioonide nimekirjade vastu skriinimiseks. Kuivõrd tegemist on virtuaalvääringutega, mille tehinguid polegi praktiliselt võimalik automatiseerimata seirata, esineb risk, et suur osa virtuaalvääringu teenuse osutajatest omab oluliste puudustega seiresüsteeme ning jäetakse tuvastamata asjaolud, millest tuleks RABi teavitada.

Virtuaalvääringu teenuse pakkujal tuleb hoolsusmeetmete kohaldamisel määrata ka isiku riskiprofiil, võttes arvesse koostatud riskihinnangut ja seaduses sätestatud asjaolusid. Küsitluse tulemusena selgus, et vaid 40% vastanutest võtab riskitaseme arvutamisel arvesse geograafilist asjaolu ning üksnes 41% turuosalistest on kasutusel kliendi riskiskoor.

RahaPTS kohaselt tuleb virtuaalvääringu teenuse pakkujal sätestada protseduurireeglites juhend, kuidas tulemuslikult kindlaks teha, kas tegemist on riikliku taustaga isikuga ning hoolsusmeetmete kohaldamisel tuleb hankida teavet asjaolu kohta, kas isik on riikliku taustaga isik, tema pereliige või tema lähedaseks kaastöötajaks peetav isik. Seejuures ei ole seaduses sätestatud seire tihedust. Küsitluse tulemusena leiab veerand vastanutest, et ettevõttes kasutatavad allikad riikliku taustaga isikute tuvastamiseks ei ole piisavad ja täiendavad meetmed jäetakse rakendamata.

Küsitluse raames hinnati ka kahtlustäratavast tegevusest teatamise mehhanismide kasutusmugavust. RAB puhul on selleks vastav veebipõhine teatevorm. Ligikaudu 40% küsitlusele vastanutest leiavad, et RAB-le kahtlaste tehingute teavitamise mehhanism ei ole siiski kasutajasõbralik või ei osanud kommenteerida. Sellest tulenevalt on oht, et ettevõtted ei esita teateid, kuna teatevorm tundub neile liiga keeruline või ajamahukas. Samas on väike protsent neid, kes sooviksid teavitamise mehhanismi oma platvormile integreerida.

Virtuaalvääringu teenuseosutajate vastavuskontrolliga seotud haavatavusi on hinnatud kõrgeks:
- vastavuse tagamise süsteemide tõhusus – kõrge;
- kahtlustäratava tegevuse jälgimise ja sellest teatamise tõhusus – kõrge.

Ühisrahastussektor
Vastavuskontrollisüsteemide ja aruandluse tõhusust ei saa hinnata, kuivõrd puudub regulatiivne kohustus. Siiski ei saa väheoluliseks pidada ärikultuuri survet ehk kui on soov koostööd teha mainekate krediidi- ja makseasutustega, siis peavad turuosalisel olema rahapesu ja terrorismi rahastamise tõkestamise sise-eeskirjad ja kontrollmehhanismid kehtestatud.

Positiivne on see, et kõigil vastanutest on määratud vastutav töötaja või töötajad rahapesu ja terrorismi rahastamise tõkestamisega tegelemiseks. Ainult 14,3% vastanutest kinnitasid, et rahapesu tõkestamine on nende ainsaks ülesandeks, ülejäänud (85,7% vastanutest) täidavad vastutava isikuna ka muid ülesandeid. Eeltoodu näitab haavatavust – turuosalised ei ole valmis panustama ja investeerima rahapesu tõkestamisse selleks vajalike inimeste värbamise näol. Kuna rahapesu tõkestamine finantsvaldkonnas on nö hügieenitaseme hoidmine, vähendaks haavatavust suuresti see, et sellega tegelemiseks on määratud konkreetne isik, kes sõltumatult saab rahapesu tõkestamisega tegeleda olles mõjutamata ärilistest otsustest.

Küsitluste tulemusena selgus, et 21,43% ühisrahastusteenuse osutajatest on puutunud kokku olukorraga, mil investor on rahastusallikate kohta keeldunud ettevõttele täiendava info esitamisest ja täheldanud seeläbi tegelike kasusaajate varjamist. 14.29% vastanutest on tuvastanud, et neile on esitatud rahastusprojekte, millel puudub arusaadav majanduslik põhjus. 7.1% vastanutest on tegevuse käigus täheldanud kriminaalse taustaga alustehinguid ja projektiomanike poolt pahatahtlikku käitumist, sooviga toime panna investeerimiskelmust.

Välisriikide järelevalveasutuste survestamismeetmeid seoses rahapesu tõkestamise nõuete rikkumisega ei oska hinnata 64,3% turuosalistest. Eeltoodu näitab, et kokkupuudet ei ole olnud ja seetõttu sektori haavatavus selles osas on väike. Ettevõtte töötajate arusaam kahtlaste tehingute teavitamise kohustusest on 85,7% vastanutest olemas ja heal tasemel, 71,4% vastanutest kinnitavad, et ettevõte hindab vastavuskontrolli piisavust regulaarselt. See on positiivne ja haavatavus puudub. Peaaegu pool vastanutest (42,9%) hindab vastavuskontrolli piisavust tihedamini kui kord aastas ja 28,6% hindab seda kord aastas. See näitab, et turuosalised võtavad rahapesu tõkestamist tõsiselt, mis vähendab ka haavatavust. Küsimustikele vastanud avaldasid, et hindasid viimati vastavuskontrolli piisavust 4-6 kuud tagasi (35,7% vastanutest), 2-3 kuud tagasi (14,3% vastanutest) ning kuu aega või nädal tagasi (mõlemad 7,1% vastanutest).

Pooled (50%) vastanutest kasutavad finantskuritegude tuvastamise süsteemides riskipõhist lähenemist. Ülejäänutel see puudub või ei oska nad seda öelda. Eeltoodu näitab, et turuosalised ei ole riskipõhisest lähenemisest piisavalt teadlikud ning see kindlasti suurendab sektori haavatavust. Finantskuritegude tuvastamise süsteemina kasutatakse enim tehingute ja klientide tegevuse monitoorimist (44,4%).

Kahtlaste tehingute monitoorimise süsteem on olemas 71,5% vastanutest, hõlmates 42,9% ulatuses rahapesu kahtlusega tehingute tuvastamise võimaldamist, 35,7% ulatuses terrorismi rahastamise kahtlusega tehingute tuvastamise võimaldamist ning 64,3% ulatuses finantssantsioonide kahtlusega tehingute tuvastamise võimaldamist. Süsteemi olemasolu vähendab oluliselt sektori haavatavust rahapesu ja terrorismi rahastamise toimepanemisele. Kahtlaste tehingute monitoorimise süsteem hõlmab erinevaid tegevusi, mitte ei piirdu ainult nt taustakontrolli tegemisega. Sh üks turuosalise monitoorimise süsteem on manuaalne ja iga tehingu kohta eraldi. 26,7% vastanutel on olemas automaatkontroll, 33,3% teeb taustakontrolli (sanktsioonide nimekiri, PEP register jne), 13,3% puhul annab süsteem teate kahtlasest tehingust ning 20% jälgivad tehingute piirmäärasid. Toimingute varieeruvus on positiivne ja vähendab haavatavust. Pooltel vastanutest (50%) on tehingute monitoorimise süsteem poolautomaatne.

78,6% vastanutest lähtub monitooringu stsenaariumites kasutatud IT-lahendusega tuvastatud riskidest. See protsent on kõrge ja see on positiivne, et turuosaliselt lähenevad suuresti rahapesu tõkestamisele riskipõhiselt. Mõningane haavatavus seisneb selles, et iga turuosaline ei tea, mis on tema valdkonna riskid ja kuidas monitoorida vastavalt tema ettevõttega seotud riskidele.

Sagedus, millal vaadatakse üle ja korrigeeritakse monitoorimise stsenaariumitega tuvastatud riske, on väga erinev alustades „kogu aeg“ ja lõpetades „kord aastas“. Viimati monitooringu stsenaariumites kasutatavaid riske vaatasid ettevõtted üle enim (21,4%) 2-3 kuud tagasi, kuid vastused on siin ka erinevad ja ühtseid järeldusi teha ei saa.

Ettevõtte ärisuhte tehinguseiresüsteem võimaldab keerukate või ebatavaliste tehingute tuvastamist 50% vastanutest, ülejäänud ei oska öelda või ei võimalda. Ärisuhte seiresüsteem lähtub ebatavaliste tehingute tuvastamisel ka kliendi profiilist 42,9% ettevõtetest, kelle ärisuhte tehinguseiresüsteem võimaldab keerukate tehingute tuvastamist. See on oluline näitaja, et suuremas osas sõltub süsteemi abil ebatavaliste tehingute tuvastamine kliendi profiilist, see võimaldab eristada ebatavalisi tehinguid paremini, kuna kliendi enda profiiliga on ebatavalise tehingu struktuur otseselt seotud. Olenevalt kliendist ei pruugi ebatavaline tehing olla nö ebatavaline. 42,6% ettevõtete ärisuhte seiresüsteemi määratlemise aluseks on summapõhine lähenemine ning kliendi tavapärasest erinev käitumine. Muid määratlemise aluseid on märkinud ainult üks turuosaline. Siit nähtub kõrge haavatavus, kuna ärisuhte seiresüsteem peaks efektiivseks rahapesu tõkestamiseks hõlmama kindlasti muid analüüsitavaid faktoreid, kui ainult summapõhine lähenemine ja kliendi käitumise erisused.

Automaatset kliendi riskitaseme arvutamist võimaldab 42,9% vastanutest. Kliendi automaatset riskitaseme arvutamist võimaldavad süsteemid on turuosaliste seas olnud järgmised: risk arvutatakse andmete põhjal, mis kliendi kohta süsteemis on (2 ettevõtet), KYC süsteem (2 ettevõtet), kasutatakse kolmanda osapoole pakutavat lahendust (1 ettevõte), süsteem võtab arvesse kliendi riski, geograafilise riski ja tehingu riski (1 ettevõte).

Rahapesuvastase programmi tehinguseire automaatsüsteemidele tehakse regulaarselt IT-auditeid üksnes 21,4% vastanutest. Näitab mõneti haavatavust, kuid samas ei tähenda, et selle tõttu protsessid ei töötaks. IT-audit seisneb selles, et seeläbi kontrollitakse riskianalüüsi õigsust.

Riskijuhtimise tehnilistesse lahendustesse investeerib 71,4% turuosalistest. See on positiivne ja vähendab sektori haavatavust. Need investeeringud seisnevad järgnevas: investeeritakse IT lahendustesse (23,1%), võetakse kasutusele turvanõuded (7,8%), kasutatakse automaatset monitoorimissüsteemi (15,4%), kasutatakse tasulisi andmebaase 7,8%), kasutatakse programme ja tarkvara (30,8%), paigaldatakse digitaalse näo- ja dokumendituvastuse süsteem (7,8%). Kõik on väga mõistlikud ja vajalikud investeeringud. Küsitlusest selgus, et kasutatakse mitmesuguseid lahendusi, mis on kindlasti positiivne asjaolu rahapesu tõkestamiseks.

Riikliku taustaga isikute (PEP) tuvastamiseks kasutatakse enim (41,1%) internetis olevaid tasulisi programme/allikaid. Kasutatakse ka PPA veebileheküljel olevaid soovitusi riikliku taustaga isikute otsimiseks, kolmandat osapoolt, veebiotsingut, vestlust kandidaadiga/ankeetküsitlusi ning https://namescan.io/FreePEPCheck.aspx veebilehekülge. 85,7% piisab eeltoodud allikatest PEP-ide tuvastamiseks. Üks vastanutest leiab, et nendest ei piisa PEP-ide tuvastamiseks, sest allikad ei anna kogu infot.

50% turuosalistest ei oska öelda, kas RABile kahtlastest tehingutest teatamise mehhanism on kasutajasõbralik. Üks vastanutest leiab, et see ei ole kasutajasõbralik põhjusel, et see on liiga ajamahukas. Ükski vastanutest pole kokku puutunud nii ületamatute probleemidega, et teade on jäänud esitamata või ei oska seda öelda. Ükski vastanutest pole saanud RABilt tagasisidet kahtlaste teadete kvaliteedi kohta või ei oska seda öelda.
Ühisrahastusteenuse osutajate vastavuskontrolliga seotud haavatavusi on hinnatud keskmiseks/kõrgeks:

- vastavuse tagamise süsteemide tõhusus – keskmine/kõrge;
- kahtlustäratava tegevuse jälgimise ja sellest teatamise tõhusus – keskmine/kõrge.

<u>Kliendi suhtes rakendatavate hoolsusmeetmete raamistiku kvaliteet</u>
Virtuaalvääringu sektor
Küsitluse raames uuriti, kas juurdepääs teabele tegelike kasusaajate kohta on lihtne. 64% vastanutest leiab, et ligipääs on lihtne. Samas on kaks teenusepakkujat välja toonud probleemi, et info on tasuline ning neli teenusepakkujat leiab, et info ei ole usaldusväärne. Samuti võib äriregistri tegelike kasusaajate tasuta ligipääsu mehhanism olla vastuolus RahaPTS § 78 lg-ga 3, kuna kohustatud isikul on õigus pääseda ligi üksnes 10 juriidilise isiku andmetele päevas, muuhulgas ei kontrolli äriregister,

kas tasuta ligipääseja on tõepoolest kohustatud isik, mistõttu vajaks antud süsteem muutmist. Antud aspekti tuleks edaspidi põhjalikumalt analüüsida.

RAB virtuaalvääringu teenuse pakkujate uuringu kohaselt moodustavad eestlased üksnes 0,15% Eesti virtuaalvääringu teenuse pakkujate kliendiportfellist. Kuivõrd eelnev statistika on hinnanguline, võib antud number olla veelgi madalam. Kuivõrd virtuaalvääringud on piiriülesed, ei ole tagatud kõikide klientide osas turvaline riiklik isikutuvastussüsteem riigi väljastatud isikut tõendavate dokumentidega.

RAB kodulehel on esitatud mittetäielik soovitusi riikliku taustaga isikute otsingu teostamiseks.[79] Küsitluse tulemusena leiab vaid 36 teenusepakkujat, et teabele ligipääs riikliku taustaga isikute nimekirjadele on lihtne. Informatsiooni peab kättesaamatuks koguni 9 teenusepakkujat. Eelnev viitab asjaolule, et ettevõtjad ei kontrolli üldse või piisavalt, kas tegemist on riikliku taustaga isikuga.

Küsitluse raames hinnati ka ligipääsu teabele, mis on vajalik välismaiste riikliku taustaga isikute kindlakstegemiseks ja kontrollimiseks. 22 vastanu kohaselt on andmetele ligipääs lihtne ja ligikaudu pooled leiavad, et andmed on küll olemas, kuid ligipääs on keeruline. Eelnevast tulenevalt on risk, et teenusepakkujad jätavad kohased meetmed rakendamata ja välismaised riikliku taustaga isikud tuvastamata.

RahaPTS sätestab suurema riskiga asjaolud ning seaduses sätestatud juhtudel tuleb kohaldada hoolsusmeetmeid tugevdatud korras. Küsitlusele vastanutest 20% ei osanud öelda, milliseid hoolsusmeetmeid kasutatakse kõrgema riskiga juhtumite korral, mis võib viidata asjaolule, et nimetatud hoolsusmeetmed on teenusepakkujatel määramata või ei hinnata piisava hoolsusega klientidega seonduvaid riske. Kui ettevõtja jätab määramata klientidega seotud ja kõrge riskiga kliendid, siis ei ole võimalik ka hoolsusmeetmeid sihtotstarbeliselt rakendada. Selle tulemusel ei ole võimalik ka tehinguid sihtotstarbeliselt seirata, sest ei tunta oma klienti ega tema tegevusala või võimalikke tehingumahte ja/või partnereid. Kõik see aga viib tulemuseni, kus kahtlasi tehinguid ei tuvastata ega teatata RAB-ile.

Kuna olemasoleva ja hinnangulise statistika kohaselt üksnes 0,15% virtuaalvääringu sektori klientidest on eestlased ja 1/3 klientidest kõrgema riskiga kolmandatest riikidest ning ei seadusandja ega järelevalve, va Finantsinspektsioon, kelle järelevalve alla virtuaalvääringute sektor veel ei kuulu, ei ole selgitanud, kuidas praktikas kahe allika isikusamasuse tuvastamise meetodit RahaPTS § 21 lg 4 järgi rakendada, võib asuda seisukohale, et kliendi suhtes rakendatavate hoolsusmeetmete, sh primaarse isikusamasuse tuvastamise tase on madal.

Virtuaalvääringu teenuseosutajate kliendi suhtes rakendatavate hoolsusmeetmetega seotud haavatavusi on hinnatud keskmiseks või kõrgeks:

- kliendi riskitaseme riskipõhist arvutamist võimaldava süsteemi olemasolu – kõrge;
- riikliku taustaga isikute kindlakstegemise tõhusus – keskmine/kõrge.

Ühisrahastussektor

Siin tuleb arvestada, et enamik ühisrahastusteenuse osutajaid ei ole kohustatud isikud RahaPTS mõttes.

Kliendi suhtes rakendatavate hoolsusmeetmete tõhusust ei saa käesoleval ajal hinnata, kuivõrd teenuseosutajatel puudub regulatiivne kohustus. Siiski ei saa väheoluliseks pidada ärikultuuri survet ehk kui on soov koostööd teha mainekate krediidi- ja makseasutustega, siis peavad turuosalisel olema kehtestatud rahapesu ja terrorismi rahastamise tõkestamisega seotud sise-eeskirjad ja paigas vastavad kontrollmehhanismid. 71.4% küsitlusele vastanutest on välja töötatud protsess, kuidas tuvastada tegelikke kasusaajaid.

[79] Vt https://fiu.ee/kasulik-info/kasulik-info.

Vaid 18,8% küsimustikele vastanud ei kasuta meetmeid, et tagada rahapesu tõkestamise eest vastutavate töötajate sõltumatus tööülesannete täitmisel. Ülejäänud, kes töötajate koolitamise eest hoolitsevad, kasutavad mitmesuguseid meetmeid, millest enim kasutatakse koolitusi, süsteemi, et palk ei sõltu tulemustest ning vilepuhumise süsteemi. Haavatavust võib pidada eelneva suhtes väikeseks.

71% vastanutest ei ole osalenud RABi/KAPO koolitustel. See ei tähenda, et koolitustel üldse ei osaleta, kuid viitab, et RABi/KAPO koolitused ei pruugi olla jõudnud turuosalisteni. Üle pooltel vastanutest puudub veendumus, et Eesti äriregistris olev info tegelike kasusaajate kohta on usaldusväärne. Ehk pigem ei usaldata riigi registris olevaid andmeid (mis iseenesest ei ole haavatavus, kuid viitab usaldamatusele). Samuti ei oska üle poole vastanutest kujundada seisukohta, kas kõrge riskiga klientide tuvastamiseks ja kontrollimiseks vajalik info on hõlpsalt kättesaadav (st turuosalised ei oska anda hinnangut).

Ühisrahastusteenuse osutajate kliendi suhtes rakendatavate hoolsusmeetmetega seotud haavatavusi on hinnatud keskmiseks/kõrgeks:

- kliendi riskitaseme riskipõhist arvutamist võimaldava süsteemi olemasolu – keskmine/kõrge;
- riikliku taustaga isikute kindlakstegemise tõhusus – keskmine/kõrge.

7.4.4. Sektoriomaste riskide hindamine sektoripõhiste kontrollide kvaliteediga

Virtuaalvääringu sektor

Kuna ettevõtted tegutsevad rahvusvaheliselt, siis see teeb antud ettevõtete kasutamise rahapesu eesmärgil märkimisväärselt lihtsamaks. Kuna ettevõtetel ei ole igas riigis kontoreid, kus isikuid tuvastatakse (erinevalt pankadest), vaid seda tehakse interneti teel, on märkimisväärselt suurem oht, et luuakse kontosid nn tankistide või varastatud identiteeti kasutades.

Hinnangut andes ei tundu, et ettevõtted peaksid teemat väga oluliseks. Ühelt poolt tundub, et huvi antud teema vastu on madal, samas teavitatakse, et teemaga tegeletakse, aga raporteerida pole midagi (ligikaudu 15% on RABle teateid esitanud). Ligikaudu 50% ettevõtetest peavad nõuete mittetäitmisel sanktsioone liiga karmiks, kuigi teiselt poolt jälle kedagi karistatud ei ole.

Kõigest 16 vastajat teevad enda sõnul töötaja tegevuse jälgimist ja teostavad tegevuse üle kontrolli, mis on taaskord märk sellest, et ühelt poolt ei peeta teemat väga oluliseks, teiselt poolt suureneb risk, et töötajaid on võimalik mõjutada kahtlaseid tehinguid mitte raporteerima. Samas läheb see vastuollu vastusega 45, kus 54 ettevõtet ütleb, et tehingute/ülesannete täitmise üle on kontroll. Samuti ligikaudu 40% ettevõtetest kas ei ole vastanud või ei kasuta meetmeid töötajate sõltumatuse tagamiseks. Huvitav on ka see, et kui ligikaudu 50% ettevõtteid kasutab töötajate teadlikkuse tõstmiseks koolitusi ja virtuaalseid seminare, siis vaid ~10% ettevõtetest testib töötajate teadmisi.

Vaid 40% ettevõtetest kasutavad automaatset kliendi riskitaseme hindamist, millest omakorda väga väike osa võtavad arvesse kliendi digitaalset käitumist.

Pea 40% vastanutest leiavad, et RAB-le kahtlaste tehingute teavitamise mehhanism ei ole kasutajasõbralik või nad ei oska seda öelda. Sellest tulenevalt on oht, et ettevõtted ei tee teateid, kuna see tundub neile liiga keeruline või ajamahukas. Samas jällegi on väike protsent neid, kes sooviksid teavitamise mehhanismi oma platvormile integreerida.

Ettevõtted on valdavalt väikesed, omades kokku 1-5 töötajat ning samal ajal pea 50% ettevõtetest teavitab, et rohkem kui 50% töötajatest on seotud rahapesu ja terrorismi tõkestamisega. Isegi kui numbrid on korrektsed, siis see tähendab, et iga ettevõtte kohta on ligikaudu 1-2 inimest, kes antud teemaga tegeleb ning vastavalt küsimusele 50, ligikaudu 65% täidab ka muid ülesandeid. Arvestades seda, et krüptoraha on väga ahvatlev vahend rahapesu toimepanemiseks, tundub antud ressurss

ebapiisav. Samuti ligikaudu 50% ettevõtetest teavitavad, et neil pole olnud juhtumeid, kus oleks vaja kasutada juhendit, kuidas kahtlastest tehingutest teavitada, mis tundub ebarealistlik, et kõik tehingud on 100% mittekahtlased olnud.

Ligikaudu 50% ettevõttest on osalenud rahapesu ja terrorismi tõkestamise teemaliste ümarlaudadel. Ülejäänuid kas ei ole kaasatud või neil pole olnud huvi osalemiseks. Mõlemal juhul on tegu nõrkusega, mis muudab pooled ettevõtted rohkem vastuvõtlikumaks rahapesule.

30 vastajat on andnud indikatsiooni, et neil ei ole süsteeme, mis suudaks tuvastada mikseritest tulevat raha. Lisaks on 22 vastanud, et nad „ei oska öelda“. Arvestades, et krüptoraha mikserid on tänapäeval üks efektiivsemaid meetodeid raha tegeliku omaniku peitmiseks, näitab see seda, et on üsna suur risk, et selliseid teenuseid hakatakse üha rohkem kasutama raha pesemiseks. Lisaks – sellise süsteemi olemasolu või puudumist on kurjategijatel lihtne ka riskivabalt kontrollida, kuna mikseri kaudu võib kanda oma kontole ka täiesti legaalset raha. Seetõttu antud süsteemi puudumisel on kindlasti kõrgendatud risk sattuda rahapesuahelasse.

Kõigest üheksa vastajat on enda sõnul teinud koostööd õiguskaitseasutustega tumeveebi jälgimisel ja kõigest 15 vastajat on RABi või muud pädevat asutust teavitanud, olgugi et raporteeritud kahtlasi indikaatoreid on märkimisväärselt rohkem olnud – kõigest 29 ettevõtet vastas, et pole „ühtegi eelpoolmainitud juhtumit näinud“. Seega on raporteerimise määr ligikaudu 20%, mis on selgelt madal. Ohuks on siin see, et isegi kui virtuaalvääringute konto peaks suletama, kuid antud info ei jõua õiguskaitseasutusteni, siis valivad kurjategijad lihtsalt järgmise platvormi ja jätkavad oma tegevust. Õiguskaitseasutuste teavitamisel on vähemalt teatud tõenäosus isikud tuvastada.

Ligikaudu 50% ettevõtetest ei ole kasutusele võetud erinevaid mehhanisme (näiteks sanktsioonidest kõrvalehoidmine, terrorismi rahastamine (see küll vaid 25%), radikaalsete liikumiste, kahesuguse kasutusega kaupadega seonduvad rahavood jne), millega saaks märkimisväärselt rahapesu ja terrorismirahastamist paremini tuvastada. Samuti vastasid „ei“ või „ei oska öelda“ ligi 40% ettevõtetest varade külmutamise protseduuri dokumenteerimise kohta.

Sektoriomaste riskide tuvastamise tõhususega seotud haavatavusi on hinnatud keskmiseks/kõrgeks.

Ühisrahastussektor
Sektoripõhiste kontrollide riskide hindamise kvaliteeti ei saa hinnata, kuivõrd puudub regulatiivne kohustus sektori kontrollimiseks. Siiski ei saa väheoluliseks pidada ärikultuuri survet ehk kui on soov koostööd teha mainekate krediidi- ja makseasutustega, siis peavad turuosalisel olema kehtestatud rahapesu ja terrorismi rahastamise tõkestamisega seotud sise-eeskirjad ja paigas vastavad kontrollmehhanismid.

Sektoriomaste riskide tuvastamise tõhususega seotud haavatavusi on hinnatud madalaks.

7.4.6. Varasemate hindamiste käigus tuvastatud riskidele reageerimise kvaliteet

Virtuaalvääringu sektor
2015. aastal avaldatud Eesti rahapesu ja terrorismi rahastamise siseriiklik riskihinnangu eesmärk oli kehtivate rahapesu ja terrorismi rahastamise tõkestamise meetmete ülevaatamine ja täiendamine; selgitada valdkondlikud riskid, mille tulemusena täpsustada asutuste tegevuste prioriteete; riskide kaardistamine; järelevalveasutuste aitamine efektiivsemalt kohaldada riskipõhist järelevalvet; kohustatud isikute mõistmine RahaPTS-ist tulenevate kohustuste hoolsusmeetmete riskipõhisel rakendamisel; MONEYVAL-i edukas läbimine. Teiste finantsteenuste pakkujate, sealhulgas virtuaalvääringu teenuse mooduli eesmärk oli analüüsida toodetest, pakutavatest teenustest ja kliendibaasist tulenevat haavatavust.

Virtuaalvääringutega, mis on kajastatud riskihinnangus kui alternatiivsete maksevahendite teenus, seotud leiud on järgmised: sektori haavatavuse hinnang on skaalal 0–1 keskmiselt madal, haavatavuse määr 0,2. Regulatsioonide taset hinnati kõrgeks, teatamisaktiivsust ja järelevalve piisavust keskmiseks. Riskihinnangus tuuakse välja, et seoses 2008. aastal jõustunud uue RahaPTS regulatsiooniga reguleeriti antud sektor ning sellest tulenevalt kadusid suurimad riskid ja vähenes rahapesijate huvi. Riskihinnangu koostamise hetkel omas alternatiivsete maksevahendite teenuse tegevusluba 16 ettevõtet ning hinnangus on analüüsitud vaid seitse äriühingut. Eelnevast tulenevalt ei saa varasemast riskihinnangu tulemustest lähtuda, kuivõrd teenusepakkujate arv on viimastel aastatel oluliselt suurenenud ning sellega seoses on ka muutunud riskid ja haavatavuse määr. Riskihinnangu tulemusena tehti ettepanek olukorda säilitada ning tõsta esindajate teadlikkust läbi koolituste, et parandada teatamisaktiivsust.

RAB 2018 aastaraamatus esitati peamiste virtuaalvääringu teenuse pakkujatega seotud riskidena:

- pettused ja vara omastamine, kuna tegevusloa olemasoluga suurendatakse usaldusväärsust;
- teistes riikides finantsjärelevalveasutuse lube vajavate teenuste osutamine;
- rahapesu;
- terrorismi rahastamine;
- teenusepakkujate ebapiisavate hoolsusmeetmete rakendamine, mida kasutavad ära kurjategijad ja liigutavad kuritegeliku raha.

Samuti on RAB tegevusloaga teenusepakkujate juures proovinud avada kontosid välisriikide isikud, kellel on terrorismikahtlused. Aastaraamatus leiti, et virtuaalvääringutega kaasnevate riskide maandamiseks ei ole RABi pädevus piisav. RAB tegi ettepanekuid, et muuta regulatsioone rangemaks, sealhulgas loamenetluse tingimusi. Vastavad muudatused RahaPTS-is jõustusid 10.03.2020. Riskide maandamiseks on vaja vastavaid regulatsioone, kus arvestataks ka tehnoloogilise arengu ja teenuseid tarbivate isikute huvide kaitsega. Samuti on riskide mõistmiseks ja ressursi efektiivseks kasutamiseks vaja suurendada strateegilise analüüsi võimekust.

SNRA (2017/2019) leiti antud sektori osas, et Euroopa-üleselt on virtuaalvääringu rahapesu ja terrorismi rahastamise risk kõrge/väga kõrge.[80] Liikmesriikidele tehti ettepanek võtta virtuaalvarade teenuseosutajad kõrgendatud tähelepanu alla. Pädevad asutused peavad virtuaalvara, sh virtuaalvääringu valdkondi monitoorima suure tähelepanelikkusega ja hindama, kas on vajalik muuta siseriikliku regulatsiooni. Eestis on seoses sellega vajalik mainida, et virtuaalvääringu teenuseosutajatega seotud õigusraamistikku on pidevalt tõhustatud ning ka edaspidi on plaanis sektorispetsiifilisi nõuded tõhustada.[81]

Alljärgnevalt on välja toodud Euroopa Komisjoni riigiülese rahapesu ja terrorismi rahastamise riskihinnangu (SNRA) 2017 ja 2019 analüüsis virtuaalvarade, sh –vääringute kohta kirjutatu.

AMLD5 käsitleb virtuaalvääringut[82], mis on kitsam mõiste kui FATFi poolt kasutatav virtuaalvara[83] mõiste. SRNA 2019 käsitleb mõlemat korraga. AMLD5 käsitleb virtuaalvääringu raha vastu vahetamise teenuse pakkujaid ja virtuaalvääringu rahakotiteenuse pakkujaid (ehk välja on jäetud virtuaalvaraga seonduvad teenuse osutajad). Virtuaalvääringute teenusepakkujad on jätkuvalt kõrgendatud tähelepanu all, millele soovitab Euroopa Komisjon pöörata erilist tähelepanu (eelkõige tehingute kiirus ja anonüümsus). Nimetatud valdkonnas on rahapesu ja terrorismi rahastamise risk kasvav (kahtlaste ülekannete arvu kasv virtuaalvara, sh virtuaalvääringuga seonduvalt). Komisjon

[80] Euroopa Komisjoni riigiülese rahapesu ja terrorismi rahastamise riskihinnangu (SNRA) 2017 ja 2019 analüüs.

[81] Ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu, vt õigusraamistiku alapunktis kirjutatut.

[82] *Virtual Currency - A digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically.*

[83] FATF - Virtual Asset - *A digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes, and that does not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.*

viib läbi hindamise, kuidas reguleerida virtuaalvara, sh virtuaalvääringu teenuse pakkujaid korrektselt rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete kohaldamise osas (sh riskide analüüs, koostöö liikmesriikidega jne).

Sektori haavatavust rahapesu osas peetakse SNRA analüüsi kohaselt kõrgeks või väga kõrgeks ning rahapesu ohule viitavad:

1. anonüümsed ja kiired ülekanded (ilma omaniku tuvastamata);
2. interneti kasutamine ehk piiriülene risk, mis võimaldab teha tehinguid kõrge riski piirkonnast või kõrge riskiga klientidega, keda ei ole võimalik tuvastada;
3. detsentraliseeritud teenuse osutamise kanalid (sh sularahaautomaadid);
4. kiiresti arenev tehnoloogia, millega riskiteadlikkusel on raske järgi püsida;
5. rahapesu andmebüroodel puudub ligipääs e-rahakottidele ja vahendite päritolu tuvastamisele;
6. laialdasema regulatsiooni puudumine (mis kataks suuremalt ka virtuaalvara).

Ühisrahastussektor

Tegemist on uue populaarsust koguva sektoriga. Seega varasemas riiklikus riskihinnangus ühisrahastuse sektorit ei käsitletud. Eelmise NRA 2015 raames ei ole antud sektorit hinnatud.

SNRA (2017/2019) leiti antud sektori osas, et Euroopa-üleselt on ühisrahastuse rahapesu ja terrorismi rahastamise risk on keskmiselt kõrge.[84] Kurjategijad võivad platvormide kaudu kaasata vahendeid (kogudes vahendeid legaalselt või kriminaalsetest tegevustest, kasutades anonüümseid tooteid) ja saata need välismaale rahapesu või terrorismi rahastamise eesmärgil. Pigem on ühisrahastussektorit kasutatud siiski kelmusteks (nt komplekssed Ponzi skeemid – kelmused ja võltsprojektid), kui ebaseaduslike vahendite rahapesuks. Liikmesriikidele tehti järgmine ettepanek: kui liikmesriik võtab üle AMLD 4 ja 5, siis peab liikmesriik kaaluma vajadust reguleerimata ühisrahastusplatvormide käsitlemist kui kohustatud isikut AML/CFT regulatsiooni mõttes. Eestis on käesoleval ajal menetlemisel ÜMIVS eelnõu, millega soovitakse reguleerida Eesti ühisrahastussektor. Nimetatud eelnõu kohaselt soovitakse ühisrahastusteenuse osutajad lisada RahaPTSi kohustatud isikuks. EL ühisrahastusmääruse, mida hakatakse rakendama alates 10.11.2021, põhjenduspunkti nr 32 kohaselt hindab Euroopa Komisjon, kas viidatud määruse kohaldamisalas olevad ettevõtjad peaksid olema kohustatud isikud AMLD mõistes (hinnangu läbiviimise ajaraam ei ole teada).

Alljärgnevalt on välja toodud Euroopa Komisjoni riigiülese rahapesu ja terrorismi rahastamise riskihinnangu (SNRA) 2017 ja 2019 analüüsis ühisrahastuse kohta kirjutatu. **Ühisrahastussektori haavatavust rahapesu osas on hinnatud keskmiselt kõrgeks, kusjuures rahapesu ohule viitavad:**

1. Krediidi- ja investeerimispõhise ühisrahastuse korral suuremate summade kaasamise võimalikkus (kõrgem risk kui annetusplatvormidel), kuigi üldjuhul on sellise platvormid reguleeritud (sh avalikustamise nõuded ja krediidiasutuste kasutamine);
2. virtuaalvääringu kasutamine ja anonüümsed kanded;
3. organiseeritud kuritegevuse poolt loodud platvormide risk;
4. vähesed teadmised kaasatud vahendite päritolust, ühisrahastuse ulatusest ja eesmärgist;
5. ühisrahastusteenuse osutajad ei ole üldjuhul kohustatud isikud RahaPTSi mõistes;
6. EL liikmesriikides ei ole kõik ühisrahastuse ärimudelid reguleeritud (osades riikides vaid osad kategooriad);
7. ühisrahastusplatvormid ei tegutse riigis, kus nad on registreeritud;
8. järelevalve puudub.

7.4.7. Järeldus

Virtuaalvääringu sektor

[84] Euroopa Komisjoni riigiülese rahapesu ja terrorismi rahastamise riskihinnangu (SNRA) 2017 ja 2019 analüüs.

Küsitluse ja töörühma arutelude tulemusena on virtuaalvääringu sektori haavatavus rahapesu suhtes kõrge. Virtuaalvääringu sektori haavatavust vähendavad aga järgmised asjaolud:

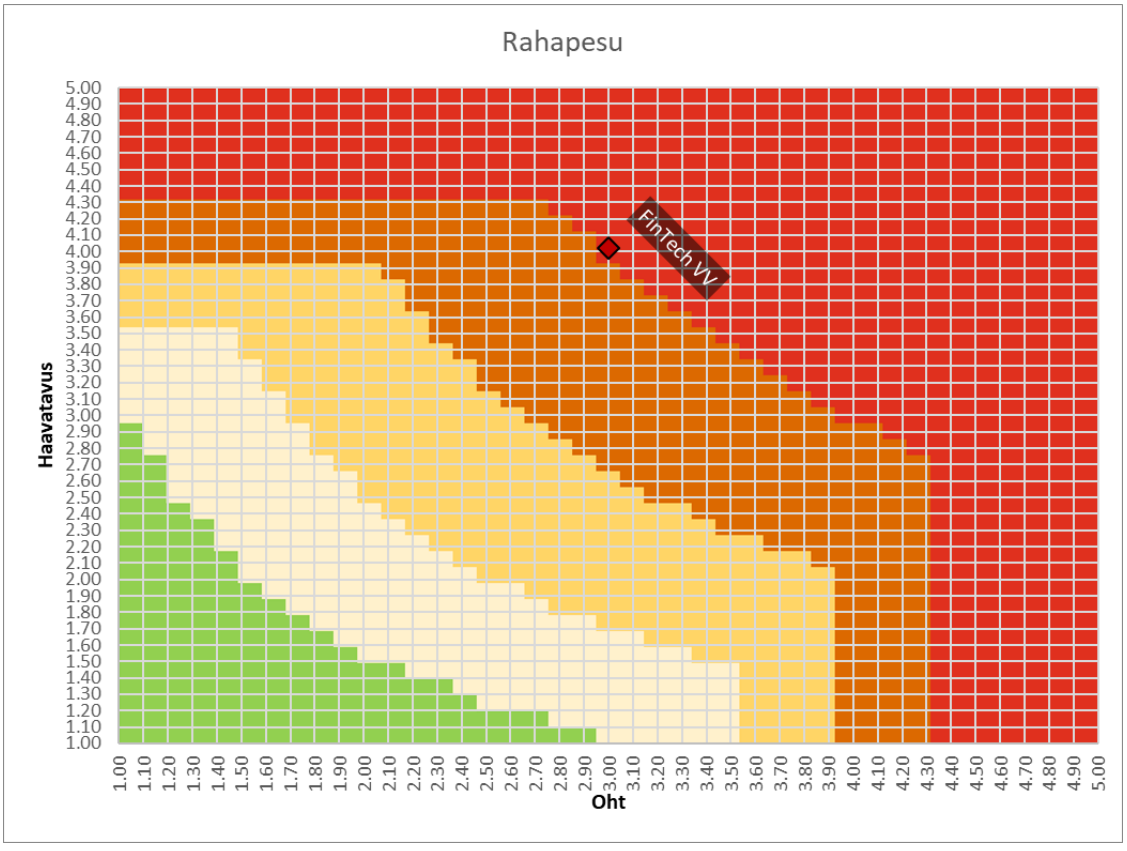
- Alates 10.03.2020 jõustusid RahaPTS-s olulised muudatused, mille tulemusena muutus virtuaalvääringu teenuse pakkujate osas regulatsioon oluliselt rangemaks, sh kehtestati teenusepakkujatele rangemad nõuded, millega tuli vastavat tegevusluba omaval ettevõtjal end vastavusse viia hiljemalt 01.07.2020. Selle tulemusel vähenes teenusepakkujate osakaal Eestis oluliselt.
- Võrreldes mitmete teiste Euroopa Liidu liikmesriikidega on Eesti RahaPTS regulatsioon heal tasemel. Samuti oli Eesti üks esimesi Euroopa riike, kus kehtestati tegevusloakohustus virtuaalvääringu teenuse pakkumiseks.
- Kui ettevõtja ei ole alustanud virtuaalvääringu teenuse osutamisega kuus kuud pärast vastava tegevusloa väljastamist, tunnistab RAB ettevõtja tegevusloa kehtetuks (RahaPTS § 75 p 3).
- Kavandamisel on asjaomane riigisisene regulatsioon.

Samuti tuvastas töörühm virtuaalvääringu sektori haavatavust suurendavad asjaolud, mis on järgmised:

- Kuivõrd muudatused RahaPTS-s jõustusid alles 10.03.2020, on tegemist uue õigusraamistikuga, mistõttu ei pruugi selle toimimise tõhusus vastata eeldatavale tõhususele ning regulatsiooni muudatuste täpsem mõju nähtub tulevikus.
- Kuigi üheks RahaPTS §-d 72 sätestatud kontrollieseme asjaoluks on juhatuse Eestis asumise nõue, on tegemist globaalse valdkonnaga ja osa teenusepakkujaid võib jätkuvalt asuda välismaal.
- Teostatud järelevalvete ja kohapealsete kontrollide maht ei ole vastavuses virtuaalvääringu sektori suurusega. See on põhjustatud järelevalve ebapiisavatest ressurssidest.
  Puudu jääb:
  a) inimestest (RAB-i järelevalve ja tegevuslubade väljastamisega tegeleb kokku 9 inimest. Kohustatud isikuid, kelle olemasolu läbi tegevusloa kohustuse on teada üle 2000, lisaks tingimuste täitumisel järelevalve aluseks saavad isikud ning isikud, kelle osas RAB pole teadlik, et ta vajab tegevusluba),
  b) nende teadlikkuse järjepidevast tõstmisest,
  c) ennetustegevuseks vajaliku info koondamisest ja saadud teadmise edastamisest kohustatud isikutele ja avalikkusele.
- RABile pole antud rahalisi vahendeid, et tõsta oma IT alast võimekust ning teha teatevorm sektori eripära arvestavaks. Samuti pole vahendeid kohaste programmide ostmiseks, et analüüsida saadavat infot efektiivselt ning süvaanalüüsidega välja selgitada õiguskaitseasutustele vajaliku info edastamise vajadus.
- Tegelike kasusaajate info puudulikkus ja selle kontrolli keerukus annab teenuse tarbijatele võimaluse peita või varjata lõpliku kasusaajat ja vara päritolu.
- Eesti virtuaalvääringu teenuse pakkujad on kaasatud rahapesu toimepanemise erinevatesse faasidesse (paigutamine, kihitamine, laotamine). On teada, et Eestis väljastatud tegevuslubadega virtuaalvääringu teenuse äriühinguid kasutatakse (investeerimis)kelmuste toimepanemiseks välismaal, pettuse teel saadud raha konverteerimiseks virtuaalvääringutesse, sularaha ATM-de opereerimiseks ilma kohase isikusamasuse tuvastamiseta. Kõik kasutavad RABi luba kui legitiimsust lisavat asjaolu. Samas ei anna Eestis väljastatud luba õigust tegutseda investeerimisteenuse pakkujana ega ka Eestist väljaspool. Kuni 2020. aasta märtsini polnud võimalik kohaselt kontrollida turule soovijaid. Olemasolevad meetmed vajavad ka pidevat tõhustamist, et olla sektori tehnoloogia arengutega kooskõlas.
- Riigisisene infovahetus õiguskaitseasutuste ja RABi vahel virtuaalvääringutega seotud kuritegude toimepanemises ei toimu automaatselt, vaid konkreetse menetluse raames. Seetõttu pole võimalik üldistada Eestis virtuaalvääringuteenuse pakkujatega seotud toimepandud kuritegevuse või kahtlase tegevuse tehingumustreid, toimimisviise ega seotud isikuid. See vähendab ka RABi võimekust valdkonna ja regiooniga seotud trendide kirjeldamist ning virtuaalvääringu sektorile juhendite koostamist.
- Problemaatiline on Eestis kriminaalmenetlusega hõlmata Eestis asutatud ja tegevuslube omavaid kurjategijatest äriühinguid, kuna enamasti on kannatanud väljaspool Eestit, rahad ei

pruugi liikuda läbi Eesti krediidiasutustes avatud arvelduskontode ning isikud ei tegutse Eestis.

Joonis 8. FinTech VV-de alamsektori rahapesu riskitaseme soojuskaart.



Kokkuvõte

Virtuaalvääringute puhul on rahapesu osas tegemist **kõrge** riskitasemega sektoriga. Sektoris tuleb rakendada hoolsusmeetmeid tugevdatud korras.

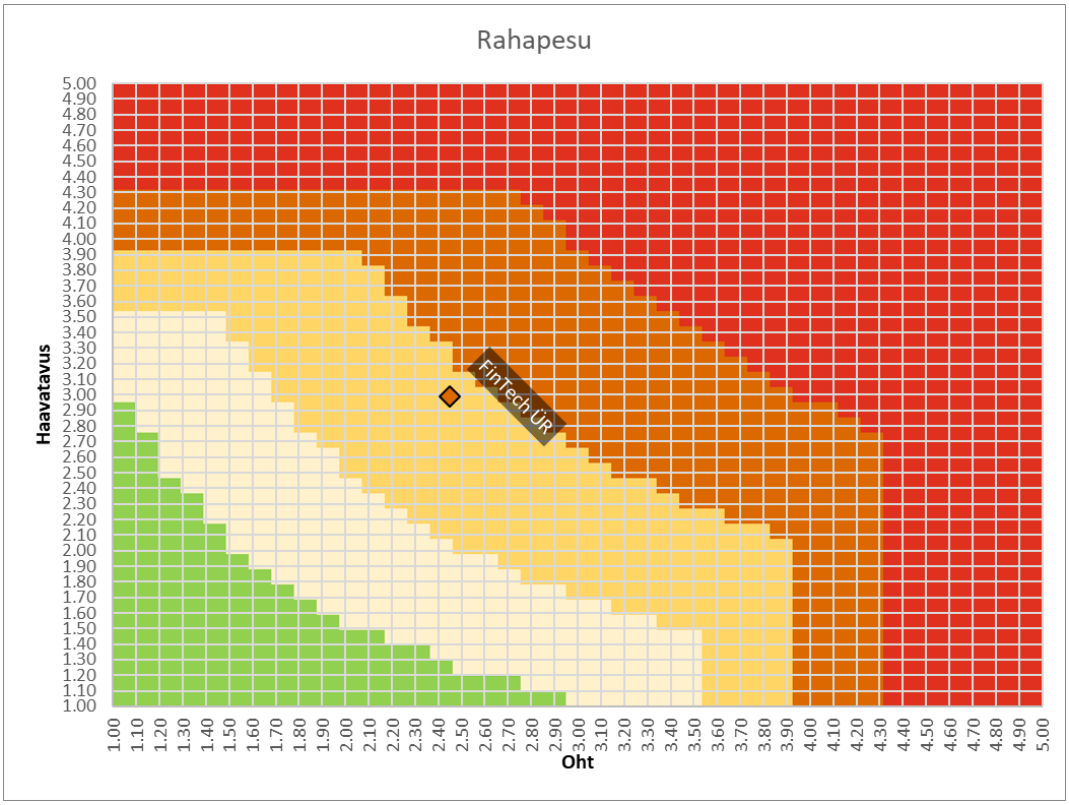
Ühisrahastussektor

Ühisrahastuse sektori haavatavuse hinnang rahapesu aspektist on keskmisest natukene kõrgem.

Sektori tugevamateks külgedeks saab pidada teenuseosutajate iseregulatsiooni, katuseorganisatsiooni olemasolu, hea tava suunise olemasolu ja selle eduka järgimise eest väljaantava tunnustuse „hea tava märgise“ programmi, head kontakti ja suhtlust riigiasutustega ning tahet teha koostööd.

Haavatavamateks kohtadeks on regulatsiooni ja järelevalve puudumine, mis saab aga 2021. aastal lahenduse. Üheks nõrgaks kohaks on peetud juurdepääs rahvusvaheliselt tegelike kasusaajate ja PEP-de teabele, lisaks on välja toodud ka äriregistris sisalduva teabe õigsuse ja ajakohasuse osas. Antud aspekt vajab lahendamist riiklikul tasandil.

Joonis 9. FinTech ÜR-de alamsektori rahapesu riskitaseme soojuskaart.



<u>Kokkuvõte</u>
Ühisrahastuse puhul on tegemist rahapesu osas pigem **keskmise** riskitasemega sektoriga. Sektoris tuleb rakendada hoolsusmeetmeid tavapärases korras.

7.4.8. Riskimaandamisstrateegia

7.4.8.1. Leevendavad meetmed riiklikul tasandil

Virtuaalvääringu sektor

Olukorra parandamiseks tehakse riiklikul tasandil järgmised ettepanekud:

- Rakendada virtuaalvääringute sektoris tugevdatud hoolsusmeetmeid.
- Kuigi 5. AML direktiivi sätteid võib pidada esimeseks sammuks, et reguleerida virtuaalvääringu rahakotiteenuse ja raha vastu vahetamise teenuseid, siis nende instrumentide üha tõusev kasutus tekitab kõrgemat riski ja vajalikud võivad olla edasised regulatiivsed abinõud. Finantssektoris on üldiste ettepanekutena liikmesriikidele välja toodud ka järelevalve seisukohalt soovitus teha jätkuvalt kohapealseid kontrolle vastavalt identifitseeritud riskidele, muuhulgas peaksid need kontrollid keskenduma konkreetsele tootele või teenusele omastele nõrkustele.
- Rahvusvahelise koostöö parandamine järelevalve osas, kuna virtuaalvääringu vahetusteenuse pakkujad ei ole üldjuhul tegevad ainult ühes riigis.
- Äärmiselt oluline on ühtlustada virtuaalvääringute teenusepakkujatele kohalduv õigusraamistik, vähemalt ELi tasemel, et kohustatud isikutel oleks tagatud võrdne konkurents, et riskid ELi üleselt oleksid maandatud proportsionaalselt ning klientidel ei oleks võimalik nii lihtsa vaevaga eirata kohustatud isiku hoolsusmeetmeid, luues hoolsusmeetmete rakendamisel koheselt uus konto teise teenusepakkuja juures.
- Üheks leevendavaks meetmeks riiklikul tasandil on suurendada pädeva asutuse (RABi ja/või Finantsinspektsiooni)[85] ressurssi järelevalve teostamiseks, kuivõrd teostatud järelevalvete ja kohapealsete kontrollide maht ei ole praegu vastavuses virtuaalvääringu sektori suurusega, lisaks avaldada rohkem juhendmaterjale ning tagada infovahetus ja regulaarne suhtlus turuosalistega.
- Samuti tuleb virtuaalvääringu teenuse pakkujate osas tõhustada teenusepakkuja tegevusnõudeid ja kehtestada aruandluskohustus. Täpne statistika annab tulevikus parema ülevaate sektorist ning selle pinnalt on võimalik teha kaalutletumaid poliitikaotsuseid ja hinnata tõhusamalt teenuseosutamisega seotud riske. Aruandluskohustuse osas nähakse tulevikus vajadust virtuaalvääringute teenuseosutajat kohustada küsima kliendilt täiendavaid isikuandmeid, nt ees- ja perekonnanimi või –nimed; sünniaeg ja -koht; kodakondsus või kodakondsused; sugu; isikut tõendava dokumendi number ja dokumendi koopia; telefoninumber ja e-posti aadress.
- RAB poolne koolitus sektorile miksertehingute tuvastamiseks ning vajalike meetodite ja lahenduste kasutuselevõtuks.
- RAB tagasisidest virtuaalvääringu teenuse pakkujatele selgus, et teateid esitas 2019. aastal RABle alla 5% ettevõtjatest[86]. See võib viidata sellele, et järelevalve asutuse poolt rakendatavad meetmed teadete esitamise kohustuse täitmata jätmise korral ei ole tõhusad, seega oleks antud aspekti vaja edaspidi põhjalikumalt analüüsida (ehk viia läbi teadete esitamisega seonduv põhjalik analüüs/järelevalve). Leevendavaks meetmeks riiklikul tasandil võiks olla haldustrahvimenetluse kehtestamine.
- Esitatud teadetest saadava informatsiooni põhjal on RABl võimalik saada ülevaade sektoris valitsevatest riskidest ja mõista haavatavusi. Sellest tulenevalt on üks leevendav meede muuta RABi veebipõhist teatevormi virtuaalvääringu teenuse pakkujate valdkonnale sobivamaks. Selleks on võimalik kasutada turuosaliste sisendit, milliseid andmeid nähakse olevat vajalikud teatevormile lisamiseks, et muuta teate esitamine võimalikult mugavaks ja vältida olukorda, kus teatevormi keerukuse tõttu teenusepakkuja teate esitamata jätab.
- Tagasidestada raporteid esitavatele sektoritele kahtlaste teadetega seonduvat.
- Rahapesu andmebüroo avaldas 2020. aasta septembris virtuaalvääringu teenuse pakkujate uuringu tulemused, milleks viidi 2019. aasta lõpus läbi ankeetküsitlus kõigi ettevõtjate hulgas, kellele oli majandustegevuse registri andmetel väljastatud tegevusluba virtuaalvääringu raha vastu vahetamise teenuse ja/või virtuaalvääringu rahakotiteenuse osutamiseks enne 30.06.2019. Uuringus anti ülevaade ka tehingute käibe ja kliendibaasi

[85] Pädev asutus või pädevuste jaotus võib tulevikus muutuda. Vt ka Euroopa Parlamendi ja nõukogu määruse ettepanekut, mis käsitleb krüptovaraturge, kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52020PC0593&from=EN.

[86] RABi info põhjal suurenes teateid esitanud ettevõtjate arv 2020. aastal ligikaudu kolm korda.

kohta. Selleks, et teha sektori kohta ka edaspidi adekvaatseid järeldusi ja tuvastada kaasnevaid riske, tuleks andmeid turu mahtude ja käibe kohta avaldada regulaarselt. Samuti toob RAB uuringus välja, et teenusepakkujatele tuleks kehtestada aruandluskohustus tehingute, klientide ja mahtude osas, mis annaks tervikliku ülevaate sektorist.

- Virtuaalvääringu teenusepakkujatele vastavuskontrolli funktsiooni (ingl *Money-Laundering Reporting Officer,* MLRO) loomise või asjaomase positsiooni määramise kohustus, sh temalt nõutav sobivus (ingl *fit&proper),* langetaks kogu sektori, turuosaliste kui ka nende kliendiportfelli riski kui ka tõstavad juhtkonna teadlikkust ja pühendumust, mille tagajärjel võiks oodata vastavuskontrollisüsteemidesse tehtavate investeeringute ja hoolsusmeetmete raamistiku kvaliteedi kasvu.
- Tuleb pidada registrit või andmevahetuskeskkonda, kus on korrektne ja ajakohane informatsioon tegelike kasusaajate kohta. Samuti peab olema järelevalvel või muul õiguskaitseasutusel ligipääs antud infole. Ettevõtetel ja aktsionäridel peab olema ülevaade, kes on nende lõplikud kasusaajad ja see info peab olema väljastatav igal ajahetkel õiguskaitse- või järelevalveasutustele.
- Tuleb kasutada juba olemasolevat informatsiooni (s.o finantsandmed, äri-, kinnisvara-, kinnistu- jmt registrid, maksuinfo, börsiinfo jne) andmete rikastamiseks.
- Ettevõtte registreerimisel tuleb luua ka maksekonto. Sellest tulenevalt tekib automaatselt ka isik, kes antud kontole ligi pääseb ja seda informatsiooni saab kasutada ühe allikana tegelike kasusaajate hindamisel.
- Defineerida tuleks indikaatorid, mille kaudu oleks võimalik tuvastada riskiettevõtteid. Selle pinnalt oleks võimalik luua nt „punaste lipukeste“ süsteemid, mis suudavad automaatselt tuvastada ettevõtteid, mille käitumine on anomaalne. Seejärel saab juba rakendada käsitsi kontrolli.
- Koostööd järelevalve ja õiguskaitseasutuste vahel tuleks tõhustada.
- RABi poolset sekkumist ja järelevalvet tuleb tõhustada. Rohkem tuleb teostada ka kohapealseid kontrolle. Seetõttu tuleks RABile ette näha täiendavad ressursid. Euroopa Komisjon rõhutab 2017. aasta riskihinnangus ka kohapealsete järelevalvekontrollide arvu tõstmise vajadust. Riskihinnangu kohaselt peavad järelevalveasutused kehtestama finantssektoris riskipõhise järelevalve mudeli (*risk-based supervision model*).[87] Euroopa järelevalveasutuste (*European Supervisory Authorities, ESA*) juhendi[88] kohaselt peaksid järelevalveasutused nii perioodiliselt kui ka *ad hoc* kontrollima, kas nende riskipõhine järelevalve mudel annab soovitud tulemuse ja kas järelevalveks eraldatud ressursside tase on proportsionaalne tuvastatud rahapesu ja terrorismi rahastamise riskidega. Seetõttu on Komisjoni hinnangul oluline, et järelevalveasutused viiksid läbi piisavaid kohapealseid järelevalvekontrolle, mis oleksid proportsionaalsed tuvastatud rahapesu ja terrorismi rahastamise riskidega.[89] Virtuaalvääringu sektoris läbiviidud kohapealsete kontrollide arv võrreldes teenuseosutajate arvuga on marginaalne.
- Koostööd järelevalve või õiguskaitseasutuse ja teenusepakkuja vahel tuleks parendada. 2017. a Komisjoni riskihinnangu kohaselt peaksid pädevad asutused ja kohustatud isikud tegema regulaarselt koostööd, mis peaks aitama lihtsamalt tuvastada kahtlaseid tehinguid. Järelevalveasutused peaksid esitama selged juhised rahapesu ja terrorismi rahastamise tõkestamisega seonduvate riskide ning hoolsusmeetmete kohta, aga ka selle kohta, kuidas tuvastada kõige olulisemad rahapesule ja terrorismi rahastamisele viitavad indikaatorid.[90] Ka 2019. a riskihinnangus kutsub Komisjon liikmesriike üles tõhustama pädevate asutuste ja kohustatud isikute vahelist koostööd.[91]

[87] Komisjoni 2017. a riskihinnang, lk 17.
[88] Joint Guidelines on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis (07.04.2017). Kättesaadav:https://esas-joint-committee.europa.eu/Publications/Guidelines/Joint%20Guidelines%20on%20risk-based%20supervision_EN%20(ESAs%202016%2072).pdf.
[89] Komisjoni 2017. a riskihinnang, lk 17–18.
[90] Komisjoni 2017. a riskihinnang, lk 19.
[91] Komisjoni 2019. a riskihinnang, lk 17.

- Kehtestatud peaksid olema selged vastumeetmed illegaalsele tegevusele. Kriminaalmenetlusega seotud küsimused, nt tõendite saamine ja hankimine, peaksid olema selgesti reguleeritud. Samuti on vaja tagada, et õigusaktides oleksid olemas asjaomased menetluslikud alused. Vajadusel tuleb läbi viia õiguslik analüüs.
- Krüptovara konfiskeerimise ja arestimise küsimused tuleks ametkondlikul tasemel läbi arutada ja kavandada asjaomased õiguslikud meetmed. Peaks olema üheselt selge, millal tuleb krüptovara vahetada fiat rahaks või millal jätta see krüptorahas hoiule. Läbi tuleb mõelda ka olukorrad, mis teha juhul, kui arestitud vara asub digitaalses keskkonnas, mis kohtumenetluse jooksul suletakse.
- Koolitused ametnikele ja regulaatoritele (nii rahapesu kui ka terrorismi rahastamise tõkestamise alased).
- Riik peaks panustama rohkem ka turuosaliste koolitamisele.
- Virtuaalvääringu teenuse pakkujate ettepanekute kohaselt tuleks rahapesu ja terrorismi rahastamise riskide tuvastamise parandamiseks eelkõige koostada selgemad ja konkreetsemad juhendmaterjalid tegevusvaldkondade lõikes ning korraldada tuleks tihedamalt rahapesualaseid praktilisi koolitusi. Selleks, et parandada Eesti õigusaktide ja rahvusvaheliste standardite täitmist, tuleb teenusepakkujate sõnul eelkõige tõsta ühiskonna teadlikkust näiteks koolituste näol, tagada selgemad nõuded ja juhised ning ametlikud, usaldusväärsed ja tasuta andmebaasid taustakontrolli teostamiseks. Mõlema teema ettepanekutest selgus eelkõige koolituste olulisus, mida võiks olla turuosalistele rohkem ning millega oleks võimalik maandada riske turuosaliste teadlikkuse osas.
- Äriregistriga seotud problemaatika.
  Risk võib väljenduda asjaolus, et registri andmed on tasulised, va kasusaaja andmed minimaalses ulatuses. Kuna tegemist on juba olemuselt piiriüleste teenustega, siis ei ole praktiline ega eelarveliselt mõistlik omandada ligipääs kõikidele EL äriregistritele, eeskätt olukorras, kus kohustatud isik pakub teenuseid üksnes füüsilistele isikutele.

  Olukorras, kus registri andmed, eeskätt ajaloolised juhatuse liikmete andmed ning nii ajakohased kui ka ajaloolised omanike andmed, oleksid tasuta kättesaadavad kõikidele kohustatud isikutele, oleks hoolsusmeetmete kohaldamine turuosaliste jaoks märkimisväärselt lihtsam ja odavam ja tooks kaasa järgmised positiivsed mõjud:
  - Äriregistri korrastamine tagab parema hoolsusmeetmete rakendamise kvaliteedi ja on otseses kooskõlas riskipõhise lähenemisega, kuna aitab kohustatud isikul säästa aega ja ressursse, et tegeleda tegelike riskide maandamisega, st kliendisuhetega, mille puhul pakutakse teenuseid mitteresidentidele, eriti nt Vahemere saartel. Väheneb aeganõudev otsekontakt Eesti klientidega.
  - See omab positiivset mõju ka olukordades, kus hoolsusmeetmeid kohaldatakse kliendiga otsekontaktis. Erinevalt pangandussektorist, kus tõhustatud taustakontrolli (EDD-de) laine käis läbi 2017. aastal, siis EL fintech sektoris ei ole see veel niivõrd tavapärane, eriti kliendi vaatest ja arvestades mh asjaolu, et fintech sektor on äärmiselt konkurentsitihe ja teenuseosutajaid palju. Erinevalt pangandussektorist, kus isikul võib ühe teenusepakkuja juures olla nii arvelduskonto, otsekorraldused, elukindlustus, kasko kui ka kodulaen, siis fintech teenuseid on reeglina kontsentreerunud ehk et teenusepakkuja vahetamine on äärmiselt lihtne. Seega, kui klient tunnetab, et ühe fintech-i hoolsusmeetmed on liiga nõudlikud ja kliendi jaoks ajakulukad, vahetab ta meeleldi teenusepakkujat, mistõttu jääb kohustatud isik ilma nii kliendist kui ka saab juurde täiendavaid kohustusi RahaPTS § 42 ja § 44 järgi.
  - Lisaks aitab eelnev kaasa kohustatud isiku turuvalikul, nimelt kui kohustatud isik leiab, et sarnaseid mahte on võimalik saavutada ka Eesti turul, siis vähenevad ka piiriülesusega kaasnevad riskid. Kokkuvõttes leiame, et nii fintech sektori, kui ka finantssektori riske tervikuna, võiks maandada äriregistri andmete tasuta kättesaadavus. Juhul, kui see on riigi jaoks siiski liiga kulukas, võiks olla andmete kättesaadavus tagatud kuni teatud kriteeriumite täitumiseni, nt X käive, X tulu või järelevalveorgan.

Enne järgmist riskihindamist tuleks teostada analüüs finantstehnoloogia sektori kohta, sh tuvastada, milliseid teenuseosutajaid tuleks täiendavalt finantstehnoloogia sektori all hinnata. Vastavalt sellele tuleks kujundada ka riskihindamise metoodika.

Ühisrahastussektor

- Ühisrahastussektor vajab reguleerimist ja järelevalve kehtestamist (asjaomane eelnõu on 2021. a menetlemisel).
- Annetus- ja auhinnapõhistele ühisrahastusmudelitele tuleks sisse seada tegevuse registreerimise kohustus majandustegevuse registris. See on vajalik, et valdkonnas tegutsevatest teenuseosutajatest oleks tervikpilt ja sektoriga seotud riskide hindamine edaspidi sujuvam.
- Ühisrahastusteenuse osutajad vajavad täiendavaid meetmeid oma teadlikkuse suurendamiseks riskidest ja sisemistest kaitsemeetmetest oma teenuste väärkasutamise vastu.[92] Seetõttu võiksid järelevalve asutused koostada suuniseid või korraldada arutelusid/koolitusi (sh nt hoolsusmeetmete kohaldamine, riskide hindamine ja praktilised näited metodoloogiast, mida tänapäeval kasutatakse).
- Üldise teadlikkuse tõstmine. Ühisrahastusplatvormide kaudu raha paigutajatel ehk investoritel tuleks enne investeeringu tegemist kontrollida teenuseosutajat/platvormi, asjaomaseid majandusnäitajaid, teenuseosutaja omanike/juhtkonna usaldusväärsust, sh varasemaid projekte. Arvestada tuleb, et kuna ühisrahastusteenuse osutajad ei kuulu praegu finantsjärelevalve alla, ei kehti neile nõuded teenuse osutaja kutseoskuse ja lojaalsuskohustuste kohta.[93]

7.2.8.2. Leevendavad meetmed kohustatud isikute tasandil

Virtuaalvääringu sektor

- Läbiviidud küsitluse tulemusena selgus, et 99 virtuaalvääringu teenuse pakkujast on RAB poolt korraldatud koolitusel osalenud vaid 35%. Kuivõrd viimane koolitus virtuaalvääringu teenuse pakkujatele toimus 2019. aasta sügisel ja oli suunatud algajatele, tuleks suurendada RAB poolt läbiviidatavate koolituste arvu antud sektoris, kusjuures koolitused peaksid olema nii teenuseosutamisega alustavatele ettevõtjatele kui ka juba tegutsevatele. Selleks on vaja tagada pädevale asutusele vastavad rahalised ja inimressursid ning aeg asjaomase personali koolitamiseks. Täiendõppe kursusi korraldab ka Tartu Ülikool ning kursused on populaarsed virtuaalvääringu teenuse pakkujate hulgas.
- Kohustatud isikuid on erialaliitude näol kaasatud RahaPTS muutmisesse. Leitakse aga, et sektorit kaasatakse aruteludesse ja seadusloomesse liiga vähe. Kuivõrd tegemist on uue ja madalamahulise valdkonnaga Eesti finantssektoris, on turuosaliste mõjuvõim madal. Sellest tulenevalt tuleks kaasata kohustatud isikuid aruteludesse ja regulatsiooni muutmisesse rohkem ning tõhustada RABi ja turuosaliste infovahetust. Ka kohustatud isikutel on võimalik RABle esitada ettepanekuid muudatuste tegemiseks või juhtida tähelepanu riskidele, tekkinud probleemidele ning kuidas saab RAB seda muuta või parendada.
- Koostööd turuosaliste ja järelevalve vahel tuleks tõhustada. Turuosalised on avatud suhtlusele järelevalvega ning ootavad, et „järelevalvelisest“ suhtest kasvaks välja koostöö, kus mõlemad pooled on teabe vahetamisel avatud ja mis põhineks konstruktiivsel teineteise harimisel.
- Virtuaalvääringu teenuse pakkujate ettepanekute kohaselt tuleks rahapesu ja terrorismi rahastamise riskide tuvastamise parandamiseks suurendada kontrolli klientide/tehingupartnerite suhtes ja kasutada automaatkontrolli. Selleks, et parandada Eesti

[92] Allikas: https://www.acamstoday.org/new-technologies-the-emerging-terrorist-financing-risk/.
[93] Eesti finantstehnoloogia sektori haavatavused, dokumendianalüüs.

õigusaktide ja rahvusvaheliste standardite täitmist, tuleb teenusepakkujate sõnul eelkõige tõsta ühiskonna teadlikkust näiteks koolituste näol, tagada selgemad nõuded ja juhised ning ametlikud, usaldusväärsed ja tasuta andmebaasid taustakontrolli teostamiseks. Mõlema teema ettepanekutest selgus eelkõige koolituste olulisus, mida võiks olla turuosalistele rohkem ning millega oleks võimalik maandada riske turuosaliste teadlikkuse osas.

Ühisrahastussektor

- MTÜ FinanceEstonia koondab Eestis ühisrahastusettevõtjaid, keda on viimastel andmetel 5. Arvestades, et valdkonnas tegutsevaid ettevõtjaid on aga oluliselt rohkem, võiksid ka ülejäänud nimetatud katuseorganisatsiooniga liituda. Selle kaudu on võimalik tõsta (sh koolitused) turuosaliste teadlikust ja teadmisi seoses terrorismi rahastamise riskidega ja asjaomaste hoolsusmeetmete kohaldamisega.
- Ühisrahastusteenuse osutajad vajavad täiendavaid meetmeid oma teadlikkuse suurendamiseks riskidest ja sisemistest kaitsemeetmetest oma teenuste väärkasutamise vastu ning vaja on täpsemat reguleerimist.[94]
- Ühisrahastusteenuse osutajad peaksid pöörama erilist tähelepanu jurisdiktsioonidele, mis teadaolevalt rahastavad või toetavad terroriakte või kus teatakse, et tegutsevad terroriakte sooritavad rühmad, ning jurisdiktsioonidele, mille suhtes kehtivad rahalised sanktsioonid, embargo või meetmed (välja andnud näiteks EL või ÜRO), mis on seotud terrorismi, terrorismi rahastamise või leviku tõkestamisega.
-

7.5. Terrorismi rahastamise tõkestamise haavatavused

7.5.1. Kokkupuude ohuga

Käesoleva riskihinnangu raames hinnati[95] finantstehnoloogia sektori **terrorismi rahastamise haavatavuse taset** järgmiselt:

Tabel 40. Finantstehnoloogia alamsektorite terrorismi rahastamise haavatavuse tasemed

Finantstehnoloogia sektor	**Terrorismi rahastamise haavatavuse tase sektori tasandil**	
Virtuaalvääringud	**2,88**	keskmine
Ühisrahastus	**2,09**	keskmine/madal

Virtuaalvääringu sektor

- Kuigi virtuaalvääringute päritolu ja sihtriigi tuvastamine on märkimisväärselt lihtsam kui fiat valuutade, eriti sularaha puhul, on sektori risk siiski kõrge.
- Kohustatud isikute kliendiportfell – riskihinnangu raames läbi viidud küsitluse kohaselt veidi alla 10% virtuaalvääringu teenusepakkujate klientidest on pärit Venezuelast, ligikaudu 5% isikutest on pärit nii Venemaalt kui ka Indoneesiast ning üle 2% isikutest on pärit Iraanist, Indiast jm. Kõrge riskiga kolmandate riikide risk ei hõlma üksnes kliente, mis moodustab kogu kliendi portfellist 1/3, vaid ka ettevõtete omanikke ja väljendub ka asjaolus, et suur osa tegevusluba omavatest ettevõtetest ei oma Eestiga seost.

Ühisrahastussektor

- Ühisrahastust peetakse populaarsust koguvaks terrorismi rahastamise meetodiks (eriti kui võimaldatakse kasutada ka virtuaalvääringuid). Praktikas puuduvad seni kaasused, kus oleks tuvastatud, et Eesti ühisrahastuse sektorit on kasutatud terrorismi rahastamiseks.

[94] Allikas: https://www.acamstoday.org/new-technologies-the-emerging-terrorist-financing-risk/.
[95] NRA ohtude töörühma poolt antud hinnangud, mis põhinevad riskihinnangu läbiviimise metoodikal.

- Terrorismi rahastamise haavatavus on keskmiselt kõrge, sest esinevad järgmised haavatavused:

- Eestis on sektor suuresti reguleerimata, kuid asjaomane eelnõu on 2021. a menetlemisel. EL ühisrahastuse määrust jõustus 10.11.2020 ja seda hakatakse rakendama alates 10.11.2021. Regulatsiooni senise ebapiisavusega on seotud ka järgmised probleemkohad, mis aga 2021. a lõpuks peaksid olema lahendatud tänu uutele sektorispetsiifilistele õigusaktidele.
  - ✓ Eestis registreeritud ühisrahastusplatvormid faktiliselt ei pruugi tegutseda Eestis, kus nad on registreeritud;
  - ✓ puudub riiklik järelevalve;
  - ✓ puudub kohustus täita RahaPTSist tulenevaid nõudeid.
- Virtuaalvääringu kasutamise võimalikkus.
- Võimalik variisikute kasutamine kurjategijate poolt.
- Eestis puudus senini riiklik ühisrahastuse riskihinnang (olemas alates 2021. a).

- Ohuga kokkupuuteks on peamiselt väikese summad ja vahendite kogumine märksõnadega, mis viitavad pigem annetustele või muule humanitaartoetusele ning lisaks anonüümsuse võimaldamine. Samuti kasutatakse piiriüleseid ühisrahastusplatvorme, mille osas investoril võib puududa tegelik ülevaade ja arusaam toetavast projektist (sh puudub võimalus projektis kajastatut infot kontrollida). Arvestades, et väikeste summade paigutamisel ühisrahastusse puuduvad inimestel üldjuhul spetsiifiliste valdkondade eriteadmised, siis mängitakse paljuski ka inimeste emotsioonide peale (nt humanitaarabi jaoks kogutavad toetused, kuid puudub selgus, kas reaalselt ka kogutud summa jõuab väidetud abivajajani).
- Kuivõrd enamus ühisrahastusteenuse osutajaid ei ole RahaPTS mõttes kohustatud isikud, siis puudub neil kohustus kohaldada terrorismi rahastamise tõkestamisega seotud hoolsusmeetmeid, mis omakorda viib olukorrani, et teenuseosutaja ei kontrolli, kes on rahastatava projekti või toetuse tegelik kasusaaja. See tõstab terrorismi rahastamise haavatavust.
- Oluline haavatavus on ka ühisrahastuse piiriülesus, mis soodustab olukorda, kus näiteks kõrgema terrorismiga riikidest isikud kaasavad rahalisi vahendeid läbi Eestis asutatud ja registreeritud ühisrahastusteenuse osutaja. Oluline on mõista, et terrorismi rahastamiseks ei ole vaja koguda suuri summasid, vaid terroristliku akti toimepanemiseks piisab väikestest summadest.

7.5.2. Riskiteadlikkus

<u>Üldine riskiteadlikkus</u>

Virtuaalvääringu sektor

- Riskiteadlikkus on pigem madal.
- Virtuaalvääringu globaalne mõõde teeb raskeks keskse järelevalve teostamise ja korrakaitseorganite uurimise. Tehinguid tehakse riigipiiride üleselt ja mitmeid erinevates jurisdiktsioonides asuvaid teenusepakkujaid kasutades. Seega on raske kindlaks määrata, kelle jurisdiktsiooni tehtud tehingud kuuluvad ja kuidas tagada vastava informatsiooni kättesaadavus. Seejuures on võimalik olukord, kus tehingud ei kuulu ühegi riigi jurisdiktsiooni, mistõttu järelevalvet ei ole võimalik teostada.
- Rahapesu andmebüroo vajab hea ülevaate saamiseks isikustatud infot nii tehingute, tehingutes kasutatud vara päritolu, rahakottide kui ka tehingute tegelike kasusaajate osas. Samuti on risk kõrgem sellistel toodetel, mille puhul limiidid on suured, kuivõrd korraga on võimalik kontol hoida suures koguses virtuaalraha ja raha on võimalik võtta sularahana välja. Haavatavuseks on ka sellised virtuaalvääringu administraatorid, kes asuvad riikides, kus on ebapiisavad rahapesu ja terrorismi rahastamise tõkestamise seadused.
- Tulenevalt tehingute teostamise kiirusest ja asjaolust, et virtuaalvääringu teenuse osutajad asuvad tihtipeale välisriigis, on RABl raskendatud virtuaalvääringute edasikandmise piiramine ja kohustatud isikult andmete nõudmine. Lisaks suurendatakse tegevusloa olemasoluga (nt virtuaalvääringu teenuse pakkuja tegevusluba) teenuse tarbijates usaldusväärsust, mis võimaldab läbi viia pettuseid ja omastada isikute vara. Samuti on

virtuaalvääringute regulatsioon riigiti erinev, mistõttu puudub riikidel ühesugune ülevaade või kontrollimise võimekus. Näiteks asub üks tehingu osapool riigis, kus tehingus osalejaid ei identifitseerita ega verifitseerita ning tehingute ajalugu, mis oleks seotud konkreetse isikuga, ei ole võimalik esitada või on regulatsioon nõrk, informatsioon RABle kättesaamatu ja raha liikumise jälgimine muutub võimatuks. Riske tekitavad ka sellised virtuaalvääringu teenuse osutajad, kes klientide nimel privaatvõtmeid ei hoiusta, vaid pakuvad nn tööriistasid, mis võimaldavad kliendil enda privaatvõtmeid hoiustada ja sellest tulenevalt võib teenuseosutajal endal puududa ligipääs rahakotile.

- Suurimaks haavatavuseks võib pidada seadusandluse puudumist või selle ebapiisavust. Samuti puudub hetkel laiem regulatsioon, mis reguleeriks laialdasemalt virtuaalvarasid. RahaPTS-s on esitatud virtuaalvääringu mõiste, mis on uuemate virtuaalvarade kontekstis liiga kitsas, kuivõrd uuemad virtuaalvarad seaduses sätestatud mõiste alla ei liigitu ja seetõttu ei allu ka regulatsioonile. Üha enam on levinud *tokenite* kasutamine, mis virtuaalvääringu mõiste alla ei liigitu. Rahandusministeeriumi on esitanud esimesele kooskõlastusringile seaduse eelnõu[96], millega soovitakse reguleerida ka selliseid krüptovarasid ja krüptovara teenuseosutajaid, kes tänase RahaPTS regulatsiooni alla ei sobitu.
- Metoodika kohaselt hinnati haavatavust seoses teenuseosutaja töötajate teadmistega terrorismi rahastamise tõkestamisest kõrgeks.

Küsitluse tulemused teadlikkuse osas:
NRA raames läbiviidud küsitluse tulemused näitavad seda, et sektori teadlikkus terrorismi rahastamise tõkestamisest on pigem tagasihoidlik. Selle põhjused on kirjeldatud ülal.

Sektori teatamise statistikat toetab küsitluse raames saadud tagasiside:

- Sektor täidab tagasihoidlikult oma teatamiskohustust. Küsitlusele vastanutest 6% ei olnud või ei osatud öelda, kas ettevõttes on välja töötatud metoodika ja/või juhend terrorismi rahastamise kahtlusest või ebatavalisest tehingust teatamiseks. Samas on teenusepakkujatel kohustuslik kehtestada metoodika ja juhend, kui tekib rahapesu ja terrorismi rahastamise kahtlus või on tegemist ebatavalise tehingu või asjaoluga, ning teatamiskohustuse täitmise juhend. Samuti selgus küsitlusest, et rohkem kui pooltel teenusepakkujatel ei ole juhendit praktikas vaja läinud. Arvestades küsitlusele vastanute aastakäivete suurust, on kahtlust tekitav, et sedavõrd suurte käivete juures ei ole ettevõtetel ette tulnud tehinguid või asjaolusid, millest tulnuks RABi teavitada. Eelnev viitab sellele, et teenusepakkujad ei järgi seadusega kehtestatud teatamiskohustust ning jätavad mitmed olulised teated ja kahtlused RABle edastamata, mistõttu puudub RABl vajalik informatsioon sektoris levivate riskide ja skeemide tuvastamiseks.
- Teenusepakkujatel puudub teadlikkus, kuidas rakendada hoolsusmeetmete kohaldamisel riskipõhist lähenemist, mis tähendab, et teenusepakkuja ei arvesta võimalike ohte ning hoolsusmeetmete kohaldamine ei ole vastavuses kliendi riskiprofiiliga, mille tulemusena kohaldatakse hoolsusmeetmeid oluliselt madalamal määral.
- Virtuaalvääringu teenuse pakkujatelt uuriti, kas sektori erialaliit või katuseorganisatsioon on sektori ettevõtetele välja töötanud suunised rahapesu ja/või terrorismi rahastamise tõkestamiseks. Veidi üle 40 teenusepakkuja sõnul on vastavad suunised olemas ning nendest on olnud praktilist kasu ettevõtte jaoks. Samas on mõned teenusepakkujad leidnud, et suunised on ebapiisavad rahapesu tõkestamise ja/või terrorismi rahastamise osas. Samuti on ligikaudu 80 teenusepakkuja vastuste kohaselt järelevalveasutus välja töötanud suunised rahapesu ja/või terrorismi rahastamise tõkestamiseks ning 80 leiab, et suunistest on olnud ettevõttele praktilist kasu. Kuivõrd suure hulga küsitlusele vastanute teenusepakkujate jaoks on vastavad suunised praktilist kasu toonud, on suurem tõenäosus, et teenusepakkujad hoiavad ära teenuse pakkumisega kaasnevad riskid, kohandavad vastavalt enda riskijuhtimise mudelit ning esitavad vajalikud andmed RABle. Teisalt on oht, et suunised ei jõua kõigi teenusepakkujateni, kuivõrd mitmed teenusepakkujad ei osanud öelda, kas vastavad suunised on välja antud ning mitme teenusepakkuja arvates suuniseid avaldatud ei ole.

[96] Vt täpsemalt ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu.

Lähtuvalt eeltoodust on sektori üldine riskiteadlikkus terrorismi rahastamisest madal.

Ühisrahastussektor

- Ühisrahastuse valdkonna riskiteadlikkust võib käesoleval ajal pidada keskmiseks. Teadmiste vähesus võib olla tingitud sektori alareguleeritusest, kuid 10.11.2021 hakatakse rakendama EL ühisrahastusmäärust ning käesoleval ajal on menetlemisel ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seaduse eelnõu. Seoses eelnevaga soovitakse kehtestada ka tõhus investorkaitse, mis muudab ettevõtjate tegevust kindlasti läbipaistvamaks. Arvestades, et valdkond on saanud viimastel aastatel ka meedia tähelepanu, siis ühiskonna teadlikkus sektorist on kindlasti tõusuteel. Sellele aitavad kaasa ka investor-blogijad, kes kirjutavad ühisrahastusega seotud teemadel.
- Eestis tegutseb mitmeid ühisrahastusteenuse osutajaid, kes on end vabatahtlikult finantssektoris tavapäraste nõuetega vastavusse viinud ja kes teevad seda ka praegusel ajal, muuhulgas eesmärgiga taotleda 2021. või sellele järgnevatel aastatel ühisrahastusteenuse osutamiseks asjaomast tegevusluba. Mitmed neist täidavad ka MTÜ Finance Estonia ühisrahastuse hea tava suunist, mis küsitluse tagasiside kohaselt on olnud teenuseosutajatele abiks[97]. Küsitluse kohaselt on umbes pooltele vastanutest viidatud suunisest kasu olnud. Üle poolte vastanutest on kasulikuks pidanud ka RABi antud suunised. Enamus küsitlusele vastanutest on kehtestanud RahaPTS §-s 14 sätestatud sise-eeskirjad, kuigi seadusest neile sellist kohustust ei tulene. Arvatavasti on tegemist ärikultuurist tuleneva survega (nt surve krediidiasutuste poolt).
- Metoodika kohaselt hinnati haavatavust seoses teenuseosutaja töötajate teadmistega terrorismi rahastamise tõkestamisest kõrgeks.

Küsitluse tulemused teadlikkuse osas:
NRA raames läbiviidud küsitluse tulemused näitavad seda, et sektori teadlikkus terrorismi rahastamise tõkestamisest on keskmine.

Sektori teatamise statistikat toetab küsitluse raames saadud tagasiside:
Ettevõtte töötajate arusaam kahtlastest tehingutest teavitamise kohustusest on 85,7% vastanutest olemas ja heal tasemel. See on väga positiivne ja vähendab haavatavust.
50% turuosalistest ei oska öelda, kas rahapesu andmebüroole kahtlastest tehingutest teatamise mehhanism on kasutajasõbralik. Üks vastanutest leiab, et see ei ole kasutajasõbralik põhjusel, et see on liiga ajamahukas. Ükski vastanutest pole kokku puutunud nii ületamatute probleemidega, et teade on jäänud esitamata või ei oska seda öelda. Ükski vastanutest pole saanud rahapesu andmebüroolt tagasisidet kahtlaste teadete kvaliteedi kohta või ei oska seda öelda.

Lähtuvalt eeltoodust on sektori üldine riskiteadlikkus terrorismi rahastamisest keskmine.

Juhtkonna pühendumine ja juhtroll
Virtuaalvääringu sektor

- Küsitluse tulemusena selgus, et riskiteadlikkus on sektoris madal ja vajab tõhustamist. Küsitluse tulemusena ei ole Eesti virtuaalvääringu teenuse pakkujad kokku puutunud välismaiste asutuste sunnimeetmetega, mistõttu Eesti teenusepakkujaid need pigem ei mõjuta. Kuigi RahaPTS § 72 lg 1 p 5 loob virtuaalvääringu teenuse pakkujale arveldus- või maksekonto olemasolu kriteeriumi, siis eelduslikult luuakse maksekonto just välisriigi makseteenusepakkuja juures, mis tõstab teenuse osutajate, skriinimise ja järelevalve riski.
- Küsitluse kokkuvõttena võib öelda, et programmi „tunne oma töötajat“ kõikehõlmavus on pigem puudulik ja tööandja ei tunne oma töötajat piisaval määral, mis tekitab kõrge riski.

Juhtkonna pühendumist ja juhtrolli hinnati metoodika järgi kolmes alapunktis, mille haavatavuse hinnangud olid järgmised:

[97] Seda on kasulikuks pidanud ligikaudu pooles vastanutest.

- turu avaldatava surve tase rahapesu tõkestamise standardite järgimiseks – kõrge;
- sisenemiskontrolli olemasolu ja tõhusus – keskmine/madal;
- töötajate ausameelsus - keskmine.

Ühisrahastussektor

- Kuivõrd turuosalised teevad üldjuhul koostööd krediidiasutustega, kohaldavad osad turuosalised RahaPTS-st tulenevaid hoolsusmeetmeid (nn ärikultuuri survel) vabatahtlikult. Ilma krediidi- või makseasutuse koostööta ei oleks võimalik omada kontot, millele kaudu rahasid kaasata.
- Enamik küsitlusele vastanutest viib töötajate värbamisel läbi taustakontrolli, mis vähendab sektori haavatavust. 35,7% vastanutest hindavad töötajate usaldusväärsuse ka töösuhte kestel. Enamik vastanutest teevad oma töötajatele ka koolitusi ja pakuvad võimalusi osaleda temaatilistel veebikursustel. See näitab, et teadlikkus on hea ning koolituste läbimise näol on haavatavus pigem madal.

Juhtkonna pühendumist ja juhtrolli hinnati metoodika järgi kolmes alapunktis, mille haavatavuse hinnangud olid järgmised:

- turu avaldatava surve tase rahapesu tõkestamise standardite järgimiseks – keskmine;
- sisenemiskontrolli olemasolu ja tõhusus – keskmine/kõrge;
- töötajate ausameelsus - keskmine/kõrge.

7.5.4. Terrorismi rahastamise avastamise ja massihävitusrelvade leviku rahastamise tõkestamise kvaliteet

<u>Järelevalve kvaliteet</u>

- Keemiarelva, bioloogilise või bakterioloogilise relva või muu rahvusvaheliselt keelustatud massihävitus- või muu relva või nende oluliste komponentide väljatöötamine, valmistamine, hoidmine, omandamine, edasiandmine, müük või muul viisil kasutamiseks andmine või pakkumine on juba käesoleval ajal karistatav (KarS § 98).

Virtuaalvääringu sektor

- Kuna järelevalve on siiani seisnenud peamiselt andmepäringutes ja tegevuslubade tühistamises, on üleüldine hoolsuskohustus ja juhtkonna pühendumine rahapesu ja terrorismi rahastamise vastases võitluses madal. Kohapealsete kontrollide arv võrreldes teenuseosutajate arvuga on marginaalne. Ka kaugkontrollide arvu tuleks edaspidi tõsta.
- Kõikidest riskihinnangu raames läbiviidud küsitluses osalenud virtuaalvääringu teenusepakkujatest on RAB kontrollinud vaid kahte teenusepakkujat kohapealse kontrolli käigus. Küsitlusele vastanute hulka arvestades on RAB kohapealseid kontrolle läbi viinud sedavõrd vähestes ettevõtetes, mistõttu võivad turuosalised tunda teatud määral kontrolli puudumist. Seevastu vastavalt 10.03.2020 jõustunud RahaPTS muudatustele peab asuma ettevõtte tegevuskoht ning juhatus Eestis, mis soosib rohkemate kohapealsete kontrollide läbiviimist, kuivõrd siiani asusid väga mitmed teenusepakkujad välisriikides ja kontrollide teostamine oli raskendatud.

Virtuaalvääringu teenuseosutajate järelevalvega seotud haavatavusi on hinnatud keskmiseks:

- karistuste olemasolu ja rakendamine – keskmine;
- järelevalvekorra ja -tavade tõhusus – keskmine.

Ühisrahastussektor

- Järelevalve kvaliteeti ei saa hinnata, kuivõrd puudub regulatiivne kontrollmehhanism ja pädev asutus. ÜMIVS eelnõuga soovib seadusandja määrata pädevaks asutuseks, kes hakkab teostama järelevalvet ühisrahastusteenuse osutajate üle, Finantsinspektsiooni. Viidatud asutus hakkab väljastama tegevuslubasid ja kontrollima teenuseosutajate vastavust seadusega

kehtestatud nõuetele. Ühisrahastusteenuse osutajad peavad edaspidi täitma ka RahaPTSi nõudeid, sh nõudeid terrorismi rahastamise tõkestamiseks.

Ühisrahastusteenuse osutajate järelevalvega seotud haavatavusi saab seetõttu metoodika kohaselt lugeda kõrgeks, kuid 2021. aastal on valdkonna õigusraamistik oluliselt muutumas.

Vastavuskontrollisüsteemide ja aruandluse tõhusus

Virtuaalvääringu sektor

Vt analüüsi vastavuskontrollisüsteemide ja aruandluse tõhususe kohta rahapesu tõkestamise haavatavuste plokis.

Virtuaalvääringu teenuseosutajate vastavuskontrolliga seotud haavatavusi seoses terrorismi rahastamisega on hinnatud keskmiseks/kõrgeks:

- vastavuse tagamise süsteemide tõhusus – keskmine/kõrge;
- kahtlustäratava tegevuse jälgimise ja sellest teatamise tõhusus – kõrge.

Ühisrahastussektor

Vastavuskontrollisüsteemide ja aruandluse tõhusust ei saa käesoleva riskihindamise raames metoodika kohaselt adekvaatselt hinnata, kuivõrd praegu puudub regulatiivne kohustus. Siiski ei saa väheoluliseks pidada ärikultuuri survet ehk kui on soov koostööd teha mainekate krediidi- ja makseasutustega, siis peavad turuosalisel olema rahapesu ja terrorismi rahastamise tõkestamise sise-eeskirjad ja kontrollmehhanismid kehtestatud. Pikemat analüüsi vt vastavuskontrollisüsteemide ja aruandluse tõhususe kohta rahapesu tõkestamise haavatavuste plokis.

Ühisrahastusteenuse osutajate vastavuskontrolliga seotud haavatavusi on olemasolevate andmete ja ankeetküsitluste pinnalt hinnatud keskmiseks/kõrgeks:

- vastavuse tagamise süsteemide tõhusus – keskmine/kõrge;
- kahtlustäratava tegevuse jälgimise ja sellest teatamise tõhusus – keskmine/kõrge.

Kliendi suhtes rakendatavate hoolsusmeetmete raamistiku kvaliteet

Virtuaalvääringu sektor

Virtuaalvääringu teenuse pakkujate uuringust selgub, et virtuaalvääringu teenuse tegevusloaga ettevõtete rakendatavad hoolsusmeetmed on selgelt ebapiisavad. Antud probleemi adresseeris teatud määral märtsis 2020 jõustunud RahaPTS muudatus, mille kohaselt peavad virtuaalvääringu tegevusloaga ettevõtted omama tegevuskohta Eestis. Sellele vaatamata on tõenäoline, et sektori ettevõtete hoolsustase ei tõuse hüppeliselt, mille tõttu peaks virtuaalvääringu valdkond pälvima jätkuvat kõrgendatud tähelepanu nii tegevusloa- ja järelevalvemenetlustes kui ka uurimisasutustelt. Virtuaalvääringu teenuse pakkujate uuringus tulemustele toetudes leiab RAB, et virtuaalvääringuid puudutavat regulatsiooni tuleb täiendavalt karmistada ja viidatud teenuseosutajatele tuleb kehtestada finantseerimisasutustega analoogne aruandluskohustus ettevõtete tehingute, klientide ja vahendatud tehingute mahtude osas. Finantseerimisasutustega võrdsustamine tähendas virtuaalvääringu teenusepakkujate jaoks rangemaks muutunud nõudeid hoolsusmeetmete rakendamiseks. Kui varasemalt ei pidanud nimetatud ettevõtjad alla 15 000 euro väärtuses juhuti tehtud tehingute puhul kliente tuvastama, siis nüüd ei sõltu isikusamasuse tuvastamine ja andmete kontrollimine enam tehingu väärtusest, isik tuleb igal juhul tuvastada. Karmistati ka nõudeid kolmandate riikide kodanike isikusamasuse kontrollimisel. Seadusemuudatused jõustusid 10.03.2020. Juba väljastatud tegevusloaga ettevõtetel tekkis kohustus oma tegevus seadusemuudatustega kooskõlla viia hiljemalt 01.07.2020.[98] 2021. aastal tõhustatakse hoolsusmeetmeid veelgi.

Kliendikontrolli raamistiku kvaliteedi osas läbiviidud küsitluse käigus leitud haavatavused:

[98] Rahapesu andmebüroo, Virtuaalvääringu teenuse pakkujate uuring 2020.

- Veidi üle poolte vastanutest leiab, et äriregistri info on usaldusväärne. Samas on valinud vastusevariandi "ei oska öelda" 30% vastanutest, mistõttu on oht, et suur hulk teenusepakkujaid ei kasuta riiklike registreid tegelike kasusaajate tuvastamiseks. Teisalt on võimalik, et teenusepakkuja osutab teenuseid vaid füüsilistele isikutele ning ei ole seetõttu pädev hindama teabe usaldusväärsust. Neli teenusepakkujat on leidnud, et äriregistri info ei ole usaldusväärne.
- Äriregistri praktika võib olla vastuolus imperatiivse RahaPTS § 78 lg-ga 3, kuna isikul on õigus pääseda ligi üksnes 10 äriühingu andmetele ööpäevas. Selleks, et pääseda ligi rohkematele andmetele, on isiku kohustus tasuda igakuiselt 11,50€. Äriregistri kohta on esitatud kommentaare, et vajaliku info kättesaamine on kulukas.
- Vaid 36 teenusepakkujat leiab, et riigisiseste riikliku taustaga isikute kindlakstegemiseks ja kontrollimiseks vajalikule teabele juurdepääs on lihtne, 37 vastajat ei oska aspekti hinnata. Viimane viitab ohule, et ettevõtjad ei kontrolli üldse või piisavalt, kas tegemist on riikliku taustaga isikuga. Informatsiooni peab kättesaamatuks koguni üheksa teenusepakkujat. Samuti võib olla probleem selles, et süsteem ei ole virtuaalvääringu teenuseosutajatele kasutajamugav. Välismaiste riikliku taustaga isikute puhul leidsid üle poole vastanutest, et andmetele ligipääs on pigem keeruline. Küsitluse vastustest võime eeldada, et kuivõrd välisriigi PEPde tuvastamiseks on juurdepääs informatsioonile kas keeruline või kättesaamatu, jätavad teenusepakkujad kohased meetmed rakendamata ja tuvastamata. RABi personaalne tagasiside on vägagi tänuväärne ja kasulik tööriist ja seda soovivad turuosalised rohkem saada.
- Vastustest tuli välja, et 20% vastanutest ei osanud öelda, mis hoolsusmeetmeid kasutatakse kõrgema riskiga juhtumite korral. See võib viidata asjaolule, et nimetatud hoolsusmeetmed on organisatsioonides määramata või on probleeme kliendiriski üldise määramisega. Kui ei ole teada aga kliendiriskid ehk kõrge riskiga kliendid, siis ei ole võimalik ka hoolsusmeetmeid sihtotstarbeliselt rakendada. Tegeleda tuleks ka sisemiste protseduurireeglite ja riskiisuga. Vastavalt RABi virtuaalvääringute uuringule kohaldab kliendikontrolli meetmeid üksnes 3% teenuseosutajatest
- 65% vastanutest hindas juurdepääsu teabele, mis on vajalik teiste suure riskiga klientide (nt saatkonnad, virtuaalvääringute pakkujad, rahateenuseid pakkuvad ettevõtjad, mittetulundusühendused jms) kindlakstegemiseks ja kontrollimiseks, usaldusväärseks.

Küsimustikest „Terrorismi rahastamise tuvastamise ja sellest teatamise tõhusus“ selgunud probleemsed kohad:

- 8% vastanutest kas ei kontrolli rahvusvahelisi sanktsioonide nimekirju terrorismi rahastamisega seoses või ei oska öelda, kas neid kontrollitakse. Samas 20% ei osanud hinnata, kui rakendatavad need nimekirjad on. Seega võib olla, et turuosaliste seas on segadus, kuidas nimetatud nimekirju terrorismi rahastamise tõkendamiseks rakendama peaks.
- Terrorismi rahastamise tõkestamise riskistsenaariumid on olemas vaid 42 teenusepakkujal. Seda ilmestab ka asjaolu, et aastal 2019 esitati terrorismi rahastamise kahtlusega teateid RABle vaid kuuel korral. Eelnev viitab sellele, et teenusepakkujad ei pööra piisavalt tähelepanu terrorismi rahastamise tõkestamisele. Tegelikult ei ole väike terrorismi tõkestamise kahtlusega teadete arv üldse ebatavaline. Seda ongi turuosalistele ülimalt raske tuvastada.
- Arvestades asjaoluga, et aastal 2019 esitati terrorismi rahastamise kahtlusega teateid vaid kuus, aastal 2018 ei esitatud ühtegi, on vastavate uurimiste arv antud sektori kohta pea olematu. Kindlasti omab terrorismi rahastamise tuvastamisel probleemi andmete konfidentsiaalsus, st turuosalised ootaksid suuremat koostööd KAPOga.
- 43% hinnangul on sektoris olemas TFR juhend, kuigi 21% hinnangul ei ole see piisav või pole seda olemas. Seega on juhendi kvaliteet küsitav. Kuigi ligipääs tasulistele allikatele on hea, siis pole kohustatud isikul võimalik kindlaks teha nende efektiivsus ja adekvaatsus. Niisamuti tõstab riski asjaolu, et riskilistides olevatel isikutel on üldjuhul kas samad või äärmiselt sarnased nimed, mistõttu on skriinimine äärmiselt ebaefektiivne ja vale-positiivse info rikas, mistõttu võib kohustatud isiku skriinimise kvaliteet saada kannatada.

- Radikaalsete liikumiste ja vaenulike infokampaaniate või välispropagandaga seotud rahavoogude tuvastamise tõhususe kohta on leitud järgmist – kaheksal teenusepakkujal vastavad kontrollimehhanismid puuduvad ning 45 ei oska öelda, mistõttu võime eeldada, et üle pooltel teenusepakkujatel need puuduvad. Eelnev viitab sellele, et teenusepakkujad ei ole ettevõttes kohaldatavaid kontrolle viinud kooskõlla sektoris valitsevate riskidega, antud juhul terrorismi rahastamise riskidega.
- Terrorismi rahastamise riskide arvestamine kliendikontrolli käigus – selgus, et radikaalsete liikumiste ja vaenu kampaaniatega seotud kontrolle on teinud lausa 47% vastajatest, mis on tegelikult väga positiivne, kuna ei ole kõige levinum terrorismi rahastamisega seotud risk. 87 teenusepakkujat hindab klientide taustakontrolli käigus terrorismi rahastamise riske, kuid tulenevalt eelmiste küsimuste tulemusest on tegemist vastuoluga ning ettevõtjad ei hinda neid riske piisaval määral.
- Ligikaudu 30% vastanutest ei teosta oma töötajatele asjaomaseid koolitusi. Kuigi koolituskohustus on olemas, siis on ligipääs terrorismi rahastamise tüpoloogiatele raskesti kättesaadav ja kinnine. Reeglina on koolitused suunatud rahapesu tõkestamisele, terrorismi rahastamise alaseid koolitusi on vähe, rääkimata massihävitusrelvade leviku tõkestamise koolitustest.
- Terrorismi rahastamise tõkestamiseks mõeldud kontrollimeetmete olemasolu – selgus, et lisaks sellele, et 87% teostab taustakontrolli, teostab 76% vastanutest ka monitooringut. Ligikaudu kolmveerand vastanutest kasutab väidetavalt vastavaid kontrollimeetmeid, kuid tulenevalt eelnevatest vastustest on vastus pigem vastuoluline ning selle pinnalt ei ole võimalik järeldusi teha.

Virtuaalvääringu teenuseosutajate kliendi suhtes rakendatavate hoolsusmeetmetega seotud haavatavusi on hinnatud keskmiseks või keskmiseks/kõrgeks:
- kliendi riskitaseme riskipõhist arvutamist võimaldava süsteemi olemasolu – kõrge;
- riikliku taustaga isikute kindlakstegemise tõhusus – keskmine/kõrge.

Ühisrahastussektor
Kliendi suhtes rakendatavate hoolsusmeetmete tõhusust ei saa käesoleva riskihindamise raames adekvaatselt hinnata, kuivõrd teenuseosutajatel puudub asjaomane regulatiivne kohustus. Siiski ei saa väheoluliseks pidada ärikultuuri survet ehk kui on soov koostööd teha mainekate krediidi- ja makseasutustega, siis peavad turuosalisel olema rahapesu ja terrorismi rahastamise tõkestamise siseeeskirjad ja kontrollmehhanismid kehtestatud.

Kliendikontrolli raamistiku kvaliteedi osas läbiviidud küsitluse käigus leitud haavatavused:
- Riigi registrites sisalduva tegelikke tulusaajaid käsitleva teabe usaldusväärsus – alla poolte vastanutest hindavad usaldusväärseks ja pooled ei oska öelda.
- Lihtne juurdepääs teabele, mis on vajalik tegelike tulusaajate kindlakstegemiseks – 14st 11 hindavad infot hõlpsasti kättesaadavaks.
- Kõikehõlmavad ja usaldusväärsed avalikud infosüsteemid, mis aitavad kontrollida klientide andmeid – pooled hindavad põhjalikuks ja usaldusväärseks, pooled ei oska öelda.
- Lihtne juurdepääs teabele, mis on vajalik riigisiseste riikliku taustaga isikute kindlakstegemiseks ja kontrollimiseks – enamuse arvates info olemas, aga pigem keeruline kätte saada. Ametipositsioonid olemas, aga raske isikut ja ametipositsiooni kokku viia (eraldi keeruline PEPidega seotud pereliikmete ja lähedaste kaaslaste osas).
- Lihtne juurdepääs teabele, mis on vajalik välismaiste riikliku taustaga isikute kindlakstegemiseks ja kontrollimiseks – enamuse arvates olemas, aga keeruline juurde pääseda. Globaalses mõttes on PEP-ide info kättesaadav läbi tasuliste teenuseosutajate.
- Lihtne juurdepääs teabele, mis on vajalik teiste suure riskiga klientide (nt saatkonnad, virtuaalvääringute pakkujad, rahateenuseid pakkuvad ettevõtjad, mittetulundusühendused jms) kindlakstegemiseks ja kontrollimiseks – juurdepääs sõltub suuresti isiku võimekusest investeerida teenuse pakkujate lahendustesse.

Küsimustikest „Terrorismi rahastamise tuvastamise ja sellest teatamise tõhusus“ selgunud probleemsed kohad:

- Radikaalsete liikumiste ja vaenulike infokampaaniate või välispropagandaga seotud rahavoogude tuvastamise tõhusus – 14st 5 kohaldavad, 5 ei oska öelda ja 4 ei kohalda (3 ei ole selliseid kliente).
- Terrorismi rahastamise riskide arvestamine kliendikontrolli käigus – 14st 13 kohaldavad, 1 ei oska öelda.
- Terrorismi rahastamise tõkestamiseks mõeldud kontrollimeetmete olemasolu – pooled kohaldavad monitoorimisel terrorismi rahastamise tõkestamisele suunatud kontrollimeetmeid, 5 ei oska öelda.

Ühisrahastusteenuse osutajate kliendi suhtes rakendatavate hoolsusmeetmetega seotud haavatavusi on hinnatud keskmiseks/kõrgeks:

- kliendi riskitaseme riskipõhist arvutamist võimaldava süsteemi olemasolu – keskmine/kõrge;
- riikliku taustaga isikute kindlakstegemise tõhusus – keskmine/kõrge.

<u>Sektoripõhiste rahvusvaheliste sanktsioonide kindlakstegemise kvaliteet</u>
Virtuaalvääringu sektor

FATF korrigeeris 2019. aastal oma standardeid, tuues riikidele sisse nõude hinnata ja maandada virtuaalvääringutega seonduvaid riske. Selleks peavad riigid virtuaalvääringute teenusepakkujaid litsentseerima või registreerima. Riigid peaksid tagama, et teenusepakkujad kasutavad kõiki võimalikke rahapesu ja terrorismi rahastamist ennetavaid meetmeid, sh kliendi kohta käivaid hoolsusmeetmeid, klientide ning tehingute andmete kogumist ja säilitamist, kahtlastest tehingutest teavitamist ja veendumist, et tehingud oleksid vastavuses rahvusvaheliste sanktsioonidega. Samuti tuleks teenusepakkujaid monitoorida ning vajadusel ka karistada, kui teenusepakkujad lähevad vastuollu rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmetega. Täpsustati ka seda, et FATFi soovitusi järgides peaks virtuaalvääringuid käsitlema kui vara, tulu või muud analoogset rahalist väärtuseühikut[38].[99]

Sanktsioonide tuvastamise kvaliteedi osas läbiviidud küsitluse käigus leitud haavatavused

- Ligikaudu 80 teenusepakkujat kontrollib rahvusvaheliste sanktsioonide nimekirju, kellest ligikaudu pooled kasutavad selleks kolmandate osapoolt loodud registreid/süsteeme. Seejuures on monitoorimise süsteem pooltel vastanutest poolautomaatne. Kuivõrd ligikaudu 20 teenusepakkujat nimekirju ei jälgi ning eeldatavasti vastavaid süsteeme ei oma, on see suureks ohuks, et nende teenusepakkujate teenuseid kasutavad sanktsioneeritud isikud. 92% kontrollib.
- Sanktsioonidest kõrvalehoidmise tuvastamise mehhanismide tõhusus – vastavat mehhanismi omab vaid 35 teenusepakkujat, mistõttu jätab enamik teenusepakkujaid tuvastamata sanktsioonidest kõrvalehoidumise. Niisamuti esineb risk, et sanktsioonikontrolli ei teostata seire käigus, üksnes ärisuhte loomisel.
- Kohaldatavate sektoripõhiste sanktsioonide teadmine ja rakendamine – vastustest nähtub, et vaid umbes pooled vastanud turuosalised omavad ülevaadet finantssanktsioonidega seonduvast. 92% teostab asjaomaseid kontrolle. Niisamuti esineb risk, et sanktsioonikontrolli ei teostata seire käigus, vaid üksnes ärisuhte loomisel.
- Varade külmutamise mehhanismide tõhusus – varade külmutamise protseduur on dokumenteeritud vaid veidi rohkem kui pooltel teenusepakkujatel. Varade külmutamise protseduur oli olemas vaid 57% vastanutest, mistõttu on oht, et turuosalised ei saa tegelikult aru sanktsioonide tuvastamise süsteemi eesmärgist. Eelnevast võib järeldada, et viidatud mehhanismid ei ole tõhusad.

[99] Rahapesu andmebüroo, Virtuaalvääringu teenuse pakkujate uuring 2020.

Virtuaalvääringu teenuseosutajate rahvusvaheliste sanktsioonide kindlakstegemise kvaliteediga seotud haavatavusi on hinnatud keskmiseks.

Ühisrahastussektor
Sanktsioonide kindlakstegemise kvaliteeti on keeruline hinnata, sest puuduvad info ja kaasused, kus oleks RAB-i poolt tuvastatud, et turuosalised on rikkunud rahvusvahelisi sanktsioonide.

Sanktsioonide tuvastamise kvaliteedi osas läbiviidud küsitluse käigus leitud haavatavused:

- Sanktsioonide olemasolu kontrollimise tõhusus – 14st 11 vastanut kontrollivad sanktsioonide nimekirju, kuid on välja toonud, et andmekvaliteedi tõttu on meetmed raskesti rakendatavad. Sanktsioonide vastu skriinivad vastanutest 10 teenuseosutajat. Vastajad leidsid, et sanktsioonide otsingumootorid võiksid olla selgemad.
- Sanktsioonidest kõrvalehoidmise tuvastamise mehhanismide tõhusus – enamusel ei ole vastavaid mehhanisme välja töötatud.
- Varade külmutamise sisemiste protseduuride olemasolu – küsimusele, kas ettevõttel on olemas varade külmutamise protseduur, vastasid 42,9%, et on. Seega olulisel osal ühisrahastusteenuse osutajatest puudub protseduur, kuidas rakendada RahaPTS tehingu tegemise keeldu hoolsusmeetmete kohaldamata jätmisel või rahapesu või terrorismi rahastamise kahtluse korral või vara edasikandmise piirangud.

Ühisrahastusteenuse osutajate rahvusvaheliste sanktsioonide kindlakstegemise kvaliteediga seotud haavatavusi on olemasolevate andmete pinnalt hinnatud madalaks.

7.5.5. Sektoriomaste riskide hindamine sektoripõhiste kontrollide kvaliteediga

Virtuaalvääringu sektor

- Kuna ettevõtted tegutsevad rahvusvaheliselt, siis see teeb antud ettevõtete kasutamise kuritegevuse eesmärgil märkimisväärselt lihtsamaks. Kuna ettevõtetel ei ole igas riigis kontoreid, kus isikuid tuvastatakse (erinevalt pankadest), vaid seda tehakse interneti teel, on märkimisväärselt suurem oht, et luuakse kontosid nn tankistide või varastatud identiteeti kasutades. Ligikaudu 50% ettevõtjatest ei ole kasutusele võtnud erinevaid mehhanisme (näiteks sanktsioonidest kõrvalehoidmine, terrorismi rahastamine (see küll vaid 25%), radikaalsete liikumiste, kahesuguse kasutusega kaupadega seonduvad rahavood jne), millega saaks märkimisväärselt rahapesu ja terrorismirahastamist paremini tuvastada. Samuti vastasid „ei“ või „ei oska öelda“ ligikaudu 40% ettevõtetest varade külmutamise protseduuri dokumenteerimise kohta. Vt täpsemalt sektoriomaste riskide hindamise kohta rahapesu tõkestamise vastava alateema alt.
- Sektoriomaste riskide tuvastamise tõhususega seotud haavatavusi on hinnatud keskmiseks/kõrgeks.

Ühisrahastussektor

- Sektoripõhiste kontrollide riskide hindamise kvaliteeti ei saa adekvaatselt hinnata, kuivõrd puudub regulatiivne kohustus sektori kontrollimiseks. Siiski ei saa väheoluliseks pidada ärikultuuri survet ehk kui on soov koostööd teha mainekate krediidi- ja makseasutustega, mistõttu peavad turuosalisel olema kehtestatud rahapesu ja terrorismi rahastamise tõkestamisega seotud sise-eeskirjad ja paigas vastavad kontrollmehhanismid.
- Sektoriomaste riskide tuvastamise tõhususega seotud haavatavusi on hinnatud madalaks.

7.5.6. Varasemate hindamiste käigus tuvastatud riskidele reageerimise kvaliteet

Virtuaalvääringu sektor

Vt täpsemalt rahapesu tõkestamise asjaomases alapeatükis kirjutatut.

2015. aastal avaldatud Eesti rahapesu ja terrorismi rahastamise siseriiklik riskihinnangu eesmärk oli kehtivate rahapesu ja terrorismi rahastamise tõkestamise meetmete ülevaatamine ja täiendamine. RABi 2018 aastaraamatus esitati peamiste virtuaalvääringu teenuse pakkujatega seotud riskidena muuhulgas ka terrorismi rahastamine. On leitud, et RAB tegevusloaga teenusepakkujate juures on proovinud avada kontosid välisriikide isikud, kellel on terrorismikahtlused.

Euroopa Komisjoni riigiülese rahapesu ja terrorismi rahastamise riskihinnangu (SNRA) 2017 ja 2019 analüüsis virtuaalvarade[100], sh –vääringute kohta (SNRA 2017/2019) leiti antud sektori osas, et Euroopa-üleselt on virtuaalvääringu rahapesu ja terrorismi rahastamise risk kõrge või isegi väga kõrge.[101] Liikmesriikidele tehti ettepanek võtta virtuaalvarade teenuseosutajad kõrgendatud tähelepanu alla.

SNRA 2017/2019 leiti, et virtuaalvääringute teenusepakkujad on jätkuvalt kõrgendatud tähelepanu all, millele soovitab Komisjon pöörata erilist tähelepanu (eelkõige tehingute kiirus ja anonüümsus). Nimetatud valdkonnas rahapesu ja terrorismi rahastamise risk on kasvav (kahtlaste ülekannete arvu kasv virtuaalvara, sh virtuaalvääringuga seonduvalt).

Terrorismi rahastamise riskidena on leitud, et virtuaalvara, sh virtuaalvääringu kasutamisel sisaldab endas näost näkku kohtumise puudumist, mis omakorda võib võimaldada anonüümselt rahastamise või toodete soetamise (sularaha sissemaksed või maksed kolmandate isikute poolt, milles ei tuvastata vahendite päritolu). Samuti on probleemiks anonüümsed ülekanded, kui saatjat ja saajat korrektselt ei tuvastata.

Olulist rahapesu ja terrorismi rahastamise ohtu kujutavad endast ka isikud, kes pakuvad virtuaalvara, sh virtuaalvääringu „segamise“ teenust *(mixing services)*, mis võimaldab suuremat privaatsust, kiiremaid ülekandeid, madalamaid ülekandetasusid ja väiksemat hinnakõikumist.

Väljakutseks on virtuaalvara, sh virtuaalvääringu teenuse osutajad kurjategijate või regulatsioonidega mittevastavuses olevate juriidiliste isikutega, kes:
1. kasutavad kuritegelikul teel saadud vahendeid, et luua virtuaalvara, sh virtuaalvääringu ettevõtte, millesse makstakse sularaha sissemaksena kuritegelikul teel saadud vahendeid;
2. isikud ostavad/müüvad suures mahus virtuaalvara, sh virtuaalvääringu teiste varade vastu (ilma vahendajata) ilma, et need isikud oleksid registreeritud teenusepakkujad (sh ei reklaami enda teenuseid);
3. makseasutused, kes pakuvad virtuaalvääringu maksekaarte, mis toetavaid erinevat virtuaalvara, sh virtuaalvääringu (üldjuhul nad registreerivad oma tegevuse „sobivaimas“ jurisdiktsioonis).

Täiendavalt leiti, et järelevalveasutuste töö muudab keeruliseks ka andmete kogumine olukorras, kus ülekanne toimub erinevas riigis võrreldes maksja ja maksesaaja asukohaga.

Seetõttu hinnati, et virtuaalvarade puhul on terrorismi rahastamise risk kõrge. Kurjategijad kasutavad järjest enam virtuaalvara, sh virtuaalvääringu terrorismi rahastamiseks (sh antakse juhiseid internetis, kuidas kasutada virtuaalvarasid).

Sektori haavatavuste puhul toodi välja, et terrorismi rahastamise oht on kõrge või väga kõrge ning sellele viitavad:
1. anonüümsed ja kiired ülekanded (ilma omaniku tuvastamata);
2. interneti kasutamine ehk piiriülene risk, mis võimaldab teha tehinguid kõrge riski piirkonnast või kõrge riskiga klientidega, keda ei ole võimalik tuvastada;

[100] FATF - Virtual Asset - *A digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes, and that does not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.*
[101] Euroopa Komisjoni riigiülese rahapesu ja terrorismi rahastamise riskihinnangu (SNRA) 2017 ja 2019 analüüs.

3. virtuaalvara, sh virtuaalvääringu kasvav populaarsus kurjategijate seas;
4. terrorismi rahastamise riski teadlikus on riikides madal (olenemata asjaolust, et virtuaalvara, sh virtuaalvääringu osas on AML/CFT regulatsioone hakatud kohaldama);
5. riske suurendavad asjaolud:
   5.1. puuduvad teadmised ja arusaamine, mis ei võimalda korrektselt mõjusid hinnata;
   5.2. puudused kehtivas regulatsioonis;
   5.3. tõenäoline krediidi- ja finantseerimisasutuste „vahendajatena“ ärakasutamine (korrektse riskihinnangu puudumise tõttu);
   5.4. investeerimissektoris internetis tehingute tegemine limiteeritud kliendi tuvastamise ja verifitseerimise kontrolliga;
6. AMLD5 kasutatav virtuaalvääringu mõiste võib olla liiga kitsas (võrreldes FATF-i virtuaalvara mõistega) ja seetõttu ei kata kõiki valdkondi (sh ICOde pakkujad)[102], sh:
   6.1. rahakotiteenuse pakkujad, kes ei hoiusta klientide nimel privaatvõtmeid, vaid pakuvad üksnes tööriistasid, et klient saaks ise oma privaatvõtmeid hoiustada;
   6.2. vahetusteenused virtuaalvarast virtuaalvääringutesse ja vastupidi;
   6.3. virtuaalvaraga pakkumistega/müügiga seotud finantsteenuste osutamine.

Ühisrahastussektor

Tegemist on uue populaarsust koguva sektoriga. Varasemas riiklikus riskihinnangus ühisrahastuse sektorit ei käsitletud. Vt täpsemalt rahapesu tõkestamise asjaomases alapeatükis kirjutatut.

SNRA 2017/2019 leiti antud sektori osas, et Euroopa-üleselt on ühisrahastuse rahapesu ja terrorismi rahastamise risk on keskmiselt kõrge.[103] Kurjategijad võivad platvormide kaudu kaasata vahendeid (kogudes vahendeid legaalselt või kriminaalsetest tegevustest, kasutades anonüümseid tooteid) ja saata need välismaale rahapesu või terrorismi rahastamise eesmärgil. Nad võivad kaasata vahendeid ka annetuspõhise ühisrahastuse kaudu, milles summad on väikesed. Tuvastatud on terrorismi rahastamised, kus:

1. kogutakse vahendeid märksõnadega: „toeta leske, märtreid või usurühmasid/usklike“;
2. summad on väikesed (nt 10, 20, 50 dollarit).

Liikmesriikidele tehti järgmine ettepanek: kui liikmesriik võtab üle AMLD 4 ja 5, siis peab liikmesriik kaaluma vajadust reguleerimata ühisrahastusteenuse osutajate käsitlemist kui kohustatud isikut AML/CFT regulatsiooni mõttes.

Leiti, et terrorismi rahastamise risk on ühisrahastuse sektori puhul keskmiselt kõrge.

Varasemas riiklikus riskihinnangus ühisrahastuse sektorit ei käsitletud. SNRA 2017/2019 leiti antud sektori osas, et Euroopa-üleselt on ühisrahastuse terrorismi rahastamise risk keskmiselt kõrge, eeskätt kasutatakse terrorismi rahastamiseks annetuspõhiseid ühisrahastusteenuse osutajaid.

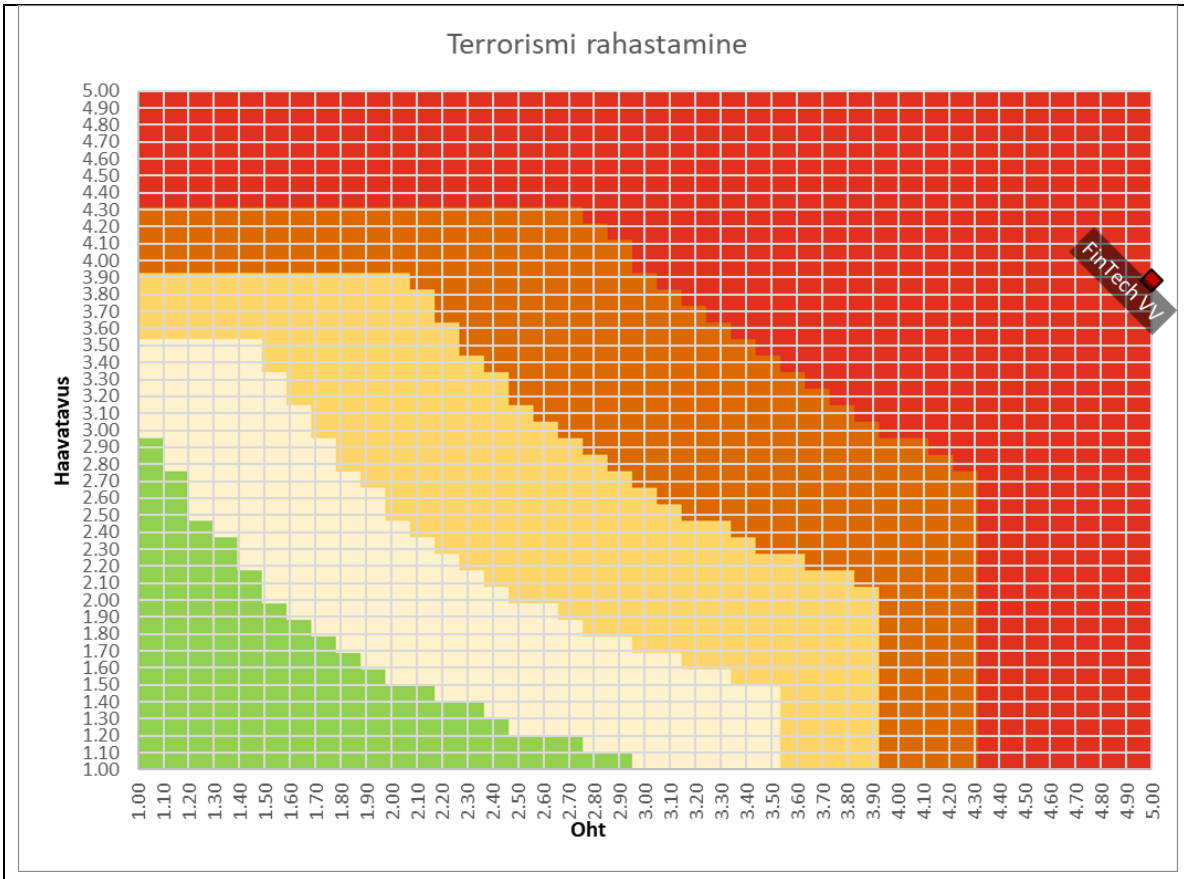
7.5.7. Järeldus

Virtuaalvääringu sektor

Küsitluse ja töörühma arutelude tulemusena on virtuaalvääringu sektori haavatavust skaalal 1-5 hinnatud terrorismi rahastamise suhtes 3,88 ehk seda võib pidada keskmiseks. Virtuaalvääringu sektori haavatavust vähendavad asjaolud on välja toodud rahapesu haavatavuste asjaomases alapeatükis.

Joonis 10. FinTech VV-de terrorismi rahastamise riskitaseme soojuskaart

[102] Esialgne müntide pakkumine (ingl *Initial Coin Offering* ehk ICO).
[103] Euroopa Komisjoni riigiülese rahapesu ja terrorismi rahastamise riskihinnangu (SNRA) 2017 ja 2019 analüüs.



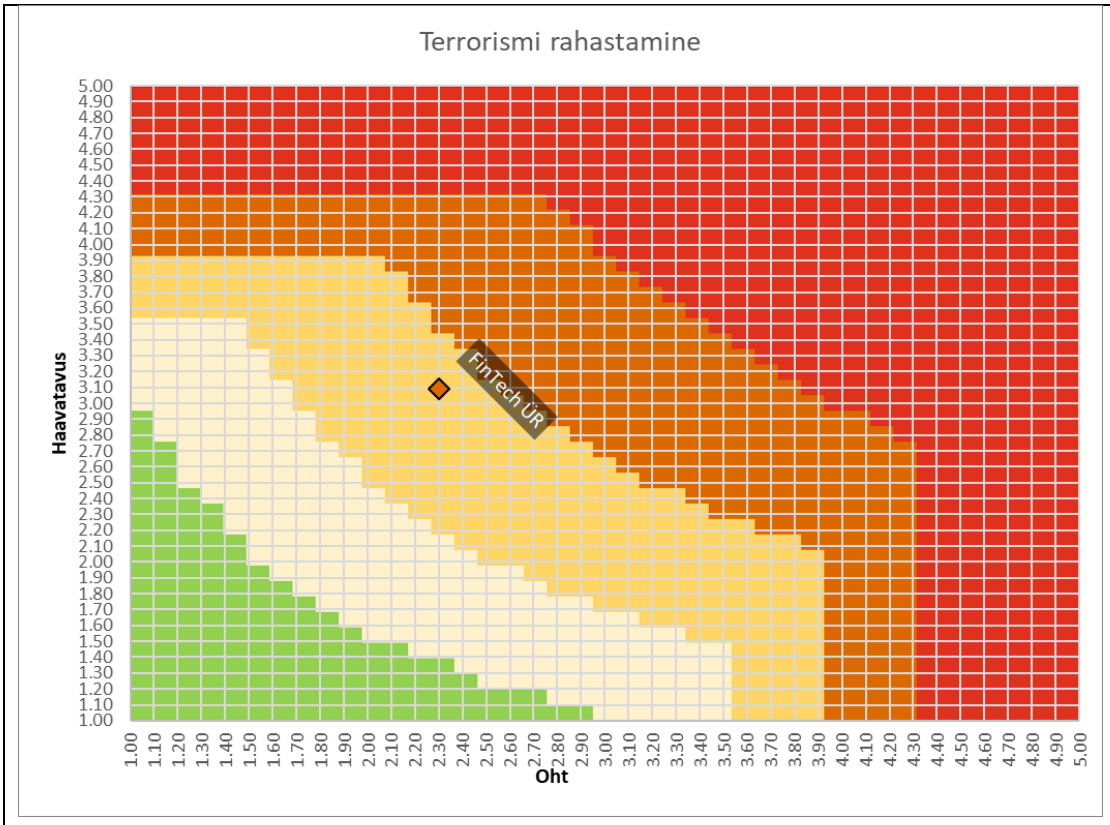
Kokkuvõte

Virtuaalvääringute puhul on terrorismi osas tegemist **kõrge** riskitasemega sektoriga ja see on tingitud kõrgest ohust. Sektoris tuleb rakendada hoolsusmeetmeid tugevdatud kujul.

Ühisrahastussektor

Skaalal 1-5 on ühisrahastuse sektori haavatavuse hinne terrorismi rahastamise aspektist 3,09 ehk seda võib pidada keskmiseks. Ühisrahastuse sektori haavatavust vähendavad asjaolud on välja toodud rahapesu haavatavuste asjaomases alapeatükis.

Joonis 11. FinTech ÜR terrorismi rahastamise riskitaseme soojuskaart



Kokkuvõte
Ühisrahastuse puhul on terrorismi rahastamise aspektis tegemist **keskmise** riskitasemega sektoriga. Sektoris tuleb rakendada hoolsusmeetmeid tavakorras.

7.5.8. Riskimaandamise strateegia

7.5.8.1. Leevendavad meetmed riiklikul tasandil

Leevendavad meetmed riiklikul tasandil kattuvad suuresti rahapesu tõkestamise haavatavuste asjaomases alapeatükis kajastatuga.

7.5.8.2. Leevendavad meetmed kohustatud isikute tasandil

Virtuaalvääringute sektor

- Eduka terrorismi rahastamise kampaania läbiviimiseks on vaja mingil tasemel e-turundust, mistõttu on asjaomaste aadresside, sh nendega seotud aadresside, tuvastamine internetiavarustest spetsialisti pädevuses. Kuivõrd virtuaalvääringute puhul on adekvaatsete mehhanismide kasutusevõtul hõlbus tuvastada virtuaalvääringute lähte- ning sihtpunkte, on koostöös julgeolekuasutustega, sh KAPO-ga, virtuaalvääringute sektoril võimalik tuvastada terrorismi rahastamisega seotud virtuaalvääringutega seotud aadressid ning kliendid, kes otseselt või kaudselt on selliste aadressidega mingil viisil seotud, mis omakorda võimaldaks eelviidatud informatsiooni vastavate pädevate asutustega jagada.
- On vaja rõhutada koostöö olulisust seadusandja, järelevalve ja turuosaliste vahel, mitte üksnes läbi erialaliidu, vaid vabatahtlikus vormis turuosaliste vahel.
- Tagamaks suurem andmetöötlusvõimekus- ja kvaliteet järelevalve poolt tuleks arendada RAB teadete esitamise süsteemi viisil, millega oleksid virtuaalvääringute tehingute andmed masintöödeldavad, kuivõrd ilma selleta on andmetöötluskvaliteet madal.

Ühisrahastussektor

- Ühisrahastusteenuse osutajad vajavad täiendavaid meetmeid oma teadlikkuse suurendamiseks riskidest ja sisemistest kaitsemeetmetest oma teenuste väärkasutamise vastu ning vaja on sektori reguleerimist.
- Erialaliidu või katuseorganisatsiooni kaudu võiks teha koolitusi, et tõsta turuosaliste teadlikust ja teadmisi seoses terrorismi rahastamise riskidega ja asjaomaste hoolsusmeetmete kohaldamisega.
- Võimalusel võiks lisada terrorismi sanktsioonide määratlustesse teabena ka e-posti aadressid, IP-aadressid ja sotsiaalmeedias kasutatavad kasutajanimed. Ehkki vastavad kasutajad saavad sellist identifitseerimisteavet hõlpsasti ja kiiresti muuta, oleks selle lisamine määramisteavetesse vähemalt lähtepunkt ettevõtete sisejuurdlusteks.
- Terrorismi rahastamisele keskendunud resolutsioonis kutsus ÜRO Julgeolekunõukogu üles selle ohu vastu võitlemiseks looma tõhusad partnerlussuhted erasektoriga, sealhulgas finantstehnoloogia tööstuse ning interneti- ja sotsiaalmeediaettevõtetega.[104]
- Ühisrahastusteenuse osutajad peaksid pöörama erilist tähelepanu jurisdiktsioonidele, mis teadaolevalt rahastavad või toetavad terroriakte või kus teatakse, et tegutsevad terroriakte sooritavad rühmad, ning jurisdiktsioonidele, mille suhtes kehtivad rahalised sanktsioonid, embargo või meetmed (välja andnud näiteks EL või ÜRO), mis on seotud terrorismi, terrorismi rahastamise või massihävitusrelvade leviku tõkestamisega.

[104] Allikas: https://www.acamstoday.org/new-technologies-the-emerging-terrorist-financing-risk/.