Rahapesu Andmebüroo

Rahapesu Andmebüroo aastaraamat 2021

Rahapesu Andmebüroo aastaraamat 2021
Keeletoimetaja: Mare Timian
Kujundus: Division OÜ
Illustratsioonid: Shutterstock

Rahapesu Andmebüroo
Pronksi 12, 10117 Tallinn
fiu.ee

ISSN 2806-190X (elektrooniline väljaanne)

Sisukord

Hea lugeja!

Foto: Annemai Sepp

Teie ees on Rahapesu Andmebüroo kui iseseisva asutuse esimene aastaraamat. Rahapesu Andmebüroo asutati 1. juulil 1999 toonase Politseiameti juurde, kuid tema teiseks sünnipäevaks saab pidada 1. jaanuari 2021, mil andmebüroost sai rahandusministeeriumi valitsemisalasse kuuluv valitsusasutus. Andmebürood on aastate jooksul juhtinud Arnold Tenusaar, Raul Vahtra, Aivar Paul ja Madis Reimand. Uue asutuse esimestel kuudel täitis büroo juhi kohusetäitja ülesandeid Marget Lundava. Mul oli au see vastutusrikas ülesanne üle võtta 14. juunist 2021.

Esimene aasta andmebüroo uuest ajajärgust on olnud tegus ja paljude väliste vaatlejate sõnutsi on andmebüroo tõusnud senisest enam suunanäitajaks Eesti rahapesu ja terrorismi rahastamise tõkestamise maastikul. Aastasse on mahtunud uue asutuse ülesehitamine ja paljude uute töötajate värbamine, uurimisasutuste abistamine keerukate rahapesu kriminaalasjade läbiviimisel, erasektori, uurimisasutuste ja prokuratuuri koolitamine ja riskipildi tutvustamine, uue strateegia kujundamine aastani 2026, prioriteetide seadmine ja tööplaanide tegemine ning uue rolliga kohanemine. Enim on aga andmebüroo tegelenud 2021. aastal rahvusvahelise finantssanktsiooniga seotud tegevuste ettevalmistamisega, Euroopa Komisjoni küsimustele vastamisega seoses IV rahapesu tõkestamise direktiivi täitmise efektiivsuse hindamisega, Euroopa Nõukogu eksperdikomitee MONEYVAL hindamise ettevalmistamisega ning turu korrastamise ja järelevalve tugevdamisega virtuaalvääringu teenusepakkujate sektoris.

Andmebüroo esimese tegevusaasta lõpp jäi aega, kui tulid uudised Venemaa vägede ja rasketehnika koondumisest Ukraina piiri äärde. Ekspertide hinnangul nähti sellise mastaabiga operatsiooni viimati II maailmasõja ajal. Sellistel hetkedel mõistame selgemalt kui kunagi varem, miks peame jõuliselt ja selgepiiriliselt võitlema rahapesu ja terrorismi rahastamise ning kuritegevuse vastu. Rahapesu vastane võitlus tagab muu hulgas selle, et kuritegelikud ühendused ja üksikkurjategijad ei saaks kasutada kuritegelikul teel saadud vara. Eesmärk on ka see, et vara – nii raha kui ka virtuaalvääringute edastamise

kanaleid läbiks vaid #ausraha. See tähendab, et kuritegelikku raha ei saaks kasutada varjatud rahastamisena näiteks Wagner grupi sõdurite jaoks, kes sõdivad Ukrainas Venemaa eest ja nimel, nagu nad tegid seda ka Süürias, Liibüas, Malis ja mujal. Ka Venemaa vastu suunatud finantssanktsioonid lähtuvad samadest põhimõtetest – lõigata läbi otse või kaude sõda toetavate kuritegevusega seotud inimeste võimalused kasutada enda vara. Venemaa tegevus Ukrainas läheb vastuollu kõikide rahapesu, terrorismi rahastamise ja massihävitusrelvade leviku rahastamise tõkestamise põhimõtetega. Me peame seetõttu võitlema rahapesu vastu, et kurjategijad ei mõtleks kuriteo toimepanemisele. Peame võitlema terrorismi rahastamise vastu, et vähendada võimalust terrorikuritegude toimepanemiseks ning massihävitusrelvade leviku vastu, et tuuma- või keemiarelva ei saaks arendada ega kasutada ei Venemaa ega ka Põhja-Korea ja Iraan.

Sõja kontekstis on palju räägitud ka virtuaalvääringutest kui varaklassist, kuhu Vene kodanikud ja sõja toetajad oma varasid paigutavad. Samuti virtuaalvääringu teenusepakkujatest, kes aitavad Euroopa Liidu kehtestatud finantssanktsioonidest kõrvale hoida ja rahastada sõjategevust. Kuid mitte ainult. Kurjategijad kasutavad virtuaalvääringu teenusepakkujaid täna ära rohkem kui eales varem, muutes krüptokanalid kohati kõige enam kasutatavaks rahapesu ja terrorismi rahastamise kanaliks.

Oleme olukorras, kus Eesti virtuaalvääringu teenuse pakkujate aastakäive ületab juba 20 miljardit eurot, mis on ligikaudu 25% Eesti pangandussektori välismaksete mahust, toimub kapitali väljavool Venemaalt ja varade suunamine Süüriasse, Pakistani ja teistesse riskiriikidesse või konfliktipiirkondadesse. Selles sektoris on mõnikümmend tuhat klienti Eestist versus ligi 5 miljonit mitteresidenti. Virtuaalvääringute teenuse pakkujatega seoses on plahvatuslikult kasvanud andmebüroole ja Eesti uurimisasutustele esitatud päringud välisriikide partnerasutustelt. Need on seotud mõne aasta taguse organiseeritud kuritegevuse, kelmuse, lapsporno, terrorismi rahastamise kahtluse, lunaraha liigutamise ja muude juhtumitega. Paraku saame selgust alles paari aasta pärast, mis toimub praegu nendes 8,5 korda kasvanud vahenduskanalites.

Võiks arvata, et ülaltoodu on kirjeldus 2018. aastast, kui avalikkusesse hakkas ilmuma Danske Bank A/S Eesti filiaali „lugu" aastatest 2007 – 2014 – see oli miski, mille mastaapsus ei olnud selle toimepanemise ajal teada. See ei ole ka eellugu sündmustele, mis järgnesid 2018. aasta uudistele, kus Eesti märgiti ära maailma suurima rahapesujuhtumi riigina, taheti osaliselt välja lõigata dollarimaksete võrgustikust ning riik kaitses ennast Euroopa Liidu rikkumise süüdistuses. Hiljem olid kõik tagantjärele targad, kuid tol hetkel ei olnud meil võlujõudu omavat klaaskuuli.

Virtuaalvääringu teenuse pakkujates toimuv on täielik *déjà-vu*. Pangandussektori asemel jutustab see lugu seekord virtuaalvääringu teenuse pakkujate sektorist. Dansket oli üks, aga virtuaalvääringu teenusepakkujaid oli meil 2021. aasta lõpu seisuga 381. Juba on avalikkuses teada Garantex Europe juhtum, kes omas Eestis tegevusluba 24. veebruarini 2022, kuid kelle kaudu liigutati rahvusvaheliselt tunnustatud ekspertor-

Pangandussektori asemel jutustab seekordne lugu virtuaalvääringu teenusepakkujate sektorist

ganisatsiooni andmetel 645 miljoni dollari ulatuses virtuaalvääringuid. Vara oli seotud eelkõige Venemaa kuritegevusega või rahakottidega, mida kurjategijad on kasutanud ebaseaduslikel eesmärkidel. Garantex Europe on tänaseks pandud Ameerika Ühendriikide sanktsioneeritud isikute nimekirja koos Eesti ettevõtte Izibits OÜ ning ühe Läti ja ühe Tšehhi ettevõttega. Kusjuures ka viimasel on seos Eestiga.

Eelnimetatud 381 ettevõtte hulgas on palju neid, kes ei tee riskantseid tehinguid või kelle kontrollisüsteemid on piisavad riskide juhtimiseks.

Valdava enamuse kohta seda paraku öelda ei saa. Just nemad on tulnud siia teenust osutama reeglitega, mille on ette valmistanud äriühinguteenuse pakkujad või juristid. Valdav enamus neist ettevõtetest ei ole kehtestatud reeglitega kunagi tutvunud ega ka lugenud seaduse nõudeid. Nad tegutsevad Eesti maine hinnaga, kuid ei ole kursis siinsete mängureeglitega või ei taha neid sisuliselt täita. Juhul, kui rahapesu või terrorismi rahastamise riskid realiseeruvad, on kannataja meist igaüks, mõjutades negatiivselt Eesti mainet, tehes Eesti residentidel välismaal finantsteenuse saamise raskemaks jne. Eestis ei ole kohta sellistel halbade kavatsustega teenusepakkujatel. Samuti ei ole Eestis kohta teenusepakkujatel, kes kasutavad siinset jurisdiktsiooni ebaseaduslikel eesmärkidel.

Need on põhjused, miks andmebüroo karmistas oluliselt virtuaalvääringu teenuse pakkumise tegevusloa saamise põhimõtteid ja hakkas süvendatult kontrollima litsentseeritud ettevõtete käitumist kaug- ja kohapealsete kontrollidega. Need on ka põhjused, miks Rahapesu Andmebüroo on järjest enam sunnitud käsutuskeeluga piirama virtuaalvääringu teenuse pakkujate vara, sest vastasel juhul jõuaksid need tagasi kurjategijateni. See on ka põhjus, miks näen kahte võimalust virtuaalvääringu teenuse pakkujate riskide maandamiseks. Teha „restart“, kus tegevusloa saavad kõik võrdsetel ja väga selgelt kontrollitud alustel. Või jätkata tavapärase järelevalvega, kus riskid realiseeruvad ja täna pannakse kuritegusid toime, kuid olukorra korrastamine ja normaliseerumine võtab aega aastakümneid. Viimase puhul peame ühiskonnana ära taluma täna realiseeruvad riskid ja tagajärjed, mis jõuavad avalikkuse ette aastate pärast. Seadusandja ei ole otsustanud „restardi“ kasuks, küll aga on ta karmistanud virtuaalvääringu teenuse pakkujatele esitatavaid nõudeid. Need on head sammud õiges suunas, kuid nende mõju saame vaadata alles järgmises aastaraamatus.

Andmebüroo jätkab oma tegevust mitte ainult virtuaalvääringu teenuse pakkujatega seotud juhtumite avastamise ja tõkestamisega, vaid täidab ka teisi talle seadusega pandud rolle.

Kõikidest nendest teemadest saabki aastaraamatust pikemalt lugeda. Esimene peatükk annab ülevaate rahapesu tõkestamise süsteemist Eestis ja sellest, kus me rahapesu ja terrorismi rahastamise riskide kontekstis täna oleme. Teine peatükk toob sektoripõhiselt välja ilmnenud riskipildi.

Ehkki ehitame uue põlvkonna rahapesu andmebürood, siis institutsionaalselt see oli, on ja jääb finantstehingute aususe valvajaks.

Head lugemist!

MATIS MÄEKER
Rahapesu Andmebüroo juht
Mais 2022

Aasta Eesti rahapesu ja terrorismi rahastamise tõkestamise süsteemis

2021. aastat võime nimetada inventuuriaastaks. Nii siseriiklikult kui ka rahvusvahelisel tasandil hinnati, kus me praegu oleme, ning seati sihid, kuidas ja kuhu edasi minnakse.

Julgelt võib öelda, et Eesti rahapesu ja terrorismi rahastamise tõkestamise süsteem on heas seisus. Teame, kus on riskid ja kes tahavad haavatavusi ära kasutada. Seda teemat selles peatükis pikemalt tutvustamegi. Ei ole juhus, et mitme teema all tuleb juttu virtuaalväärингu teenuse pakkujatest – mitmest küljest vaadatuna ongi tegemist Eesti Vabariigi kõige riskantsema sektoriga. Oleme neid riske märganud ning need hakkavad realiseeruma. Selle sektori tegemistest ja läbi nende kanalite toime pandud rahapesust ja terrorismi rahastamisest saame lugeda järgnevatel aastatel nii andmebüroo aastaraamatutest, teiste riikide tegevusaruannetest kui ka meediast.

2021. aasta ajajoonel

Jaanuar
- 1. jaanuaril sai Rahapesu Andmebüroost iseseisev valitsusasutus
- Hoo sai sisse Eesti-Ameerika koostööprojekt suurendamaks rahapesuga seotud teadmisi ja oskusi
- Avaldati Rahapesu Andmebüroo 2020. aasta väliskoostöö kokkuvõte
- Algasid ettevalmistused MONEYVALi hindamiseks

Märts
- Algas ELi IV direktiivi hindamine

Aprill
- Kinnitati riikliku riskihinnangu tulemused

Mai
- Langetati kohtuotsus, mis ei karistanud enesepesu

Juuni
- EL Nõukogu karmistas Valgevene sanktsioonirežiimi, mida täiendati ka aasta lõpus
- 14. juunil alustas Rahapesu Andmebüroo juhina tööd Matis Mäeker

August
- Rahapesu Andmebüroo piiras esimest korda teise riigi palvel krüptovara

September
- Algas Euroopa Nõukogu tehnilise abi projekt

Oktoober
- Kohus tõlgendas virtuaalvääringu teenusepakkuja asukohta formaalsusena
- Rahandusministeerium algatas rahapesu ja terrorismi rahastamise tõkestamise seaduse muutmise eelnõu

November
- Tühistati tegevusluba virtuaalvääringu teenuse pakkujal, kes osales finantskuritegudega seotud platvormi tegevuses
- Avaldati äriühinguteenuse pakkujate riskihinnang
- Valmistati ette kahtlaste tehingute juhendi muudatused terrorismi rahastamise tõkestamiseks

Detsember
- ELi taastefondi toel algasid ettevalmistused Rahapesu Andmebüroo strateegilise analüüsi võimekuse tõstmiseks

- Alustati üheksa täiendava järelevalvega virtuaalvääringu teenuse pakkujate seas
- Anti välja esimene tegevusluba virtuaalvääringu teenuse pakkumiseks peale andmebüroo uue juhi ametisse astumist
- Valmis virtuaalvääringu teenuse pakkujate teine riskihinnang
- Kinnitati Rahapesu Andmebüroo strateegia aastani 2026

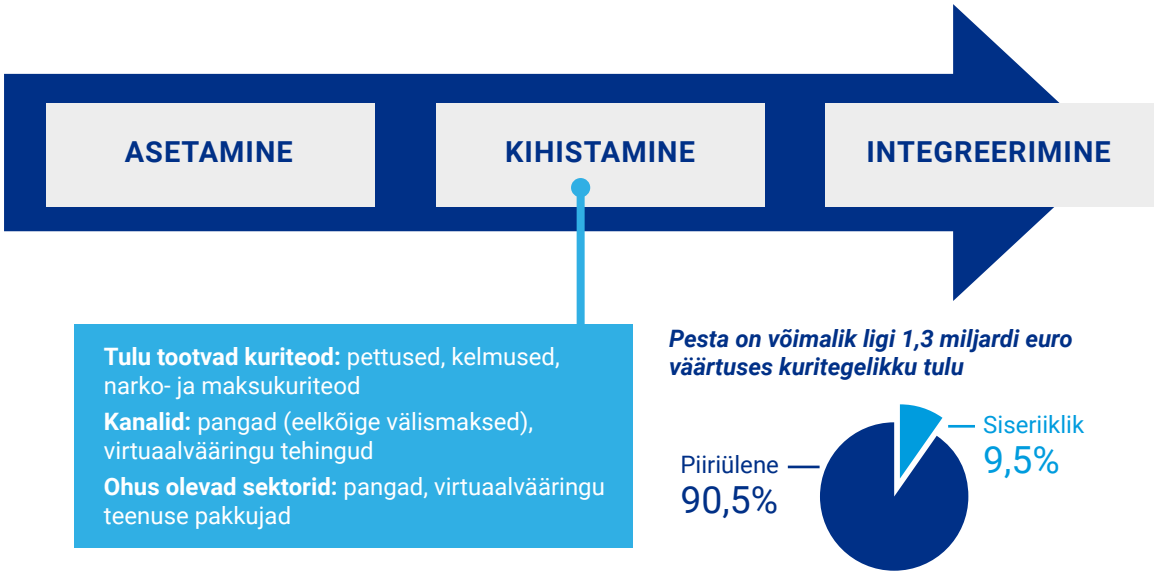
Andmebüroo ülesanne on koguda, analüüsida ja vajadusel jagada finantsluureteavet, et ennetada ja tõkestada Eesti Vabariigi rahandussüsteemi ning majandusruumi kasutamist rahapesuks, terrorismi rahastamiseks ja finantssanktsioonidest kõrvalehoidmiseks.

Rahapesu tõkestamine

Rahapesu ja terrorismi rahastamise tõkestamise töös on väga oluline suurem riskipilt, kuhu panustavad Rahapesu Andmebüroo igapäevase töö ja riskianalüüsidega, riiklik riskihinnang ning siseriikliku koostöö raames valminud riskide hindamise dokumendid, samuti koostöö välisriikidega ja selle pinnalt koostatav riskipilt. Neid riskipilte ja nii siseriikliku kui ka rahvusvahelise koostöö eredamaid momente hakkamegi järgnevalt kirjeldama.

Võttes arvesse eelnimetatud hinnangute alusel koostatud ohtude ja haavatavuste analüüsi, on 2021. aasta rahapesurisk Eestis keskmisel tasemel.

Rahapesuriski tase Eestis 2021: KESKMINE



Nagu andmebüroo varasemad analüüsid näitasid ning kinnitas ka riiklik riskihinnang, on rahapesu toimepanemise risk kõige suurem finants- ja finantstehnoloogia sektoris. Kiiresti areneva *fintech* maailma üks osa, virtuaalvääringud, on digitaalselt rahaliselt mõõdetava väärtuse liigutamiseks esmapilgul piisavalt anonüümne, et see pakuks huvi ka kurjategijatele. Varasemad rahapesu ja terrorismi rahastamise tõkestamise seaduse redaktsioonid tõid kaasa Eestis väljastatava tegevusloa taotlemise suure huvi virtuaalvääringu teenuse pakkumiseks ning kogu maailma mastaabis virtuaalvääringu teenusepakkujate Eestisse koondumise koos sektori riskidega.

Ohukohaks on välisriigis toime pandud eelkuriteost pärinevate vahendite kihistamine Eestis. Selleks kasutatakse isikuid, kes lubavad kasutada äriühingute või füüsiliste isikute arvelduskontosid, mille kaudu liigutatakse kuritegelik tulu Eesti finantssüsteemi, või kes võtavad sularaha välja ning annavad selle kurjategijatele tagasi.

Ohukohaks on välisriigis toime pandud eelkuriteost pärinevate vahendite kihistamine Eestis.

Teatamine

RAHAPESU ANDMEBÜROO SAI ENAM KUI 16 000 TEADET, SH

ligi
14 500
kahtlusel põhinevat teadet

9860
kelmusega seotud teadet

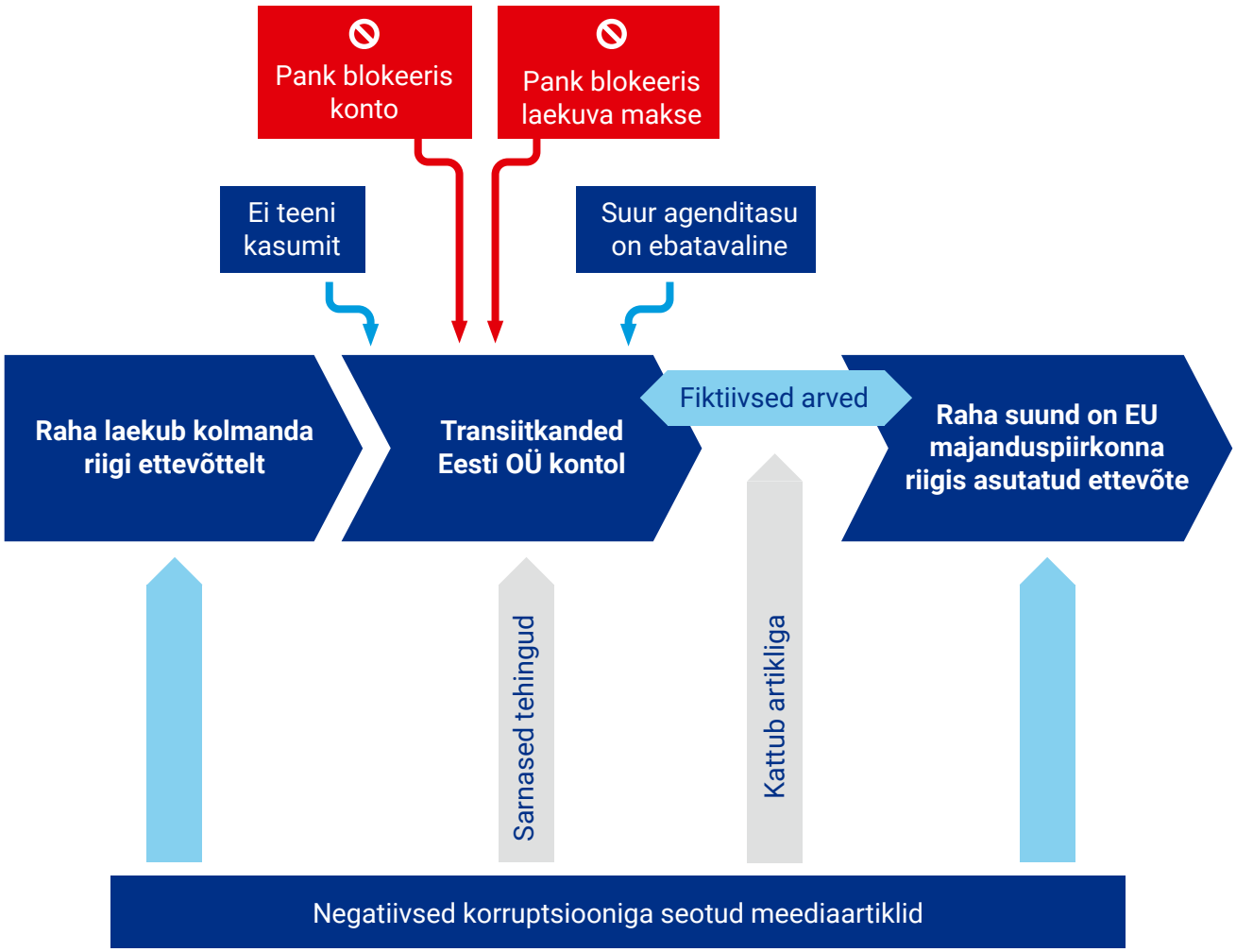
andis
543
teatele operatiivselt tagasisidet

Andmebüroole saadetud teadete koguarv ületas 16 000 teate piiri, mis tähendab, et nende hulk kahekordistus võrreldes 2021. aastat eelneva aastaga. Sellist teadete hüppelist kasvu on andmebüroo näinud varem 2000. aastate lõpus, kui rakendus summapõhine teatamiskohustus. Nüüd oli põhjuseks aga hoopis kelmusega seotud teadete ligi 6-kordne aastane kasv.
Andmebüroo seadis üheks eesmärgiks teatamiskohustuse tõhustamise kõikides sektorites. 2021. aasta lõpus ja 2022. aasta esimestel kuudel korraldati 21 koolitust kõikide sektorite esindajatele. Koolitustel käsitleti sektorite rahapesu ja terrorismi rahastamise riske, trende ning laiemalt ka tüpoloogiaid. Kui teate esitaja on teadlik oma tegevusvaldkonna suuremast riskipildist, oskab ta olulisi detaile ka teates kirjeldada. Koolitused võeti hästi vastu. Katusorganisatsioonid panustasid info levitamisse ning COVID-19 pandeemia tõttu toimusid webinarid virtuaalselt, mille positiivseks küljeks oli osalejate ootamatu rohkus – mõnel koolitusel tõusis osalejate arv üle 230. Koolitused ja kohtumised siht- ja huvigruppidega päädisid näiteks virtuaalvääringu teenuse pakkujate tehtud 1865 teatega kahtlastest tehingutest, mida oli 3,5 korda rohkem kui aasta varem.

Eesmärgiga tõhustada märgatavalt teatamise kvaliteeti, andis andmebüroo teate esitajale senisest enam otse ja operatiivset tagasisidet ning ka jätkab selle praktikaga. Teadetega seotud suhtluse käigus selgus ka muid kitsaskohti virtuaalvääringu teenuse osutamisel seoses rahapesu ja terrorismi rahastamise tõkestamisega, millest osa on koostöös kohustatud isikuga suudetud juba ka lahendada.

Üldiselt on teabe kvaliteet ja klientide teatamiskohustusega seotud hoolsusmeetmete kohaldamine paranemise trendis, kuid mitmes aspektis endiselt oluliste puudustega. Teadete hea sisu ja kvaliteet loob aluse rahapesu juhtumite avastamiseks ning panustab sektoripõhiste riskide, trendide ja tüpoloogiate täpsustamisse. Kahtlaste tehingute teadete allika kaitse on andmebüroo üks tähtsamaid tööpõhimõtteid, mistõttu aasta parima teate puhul saame pangale viidata üldistatult.

2021. aasta teatamise parima praktika näide tuli pangandussektorist



1. Pank on kursis meedias ilmunud negatiivsete artiklitega oma kliendist, kes on Eesti osaühing
2. Märgatakse raha laekumist kolmanda riigi ettevõttelt
3. Toimuvad sarnased tehingud, transiitkanded kahele ettevõttele Euroopa Majanduspiirkonnas
4. Pank tuvastab, et kontol toimuvad tehingud on väga sarnased meediaartiklites kirjeldatuga
5. Eesti osaühing samal ajal kasumit ei teeni, kuid rakendab ebatavaliselt suurt agenditasu
6. Pank blokeerib konto ja sinna laekuva makse
7. Tuvastatakse fiktiivsed arved Eesti osaühingu ja Euroopa Majanduspiirkonna ettevõtte vahel
8. Juhtunu kohta tehakse Rahapesu Andmebüroole õigeaegne teade, lisades selgelt struktureeritult kõik vajalikud seosed ja kahtlused
9. Pank hoiab oma sisemistest protseduuridest lähtudes varasid blokeeringu all, kuni andmebüroolt saabub vara käsutuspiirangu ettekirjutus

Antud juhul näitas panga proaktiivne tegevus, et kohustatud isikud on teadlikud oma õigustest ja kohustustest rahapesu ja terrorismi rahastamise tõkestamisel ega karda neile antud vahendeid ja tööriistu kasutada täies ulatuses. Sellise hoolsuskohustuse täitmise tulemusena on andmebüroo suutnud peatada ka võimaliku kuritegelikul teel saadud vara kihistamise kõrge riskiga virtuaalvääringutesse ning suutnud piirata ka virtuaalvääringu rahakotis olevaid kuriteokahtlusega varasid.

Siseriiklik ametkondlik koostöö

2021. AASTAL RAHAPESU ANDMEBÜROO

avas
196
juhtumianalüüsi toimikut,

mis olid seotud
1599
teatega

tegi
287
kuriteoteadet või teabeedastust uurimisasutustele

2021. aastal keskenduti andmebüroo juhtumianalüüsis organiseeritud kuritegevusele. Sellest oli tingitud pidev koostöö, sh andmevahetus, kohtumised ja igapäevane suhtlus Politsei- ja Piirivalveametiga. Fookuses olid Rahapesu Andmebüroo ja finantsluureteabe analüüsi vaatest erinevad Eesti organiseeritud kuritegelikud grupid ja tegutsemismeetodid. Lisaks saavutatud tulemustele võimaldas kahe asutuse menetluslike üksuste koostöö jagada ekspertteadmisi ning seeläbi tugevdada mõlema asutuse ametnike analüüsi- ja menetlusoskusi.

Hea näide asutuste vahel info kiirest liikumisest ja operatiivsest koostööst on ka juhtum, kus maksu- ja tolliamet teavitas andmebürood piiril kinni peetud kahtlasest kaubast ja sellega seonduvast võimalikust rahapesukahtlusest. Lisaks sellele, et mõlemad asutused alustasid oma töölõikudes menetlusi ja toiminguid, toimus juba loetud päevade järel ka täiendav operatiivne koostöökohtumine. Arutati juhtumi ja sellega seotud isikute tausta, erinevate tegutsemismeetodite võimalikke eesmärke ja hüpoteese ning lepiti kokku mõlema asutuse edasised ülesanded ja olulisemad koostööpunktid, et tulevikus sarnaseid skeeme tõhusalt avastada.

Andmebüroo edastatud materjalide arv uurimisasutustele jäi eelnevale aastale alla muu hulgas seoses suurte pankade rahapesumenetluste jõudmisega faasi, kus andmebüroo sisend menetlustesse oli juba suuresti antud.

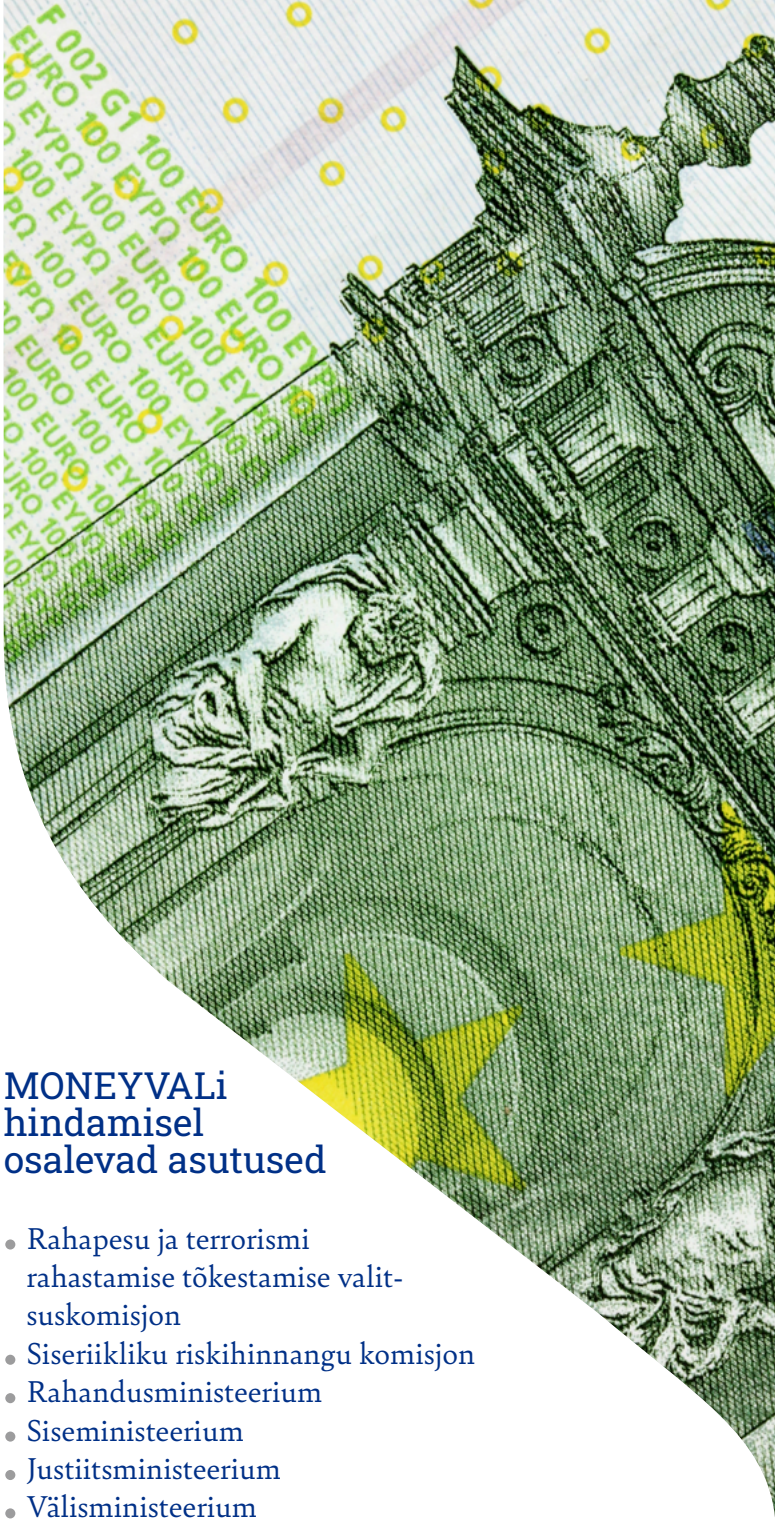
Korralik ametkondade vaheline koostööharjutus oli ka kevadel lõpule jõudnud rahapesu ja terrorismi rahastamise tõkestamise teise siseriikliku riskihinnangu koostamine. Sellesse panustas ligi 80 spetsialisti avalikust ja erasektorist. Andmebüroo toetas finantsluureteabe kompetentsiga kõiki 10 töögruppi, juhtides neist mitut ka ise. Valdkonna valitsuskomisjon kinnitas riskihinnangu aruande 28. aprillil 2021[1], ent sellega riigiasutuste töö ei lõppenud. Sektoripõhised teadmised riskidest viidi järgnenud koolitustega erasektorini ning tõsteti teadlikkust ka avalikus sektoris. Töö jätkus vastavalt riskihinnangu osaks olevale tegevuskavale, mille elluviimine aitab ületada välja toodud kitsaskohti.

Ettevalmistused MONEYVALi hindamiseks

2022. aasta kevadel ootas Eestit ees Euroopa Nõukogu rahapesu ja terrorismi rahastamise vastase võitlusega tegeleva ekspertkomitee MONEYVAL hindamine. Selliste hindamiste tsüklid leiavad aset ligikaudu iga seitsme aasta tagant. Sel korral on hindamise fookus efektiivsusel ehk tulemuslikkusel: kuidas Eesti rakendab seadusi ja regulatsioone praktikas ellu ja milline on Eesti asutuste tegelik võimekus tõkestada rahapesu ja terrorismi rahastamist. Eesti riigiasutused pidid oma töö tulemuslikkuse näitamiseks osalema kahe nädala vältel ligi 80 kohtumisel ning koostama vastuseid, mille mahud ulatuvad kuni 5000 leheküljeni.

Andmebüroos algasid laiaulatuslikumad ettevalmistused MONEYVALi hindamiseks 2021. aasta keskpaigas. Lisaks tehnilise vastavuse ja efektiivsuse küsimustike täitmisele, mis on oluline osa hindamisest, korraldas andmebüroo osana hindamiseks valmistumiseks ka koolitusi oma töötajatele, teistele õiguskaitseasutuste esindajatele ning abistas riiki tervikuna hindamisel võimalikult parima tulemuse saamisel. Koolituste lektorid olid maailmatasemel rahapesu ja terrorismi rahastamise tõkestamise hindamiste eksperdid.

Hindamise lõplikke järeldusi on oodata 2023. aasta alguses. Töö sellega ei lõppe, sest hindamise tulemusel annab MONEYVAL Eestile lugematuid soovitusi oma süsteemide parandamiseks ja tõhustamiseks. Eesti on tuvastanud osa puudustest ka riikliku ohuhinnangu koostamisel ning on koostanud nende maandamiseks tööplaani, kus tähtajad ulatuvad 2024. aastasse.



MONEYVALi hindamisel osalevad asutused

- Rahapesu ja terrorismi rahastamise tõkestamise valitsuskomisjon
- Siseriikliku riskihinnangu komisjon
- Rahandusministeerium
- Siseministeerium
- Justiitsministeerium
- Välisministeerium
- Rahapesu Andmebüroo
- Finantsinspektsioon
- Politsei- ja Piirivalveamet
- Maksu- ja Tolliamet
- Kaitsepolitseiamet
- Riigi Infosüsteemi Amet
- Prokuratuur
- Kohtunikud
- Notarite Koda
- Advokatuur
- Ettevõtluse Arendamise Sihtasutuse e-residentsuse programm
- Valitud turuosalised, sh suuremad pangad ja virtuaalvääringu teenuse pakkujad, vabaühendused, nende katusorganisatsioonid

Rahvusvaheline koostöö

RAHAPESU ANDMEBÜROO SAI

673

VÄLISPÄRINGUT JA SPONTAANSET INFOEDASTUST,

millest

107

puudutas virtuaalvääringu teenuse pakkujaid

ligi

1/3 puudutas Eesti ettevõtteid, kelle pangakontod ja rahapesu tunnustega tehingud olid välisriigis

ligi

1/3 on seotud Eesti krediidiasutustes avatud korrespondentkontodega

TEGI

222

VÄLISPÄRINGUT JA SPONTAANSET INFOEDASTUST,

sh

54

Eesti õiguskaitseasutuse palvel

2021. aastal toimus märgiline nihe teiste riikide rahapesu andmebüroode ja õiguskaitseasutuste esitatud päringute iseloomus. Üha rohkem küsitakse infot Eesti tegevusloaga virtuaalvääringu teenuse pakkujate vahendatud tehingute kohta.

Eelmisesse aastasse jäi ka juhtum, kus Rahapesu Andmebüroo seadis teise riigi palvel esmakordselt piirangu krüptovarade liikumisele. Virtuaalvääringu teenusepakkujatega seotud välispäringud – hõlmates kuritegusid kelmustest narkokuritegevuse, lapsporno ja mõrvade tellimiseni – seonduvad paari aasta taguse ajaga, kus virtuaalvääringu teenuse pakkujate teenuste käive oli tänasega võrreldes kaheksa korda väiksem.

Teades seda ning virtuaalvääringu teenusepakkujate klientide geograafiat ja tehingusuundade riskantsust prognoosime, et tulevikus kasvab välispäringute arv veelgi. Kui andmebüroo näeb kuritegusid sageli alles paari aasta möödudes alates nende toimepanemisest, siis avalikkuse ette jõuavad need vahel ligi viieaastase nihkega. Kuigi Eestiga otsene seos nende kuritegudega puudub, siis risk on kõrge, et kuritegelikel eesmärkidel võidakse ära kasutada Eesti tegevusloaga virtuaalvääringu teenuse pakkujaid. Leidub lugematul arvul foorumeid ja rahvusvaheliselt palju loetavaid veebilehekülgi, mis hoiatavad investoreid ja kliente Eesti teenusepakkujate eest. Eesti on ka üks väheseid riike, kelle virtuaalvääringu teenuse pakkuja on lisatud Ameerika Ühendriikide Rahandusministeeriumi (Office of Foreign Asset Control, OFAC) sanktsioonide nimekirja. Eestis kehtima hakanud karmistunud seadusandlus neid tänaseks juba toimepandud juhtumeid paraku ei muuda.

Seoses Eesti krediidiasutustes avatud korrespondentkontodega laekus endiselt väga palju päringuid – kokku 32% kogu sissetulevast välissuhtlusest. Tegemist on kontoga, mida kasutab teine finantsteenuse osutaja, tavapäraselt e-raha asutus, makseasutus või virtuaalvääringu teenuse pakkuja, kes kasutab kontosid enda klientide teenindamiseks. Need välispäringud olid peamiselt seotud teistes riikides toime pandud kelmustega.

Traditsiooniliste pangakontode kohta laekuvate välispäringute arv on langustrendis. Paljud neist puudutavad tehinguid aastatest 2012–2016 ning on seotud mitteresidentidest klientide teenindamisega.

Märkimisväärne osa, ligi kolmandik välispäringutest puudutas Eesti ettevõtteid, kelle pangakontod asuvad välisriigis ja rahapesu tunnustega tehingud on toimunud väljaspool Eestit. Ka enamikul Eesti tegevusloaga virtuaalvääringu teenuse pakkujatest on pangakontod välisriikides, mitte Eestis. Põhjus võib peituda muu hulgas ka selles, et 44 % virtuaalvääringu teenuse pakkujatest on seotud isikute hulgas vähemalt üks endine või praegune e-resident[II].

Andmebüroo ise esitas 2021. aastal 222 välispäringut ja spontaanset infoedastust. Eesti õiguskaitseasutuste palvel tehti 54 välispäringut, millest kaks puudutas terrorismi rahastamist. Politsei- ja Piirivalveameti taotlusel tehti päringuid mitmes suures rahapesu kriminaalasjas. Vähenes nende taotluste alusel tehtavate päringute maht, kus tegemist oli kelmuste üksikjuhtumitega.

Kõige rohkem tegime 2021. aastal koostööd Ukraina, Venemaa, Läti, Leedu, Soome, Hollandi, Luksemburgi, Prantsusmaa, Suurbritannia, Hispaania, Saksamaa, Poola, Sloveenia, Rumeenia ja Malta rahapesu andmebüroodega. Nendest üheksa andsid Eesti andmebüroole tagasisidet, hinnates koostööd kõrge 9-pallise hinnanguga 10-pallisel skaalal. Välja toodi nii vastuste kiirust kui ka edastatud andmete täielikkust. Märgiti ka, et enamik Eesti andmebüroo päringute põhjal koostatud raportitest vajasid edastamist riigisiseselt asjassepuutuvatele asutustele.

2019. aastal alustas Egmont Grupi töögrupp Saksamaa rahapesu andmebüroo juhtimisel rahvusvahelist projekti *Conclusions from Large Scale Cross-Border Money Laundering Schemes*, kuhu panustab aktiivselt ka Eesti Rahapesu Andmebüroo. Projekti eesmärk on ühendada riikide rahapesu andmebüroode teadmised ja praktika piiriüleste rahapesuvoogude võrgustike ja mustrite tuvastamiseks ning andmete analüüsimiseks. Lisaks töötatakse välja indikaatoreid, tüpoloogiaid, näidisjuhtumeid ja muid vahendeid, millega hõlbustada rahapesu tõkestamist. 2021. aastasse planeeritud projekti lõppu pikendati 2022. aastani eesmärgiga kaasata kahtlaste tehingute indikaatorite rakendamisse ja testimisse vastavate riikide krediidiasutused.

Andmebüroo kaasas projekti suurimad Eestis tegutsevad krediidiasutused. Testimise tulemustest koostati väärtuslik tagasiside, mis edastati edasiseks analüüsiks Saksamaa rahapesu andmebüroole.

Rahapesu Andmebüroo erinevate üksuste juhid osalevad ELi *FIU Platform* töös, mille eesmärkide hulgas on koordineerida rahapesu andmebüroode koostööd omavahel ELis ja teiste partnerorganisatsioonidega nii operatiivsel kui ka strateegilisel tasandil. Üksuse ülesandeks on nõustada ka Euroopa Komisjoni tegevust rahapesu andmebüroode tegevusvaldkonda puudutavates küsimustes.

Rahvusvahelisi standardeid loovas FATFis (*Financial Action Task Force*) on andmebüroo juht Matis Mäeker virtuaalvääringu teenusepakkujate eritöögrupi vaatleja ning rahvusvahelise koostöö ülevaatamise töögrupi liige.

Viimase ülesanne on hinnata ja teha ettepanekuid, kas teatud tunnustele vastavaid riike lisada nn halli nimekirja või kas seal olev riik tuleks nimekirjast eemaldada.

Osalemine rahvusvaheliste standardite täitmist hindavas Euroopa Nõukogu eksperdikomitees MONEYVAL viis andmebüroo ühe teenistuja hindama Lichtensteini rahapesu, finantssanktsioonidest kõrvalehoidmise ja massihävitusrelvade rahastamise tõkestamist. Andmebüroo juht Matis Mäeker on MONEYVALi tööd juhtiva büroo liige ning samuti Eesti delegatsiooni liige, kes osaleb nimetatud komitee töös.

ELi Coordination and Support Mechanism töögrupis osales andmebüroo teenistuja diskussioonides uue ELi rahapesu ja terrorismi rahastamise järelevalveasutuse loomise, selle õigusliku raamistiku ning asjasse puutuvates tehnilistes detailides ja rakendusküsimustes. Töögrupi tegevus algas 2020. aastal ning see jätkub.

Piiriülene juhtum

2021. aasta lõpus jõudis avalikkuse ette juhtum, kus Eestis 2013. aastal üles ostetud osaühingu kaudu liigutati kuni 2019. aastani ebaseaduslikult Ukraina dokumenditehasega seotud kümneid miljoneid eurosid.

Andmebüroo avas juhtumi toimiku 2018. aastal. Järgnes pikalt väldanud analüüs ja rahvusvaheline suhtlus, et selgitada välja seotud juriidilised ja füüsilised isikud, tehingupartnerid ja kahtlased tehingud nendega ning teised asjasse puutuvad juhatuse liikmed, omanikud ja tegelikud kasusaajad.

Andmebüroo analüüs päädis kuriteoteate edastamisega Politsei- ja Piirivalveametile 5. oktoobril 2020. Nädal hiljem alustati kriminaalmenetlust rahapesu tunnustel.

Muudatused õigusloomes

2021. aastal algatas rahandusministeerium rahapesu ja terrorismi tõkestamise seaduse muutmise eelnõu. Eelnõu väljatöötamise vajaduse tingis peaasjalikult aastatel 2019–2021 läbiviidud rahapesu, terrorismi rahastamist ja massihävitusrelvade leviku rahastamist käsitlev riiklik riskihinnang.

Riskihinnangu tulemusel selgus, et riske maandavaid tegevusi on vaja teha mitmes sektoris, sh kõrge riskiga virtuaalvääringu teenuse pakkujate, äriühinguteenuse pakkujate ja mittetulundusühingute puhul.

Virtuaalvääringu teenuse pakkujatele sätestati rahvusvahelisele standardile vastavad nõuded. Peamiselt toetuti standardiseadja FATF (*Financial Action Task Force*) soovitustele. Ajakriitiliste probleemide lahendamiseks tugevdati andmebüroo pädevust virtuaalvääringute teenuste loamenetluses ja järelevalve tegemisel. Eelnõu tagasisideringi läbimist huvigruppide ja turuosaliste seas saatis meediakära. Ühelt poolt üllatas avalikkust, kui suure riski on Eesti endale võtnud teenusepakkujate liberaalse litsentseerimisega. Teiselt poolt laiendas avalik debatt ekslikult seaduse nõuete karmistamist kogu krüptorahaga seotud ettevõtlusele, sh virtuaalvääringu rahakotihoidjatele, vahetajatele, emiteerijatele ja edastajatele.

Seadusemuudatus võeti Riigikogus vastu 23. veebruaril ning see jõustus 15. märtsil 2022.

Suurimad muudatused virtuaalvääringute teenuse pakkujatele

Suurimad seadusemuudatused, millega tuleb tegutsevatel turuosalisel end kooskõlla viia ning uutel virtuaalvääringu tegevusluba taotleda soovijatel arvestada:

- Virtuaalvääringutega tehtavatele tehingutele kohaldati nn „travel rule“ nõuet. Selle kohaselt peavad teenusepakkujad lisama ülekannetele sisuliselt samaväärse informatsiooni, mis käib kaasas pankade ja maksevahendajate kaudu rahaliste vahendite ülekandmisel.
- Teenusepakkuja aktsia- või osakapitali nõue tõusis 250 000 või 100 000 euroni, sõltuvalt pakutavast teenusest, ning ette nähti nõuded omavahenditele.
- Kehtestati välisauditi ja sõnastati selgesõnalisemalt sisekontrolli kohustus.
- Tegevuskoht peab võimaldama virtuaalvääringu teenuse pakkumist. Asu- või tegevuskoha kaudu peab olema igal ajal võimalik tagada järelevalve- või uurimisasutuse esindajale juurdepääs kogutavatele ja säilitatavatele andmetele.
- Juhatuse liige ei või olla enama kui kahe virtuaalvääringu teenuse pakkuja juhatuse liikme ametikohal ning kontaktisik ei või olla teise virtuaalvääringu teenuse pakkuja kontaktisik või struktuuriüksuse juht.
- Tegevusloa taotlemise eest tasutav riigilõiv tõusis 3300 eurolt 10 000 euroni. Lisandus riigilõiv tegevusloa muutmise eest.

Virtuaalvääringu teenuse pakkujatele sätestati rahvusvahelisele standardile vastavad nõuded.

Kohtupraktika

2021. aastal jõustus Eestis neli rahapesuga seotud kohtuotsust: kaks maakohtu otsust ja kaks ringkonnakohtu otsust.

Jõustunud otsuste alusel mõisteti rahapesu toimepanemises süüdi 11 ja õigeks kaks inimest. Kahel juhul oli rahapesu eelkuriteoks kelmus ning ühel juhul arvutikelmus, ühes kohtuasjas mõisteti kõik süüdistuse saanud isikud rahapesus õigeks. Otsuste kohaselt konfiskeeriti kokku ligikaudu 116 000 eurot ja asenduskonfiskeerimist kohaldati üle 18 000 euro. Lisaks konfiskeeriti üks mobiiltelefon ja korteriomand.

Tallinna Ringkonnakohtu 13.05.2021 lahendiga mõisteti rahapesusüüdistuses õigeks kaks isikut, kellest üks mõisteti sama otsuse alusel süüdi arvutikuritegude ettevalmistamises, arvutikelmuses ja ebaseaduslikult arvutisüsteemide kasutamises. Talle määrati neljaaastane liitvangistus. See lahend on märgiline seoses rahapesusüüdistuses õigeks mõistmisega. Järelduste kohaselt on enesepesu ehk ise-rahapesu (inglise keeles *self-laundering*) Eestis karistatav piiratud juhtudel. Täpsemalt leidis kohus, et juhtudel, kus ei ole selgelt tuvastatav isiku soov raha kuritegeliku päritolu varjamiseks, ei saa isikut rahapesus süüdi mõista. Vaatame seda kaasust lähemalt.

Kohtuasi 1-18-8474

Isikule oli esitatud süüdistus grupiviisilises suureulatuslikus rahapesus. Süüdistatu oli kandud kuritegeliku päritoluga krüptoraha üle oma isale, samuti anonüümsetesse virtuaalrahakottidesse ning värvanud kolm inimest, kelle pangakontosid kasutada raha väljavõtmiseks ning ülekannete tegemiseks. Ringkonnakohus leidis, et isik on teinud toiminguid rahaga, mis on hangitud arvutikelmuste ja hasartmängudega, krüptoraha kaevandades, investeerides või muul viisil, kuid tema teod ei liigitu klassikalise rahapesu alla. Kohtu hinnangul ei olnud tõendatud, et isikul oleks olnud soov raha kuritegelikku päritolu varjata – tema sooviks saab pidada raha kätte saamist tarbimiseks või anda teisele isikule kasutamiseks.

Rahapesu mõistet avava seaduse (RahaPTS § 4 lg 1 p-de 1 ja 3) osas tõi kohus välja, et isiku poolt teistele isikutele raha ülekandmise eesmärgiks oli raha sularahas enda kätte saamine, mitte aga raha kuritegeliku päritolu varjamine. Kohus tõi lisaks välja, et ka anonüümsetesse virtuaalrahakottidesse ülekannete tegemisel pole võimalik tuvastada raha kuritegeliku päritolu varjamist kui primaarset eesmärki.

RahaPTS § 4 lg 1 p 2 osas leidis kohus, et see ei rakendu eelkuriteo sooritaja suhtes. Isik pani toime eelkuriteod, mistõttu ei kujuta võimalik tema poolt eelkuriteoga saadu omandamine, valdamine või kasutamine endast rahapesu.

Samas asjas leidis kohus, et isiku isa ei olnud toime pannud eelkuritegu, kuna kõnealuse normi kohaselt peab sellisel juhul isikule olema raha saamisel teada, et raha on kuritegelikku päritolu. Kuivõrd polnud tuvastatud, et isal oleks see teadmine olnud, ei saa kohtu hinnangul teda rahapesus süüdi tunnistada.

Nimetatud lahendile annavad oma hinnangu ka 2021. aastal alanud Euroopa Nõukogu eksperdikomitee MONEYVAL'i hindajad. On äärmiselt tõenäoline, et see toob kaasa vajaduse taaskord rahapesu mõistet täpsustada, arvestades Eestile siduvaid rahvusvahelisi standardeid ja konventsioone.

Halduskohtumenetlused

2021. aastal sai alguse 19 uut Rahapesu Andmebürooga seotud kohtuasja ning lõppes 18 varasemalt alanud kohtuasja. 2021. aastal alanud kohtuasjadest lõppes samal aastal kaks kohutuasja. Üks neist oli seotud vaidlusega, mis puudutas tegevusloa andmisest keeldumist valeandmete esitamise tõttu (kohtuvaidlus lõppes kompromissi sõlmimisega). Teine kohtuasi oli seotud andmebüroo taotlusega seada halduskohtu loal vara käsutamise piirang üheks aastaks, mille Tallinna Halduskohus rahuldas 1. detsembril 2021.

2021. aasta oktoobris tegi Tallinna Ringkonnakohus otsused kolmes virtuaalvääringute tegevuslubadega seonduvas vaidluses tegevuskoha osas (lahendid 3-20-1750, 3-20-1752 ja 3-20-1965). Kohtu hinnangul on fakti küsimus seadusest tulenev nõue, et virtuaalvääringu tegevusluba omava ettevõtja tegevuskoht peab olema Eestis, ning andmebürool ei ole õigust hinnata tegevusloa taotluste menetlemisel tegevuskoha sobivust virtuaalvääringu teenuse pakkumiseks. Kohus jõudis järeldusteni, et seadus ei sisalda Eestis asuva tegevuskoha osas erinõudeid, mistõttu ei ole välistatud ka mitme või mitmekümne virtuaalvääringu teenuse pakkuja tegutsemine samal büroopinnal. Antud vaidlused lõppesid Riigikohtus. Viimane ei olnud nõus andmebüroo kaebuseid menetlusse võtma vaatamata andmebüroo viidetele märkimisväärsetele rahapesu ja terrorismi rahastamise riskidele, mis kaasneksid, kui mitukümmend teenusepakkujat asuksid teenust pakkuma paarikümnelt ruutmeetrilt. Andmebüroo oli kohustatud tegevusloa taotlused uuesti läbi vaatama.

Kohtuvaidluste raames ilmnenud kitsaskohti märkas ka seadusandja. Rahapesu ja terrorismi rahastamise tõkestamise seaduse eelnõu menetlemisel lisati virtuaalvääringu teenuse pakkuja tegevuskohale kõrgendatud nõuded. Eelnõu seletuskirja kohaselt peab andmebüroo tegevuskoha puhul hindama igakordselt lisaks Eestis asumisele ka seda, kas on eluliselt usutav, et ettevõtja määratud tegevuskoht reaalselt võimaldab sealt virtuaalvääringu teenuse osutamist, seadusest tulenevate kohustuste täitmist ning järelevalve tegemist.

Enamus 2021. aastal alanud uutest vaidlustest on jätkuvalt seotud virtuaalvääringu teenuse pakkujate tegevuslubade andmisest keeldumise või tegevuslubade kehtetuks tunnistamisega. Üks pooleliolev menetlus on seotud kohtule esitatud taotlusega vara riigituludesse kandmiseks (RahaPTS § 57 lg 7 alusel). Üks pooleliolev menetlus on seotud andmebüroo ettekirjutuse alusel seatud piiranguga ning on tänaseks arenenud kriminaalmenetluseks, millega seati varale käsutuspiirang summas üle poole miljoni euro. Samal ajal, kui halduskohtus on pooleli vaidlus seoses andmebüroo ettekirjutuse õigusvastasuse tuvastamisega, on kõnealune juhtum arenenud kriminaalmenetluseks.

Kohtuvaidlustes ilmnenud kitsaskohti märkas ka seadusandja

Seoses rahvusvaheliste finantssanktsioonide rakendamisega on varasemates aastaraamatutes kajastamist leidnud vaidlused meediakontserniga Rossija Segodnja. Tallinna Ringkonnakohtu 31.03.2022 otsusega 3-20-2288 nõustus kohus halduskohtu järeldustega, et Rahapesu Andmebüroo on jätnud kaebaja taotlused erandi kohaldamiseks õiguspäraselt rahuldamata. Muu hulgas analüüsis Tallinna Ringkonnakohus oma otsuses ka MIA Rossiya Segodnya suhtes finantssanktsioonide kohaldamise õiguspärasust.

Kohus jõudis kokkuvõtvalt järelduseni, et Rossija Segodnja rahalised vahendid on määruse (EL) nr 269/2014 art 2 lg 1 alusel õigesti külmutatud, sest vastasel juhul võiksid need saada kaudselt kättesaadavaks D. Kiselyovile kui finantssanktsiooni subjektile.

Rahvusvaheline finantssanktsioon

RAHAPESU ANDMEBÜROOLE ESITATI 99 RAHVUSVAHELISE SANKTSIOONI TEADET, SH

24 juhul tuvastati, et tegemist on finantssanktsiooni subjektiga

5 juhul vahendid külmutati ja jäid külmutatuks peale andmebüroo kontrolli

11 juhul tehingutest keelduti, kuna muidu oleks tehtud vahendeid kättesaadavaks finantssanktsiooni subjektile või tehing oleks rikkunud finantssanktsiooni

1 juhul vahendid vabastati, kuna kohaldati erandit

Ülejäänud puhkudel teavitati varasematest kaasustest, kus meetmeid oli juba kohaldatud või tegemist oli küll finantssanktsiooni subjektiga, aga tehing ei rikkunud finantssanktsiooni.

Rahvusvaheline sanktsioon ei ole rahvusvahelises diplomaatias uudne mõiste. Esimene kinnitatud sanktsiooni kehtestamine oli aastal 432 eKr, kui Ateena impeerium keelas Megara kauplejad oma turuplatsidel, lämmatades sellega konkureeriva linnriigi majanduse. Kuid rahvusvahelise sanktsiooni rakendamine muutus aktiivsemaks alles 20. sajandil, esimese maailma sõja ajal. Rahvusvaheline sanktsioon jõudis Eesti ametiasutuste ja erasektori töölauale 2021. aasta suvel, seoses inimõiguste tõsiste rikkumiste eskaleerumisega Valgevenes ning kodanikuühiskonna, demokraatliku opositsiooni ja ajakirjanike vägivaldse represseerimisega. See kasvatas märgatavalt andmebüroole sanktsiooniteadete edastamist, kuid oli lapsemäng võrreldes töömahuga, mille tõid kaasa sanktsioonimeetmete kohaldamised seoses Venemaa sõjalise agressiooni algusega Ukrainas 24. veebruaril 2022.

2021. aastal esitati andmebüroole 99 rahvusvahelise sanktsiooni kahtluse või kohaldamise teadet, neist 81 esitasid krediidiasutused. Õiguspäraselt külmutati vahendeid 1078,94 euro ulatuses, millele lisandusid ressursside kättesaadavaks mitte tegemine ning luba erandiks (vaata Lisa 2021. aasta arvudes). 32 teadet olid seotud Valgevene sanktsioonirežiimiga. Võrdluseks, alates Venemaa sõjalise agressiooni algusega Ukrainas, laekus andmebüroole esimese kahe kuuga üle 200 teate.

Rahvusvahelise sanktsiooni verstapostid

1919 pärast I maailmasõda lepiti kokku õiguses seada kollektiivne embargo selle riigi suhtes, kes alustab sõda

1935 Itaalia ründab Etioopiat ja teised riigid lõpetasid Itaaliale laenu andmise ja kaupade importimise

1940 USA külmutab Norra ja Taani varad USA-s, et Saksamaa ei saaks ligi nendele varadele

1958 kehtestatakse USA embargo Kuuba suhtes

1960ndad ÜRO sanktsioonid saavad hoo sisse

2014 Venemaa vastased sanktsioonid seoses Krimmi annekteerimisega

2016 USA Magnitsky nimekiri inimõiguste rikkujatest

2022 sanktsioonid seoses Venemaa sõjalise agressiooniga Ukrainas

Seoses Valgevene sanktsioonidega anti välja üks erand. Antud kaasuses oli Eesti ettevõte lepingulistes suhetes Valgevene ettevõttega enne sanktsiooni kehtestamist. Pärast seda, kui Valgevene ettevõte lisati sanktsiooninimekirja, peatas Eesti krediidiasutus Eesti ettevõtte edastatava makse. Kuivõrd Eesti ettevõte oli sanktsioneeritud Valgevene ettevõttega loonud lepingulise suhte enne viimase lisamist sanktsiooninimekirja ja makse oli lepingust tulenev kohustus, andis andmebüroo selle makse osas loa erandiks ja loa makset teostada.

Finantssanktsiooni kohaldamine on Eestis iga juriidilise ja füüsilise isiku kohustus. Et rahvusvahelisi sanktsioone mitte rikkuda, tuleb Venemaa, Valgevene või Ukrainaga (eelkõige teatud Venemaa kontrolli all olevad piirkonnad Ukrainas) seotud ettevõtluse puhul selgitada oma koostööpartnerite tausta ning üle vaadata kõik teenused ja kaubad. Just füüsilistel ja juriidilistel isikutel on parim ülevaade oma partneritest, kaupadest ja teenustest, et hinnata, kas tegemist on finantssanktsiooni subjektiga, kohaldamise olukorraga või tehinguga, mis rikuks finantssanktsiooni.

Valgevene sanktsioonirežiimi muudeti järgnevalt:

- **4.06.2021** kehtestas EL keelu Valgevene lennuettevõtjatele ja ELi Nõukogu otsustas tugevdada kehtivaid piiravaid meetmeid seoses olukorraga Valgevenes, keelates kõigil Valgevene lennuettevõtjatel ELi õhuruumist üle lendamise ja pääsu ELi lennujaamadesse.
- **21.06.2021** võttis EL seoses jätkuvate repressioonidega ja 23. mail 2021 Ryanairi lennu maanduma sundimisega Minskis, vastu neljanda sanktsioonide paketi. Piiravad meetmed kehtestati 78 Valgevene isikule ja 8 üksusele. Lisaks kanti loetellu seitse isikut ja üks üksus, kellele kohaldatakse uusi piiravaid meetmeid – varade külmutamist ning ELi kodanikel ja ettevõtetel keelati teha neile kättesaadavaks rahalisi vahendeid.
- **15.11.2021** EL laiendas sanktsioone ning võttes arvesse olukorda ELi ja Valgevene piiril, muutis nõukogu oma sanktsioonirežiimi, et reageerida inimeste poliitilistel eesmärkidel ärakasutamisele Valgevene režiimi poolt.
- **2.12.2021** kehtestati viies sanktsioonide pakett seoses jätkuvate inimõiguste rikkumiste ja rändajate ärakasutamisega. Nõukogu kehtestas piiravad meetmed veel mitmele isikule ja üksusele. Meetmeid kohaldatakse kohtuvõimu silmapaistvatele esindajatele ja propagandaväljaannetele, kes aitavad kaasa kodanikuühiskonna, demokraatliku opositsiooni, sõltumatute meediaväljaannete ja ajakirjanike jätkuvale represseerimisele. Meetmeid kohaldatakse ka Valgevene presidendi Aleksandr Lukašenka režiimi kõrgete poliitilistele ametnikele, samuti ettevõtjatele (nt Belavia Airlines), reisikorraldajatele ja hotellidele, kes on aidanud õhutada ja korraldada ebaseaduslikke piiriületusi läbi Valgevene Euroopa Liitu. Sel viisil osaleti rände ärakasutamises poliitilistel eesmärkidel.

Kolm sammu, mida võiksid juriidilised ja füüsilised isikud järgida:

1. Määrake kindlaks äripartnerite riskitase, kui nad on seotud Venemaa, Valgevene ja Ukraina füüsiliste või juriidiliste isikutega.

- Kas on Venemaa, Ukraina või Valgevene asukoht või päritolu? Jälgige tähelepanelikult nende partnerite käitumise muutusi. Tuvastage hiljuti loodud suhteid kõrge riskiga sanktsioonide jurisdiktsioonist. Geograafilise riski olemasolu võib viidata keelatud tegevusele.
- Kui palju on tehinguid kõrge sanktsiooni riskiga riikidesse või nendest riikidest? Vaadake läbi suurenenud aktiivsus potentsiaalselt suurema riskiga geograafilistes piirkondades nagu Hiina, Araabia Ühendemiraadid, vabakaubanduspiirkonnad ning riigid, mis asuvad Venemaa, Valgevene ja Ukraina vahetus läheduses. Nende riikide kaudu võidakse varjata kauba tegelikku päritoluriiki või kauba lõppsihtriiki.

- Vaadake läbi varasem tegevus, et teha kindlaks partnerid, kes ei pruukinud enne nende kaasamist sanktsioone rikkuda, kuid nüüd rikuksid uusi sanktsioone. Veenduge, et tegevus ei korduks. Sanktsioon on ajas muutuv ja see, mis oli enne lubatud, ei pruugi uue kehtestatud sanktsiooniga enam nii olla.

- Kui palju partnereid on seotud tööstusharudega, mille osas on kehtestatud sanktsioone, näiteks põllumajandus, lennundus, ehitus, pangandus, sõjavägi/kaitse, kaevandamine, tekstiilitööstus, metallid/mineraalid, nafta/naftakeemia/energia, raudteed, laevandus, tehnoloogia, telekommunikatsioon, teadus- ja arendustegevus jne? Kui mõni partner on tegev piiranguga kaetud äritegevusega, tuleb veenduda, et piirang ei kehtiks riigi suhtes, kus teenust soovitakse osutada või kaupa müüa.

- Vaadake üle partnerid, kelle kasusaajad ei ole teada või kelle kasusaajaid on keeruline tuvastada. Kasusaaja varjamine on enam enamlevinud viise, kuidas sanktsioonist kõrvale hoida.

2. Kriitiliste andmete tuvastamine ja jälgimine

- Tehke teavitustööd oma ettevõttes, tuues välja sanktsiooniga kehtestatud piiranguid ja ohumärke. Looge protseduure, kuidas partnerite, teenuste ja kaupade osas teha sanktsiooni kontrolli.

- Kasutage kogu ettevõtet hõlmavaid andmeid ja avalikke andmebaase, kui riigi osas on juba risk tuvastatud.

- Tehke koostööd oma asutuse erinevate osakondadega, nt müügiosakond, raamatupidamine, logistika jne.

- Jagage ettevõtte sees infot sanktsioonide seisu ja meetmete kohta, mida tehakse sanktsioonide riski/kokkupuute leevendamiseks juhatuse ja kõrgema juhtkonnaga. Samuti kaaluge teadaannete kasutamist, et suhelda partneritega sanktsioonide, nende nõuete ja võimaliku mõju teemal.

- Tehke koostööd partnerinstitutsioonidega, et arutada parimaid tavasid, kogemusi, sanktsioonide tõlgendamist jne.

3. Raporteerimine

- Teavitage sanktsiooni kohaldamisest ametiasutusi, sh kui tehingust keeldutakse ehk ei tehta finantssanktsiooni subjektile kättesaadavaks rahalisi vahendeid ega ressursse.

- Olge kursis sanktsiooni uuendustega.

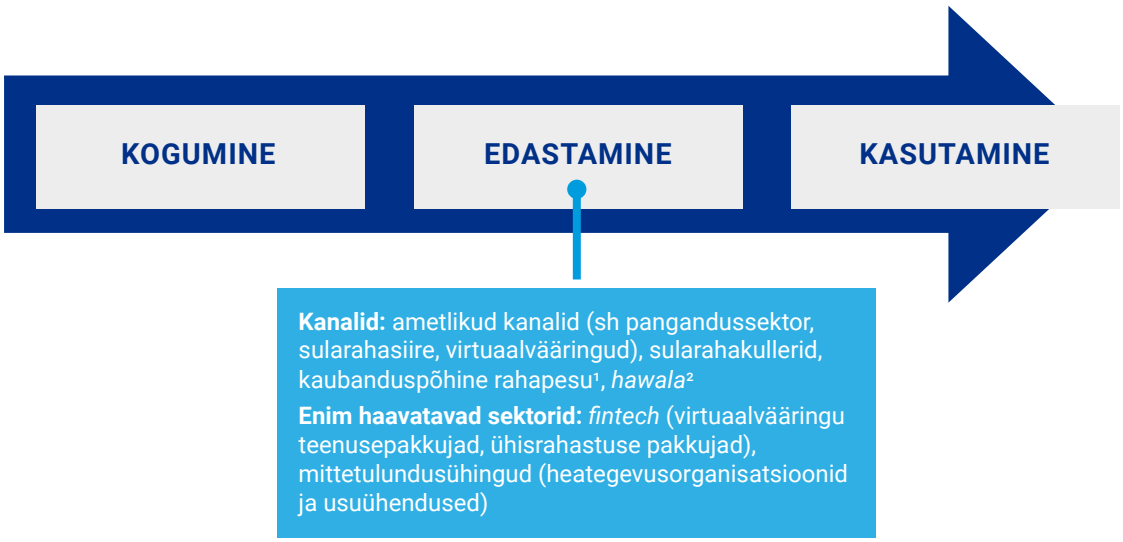
- Rahapesu Andmebüroo on välja andnud juhendeid, suuniseid ja abimaterjale, mis aitavad füüsilistel ja juriidilistel isikutel edukamalt tuvastada finantssanktsiooni subjekti, finantssanktsiooni rikkuvaid tehinguid, erandite küsimist ja teate tegemist. Materjalid on avaldatud andmebüroo kodulehel: fiu.ee/rahvusvahelised-sanktsioonid/venemaa-sojaline-agressioon-ukrainas. Kodulehel ja sotsiaalmeedias teavitatakse avalikest infotundidest finantsasutustele ja laiemalt teiste sektorite ettevõtetele.

Terrorismi rahastamise tõkestamine

Terrorismi rahastamise juures eristatakse tavapäraselt vahendite kogumise, edastamise ja kasutamise faasi. Eesti puhul on terrorismi rahastamise vaatest kõige suurema riskiga edastamise faas. Enamikes sektorites oli 2021. aastal terrorismi rahastamise riskitase madal. Siiski on virtuaalvääringute teenuse pakkujate sektor Eestis tervikuna põhjustanud viimaste aastate terrorismi rahastamise riskitaseme tõusu madalalt keskmisele.

Virtuaalvääringu teenusepakkujate sektor on haavatav eelkõige vahendite edastamise faasis. Sektori karakteristikutest, mis mõjutavad terrorismi rahastamise riski, saab lähemalt lugeda aastaraamatu teises pooles. Samuti on kõrge riskiga ehk keskmisest haavatavamad ka mittetulundusühingute sektor usuühenduste ja heategevusorganisatsioonide seas, seda eelkõige varade kogumise faasis.

Terrorismi rahastamise riskitase Eestis 2021: KESKMINE



Eestis on suurim terrorismi rahastamise risk sarnaselt ülejäänud Euroopaga olnud seotud islamiäärmuslusega. Nagu ka Kaitsepolitseiameti aastaraamatus märgitud, on Kaitsepolitseiamet koostöös Rahapesu Andmebürooga tuvastanud vähemalt viis islamiäärmuslikku isikut, kes on teinud tehinguid Eesti turuosaliste kaudu. Samuti on olnud üksikuid näiteid potentsiaalsest paremäärmusluse rahastamisest, mis on ka Eestis tõenäoliselt tõusuteel.

[1] Kaubanduspõhine rahapesu (TBML, *trade-based money laundering*) – kuritegeliku tulu varjamine ülepiiriliste kaubandustehingutega (arvel näidatakse valesti hinda, kogust, kvaliteeti, kauba nimetust või esitatakse topeltarveid). Erinevalt kaubanduspõhise rahapesuga seotud eelkuritegudest pole selle eesmärk mitte kauba, vaid võltsitud kaubandustehingute abil raha ja vahendite liigutamine, kasutades selleks nn professionaalseid rahapesijaid. Kaubanduspõhine terrorismi rahastamine (TBTF, *trade-based terrorist financing*) kasutab TBMLi võtteid, kuid olulise erinevusega – raha ja vahendid, mida edastatakse, võivad pärineda nii mittelegaalsest kui ka legaalsest allikast.

[2] *Hawala* – Lähis-Idas, Aafrikas ja Aasias levinud usaldusel põhinev traditsiooniline raha edastamise viis, kus raha ülekandmiseks ei pea seda füüsiliselt sihtkohta saatma. Raha asemel võidakse sihtriigis, kus toimib kogukonnasuhetele tuginev arveldussüsteem, aktsepteerida näiteks vallas- või kinnisvara.

2021. aastal esitati andmebüroole 303 terrorismi rahastamisele viitavat teadet. Seda on kolmandiku võrra rohkem kui aasta varem. Ehkki kohustatud isikute esitatud teadete kvaliteedis oli olulisi puudujääke, on iga terrorismi rahastamisele viitav teade tähtis. See võimaldab ühelt poolt pöörata ametiasutustel süvendatud tähelepanu potentsiaalsele terrorismi rahastamise juhtumile, teisalt täiendab esitatud teave finantsluure üldpilti, võimaldades panna eri allikate infokillud kokku kõnekaks mosaiigiks.

Terrorismi rahastamisele viitavaid teateid esitasid sektoritest kõige enam finantseerimisasutused. Virtuaalvääringu teenuse pakkujatelt aga tuli sektori suurust, mahtu ja kõrget riskitaset arvestades teateid ebaproportsionaalselt vähe. Murelikuks teeb ka see, et krediidiasutused esitasid terrorismi rahastamisele viitavaid teateid aasta jooksul vaid mõned korrad. Ühelt poolt on pankadel rahvusvaheliste skandaalide järel vähe kliente kõrgema terrorismi rahastamise riskiga riikidest. Teisalt võib napi teadete arvu taga olla madal teadlikkus riskidest ning vastavuskontrollisüsteemide nõrkus tuvastada terrorismi rahastamise stsenaariume. Ohumärk on ka see, et hasartmängukorraldajad ei esitanud erinevalt varasemast ainsatki terrorismi rahastamisele viitavat teadet.

Puudujäägid andmebüroole esitatud teadete kvaliteedis näitavad vajadust teadlikkuse tõstmise järele koolituste näol. Eesmärk on see, et turuosalised orienteeruksid terrorismi rahastamisele viitavates märkides, tunneksid ära terrorismi rahastamise indikaatoreid, kohaldaksid riskile vastavaid hoolsusmeetmeid ning oskaksid esitada piisava detailsusega teateid. Samuti osutab terrorismi rahastamise kahtlusega teadete madal kvaliteet teadete esitamise süsteemi keerukusele. Seetõttu asus andmebüroo ette valmistama süsteemimuudatusi.

Terrorismi rahastamise risk

SEOTUS RISKIRIIGIGA + RISKIINDIKAATOR

Esitada TFR-1 ehk terrorismi rahastamise riski teade

- Märkida teatesse kõik teadaolevad riskiindikaatorid
- Tehingut või toimingut võib jätkata, kui kohaldatakse tugevdatud hoolsusmeetmeid

Illustratiivne näide. Isik, kes ei tegele kaupade müügi ega teenuste osutamisega, saab regulaarselt ülekandeid kahest Euroopa riigist, kusjuures tehingu kirjelduses on ebamäärane selgitus. Kord kuus kannab isik saadud summa üle mittetulundusühingule, mis tegutseb kõrgema terrorismi rahastamise riskiga riigis. Kodulehekülje andmetel pakub mittetulundusühing abi orvuks jäänud põgenikele.

Terrorismi rahastamise kahtlus

KAHTLUSINDIKAATOR

Esitada TFR-2 ehk terrorismi rahastamise kahtluse teade

- Märkida teatesse kahtlusindikaator ja kõik teadaolevad riskiindikaatorid
- Tehing tuleb peatada kuni pädeva asutuse edasise juhiseni

Illustratiivne näide. Isik edastab ühisrahastuse platvormil kogutud summa organisatsioonile, mille kodulehekülje kutsutakse üles poliitilisele vägivallale. Ka muud avalikud allikad viitavad, et organisatsiooni liikmed toetavad vägivaldset äärmuslust.

Koostöös Kaitsepolitseiametiga valmistati ette kahtlaste tehingute tunnuste juhend, mis aitab ära tunda potentsiaalseid terrorismi rahastamise tehinguid[III]. Juhendis eristatakse kahte tüüpi terrorismi rahastamisele viitavaid teateid: TFR-1 ja TFR-2. Esimene neist eeldab tehingu osapoole seost riskiriigiga ja riskiindikaatorit. Teise puhul peab olema konkreetsele terrorismi rahastamise kahtlusele viitav asjaolu ehk kahtlusindikaator. Täiendati nii riski- kui ka kahtlusindikaatorite nimekirja. Teatamiskohustuse täitmise hõlbustamiseks on indikaatorite juures välja toodud valdkonnad, millega juhitakse muu hulgas tähelepanu sektoriaalsetele haavatavustele (sh virtuaalväärингu teenuse pakkujad ja vabaühendused).

Olulise muudatusena avalikustati juhendi lisana kõrgema terrorismi rahastamise riskiga riikide nimekiri. Nimekirja koostamisel võeti arvesse nii rahvusvaheliste organisatsioonide hinnanguid ja raporteid kooskõlas ametiasutuste ohuhinnangutega kui ka Eesti teenusepakkujate seniseid seoseid erinevate riikidega. Terrorismi rahastamise kõrgem risk ei tähenda, et konkreetne riik rahastab terrorismi, vaid see viitab riskile, mis võib asjaolude kokkulangemisel realiseeruda. Kõrgema riskiga terrorismi rahastamise riikide nimekirja hakatakse üle vaatama vähemalt kord aastas.

Alates 2021. aasta lõpust on andmebüroo tõstnud võimekust terrorismi rahastamise analüüsimisel ning see jätkub ka 2022. aastal. Eesmärk on Eesti riigi tõhus ja süsteemne terrorismi rahastamise tõkestamine, mille osaks on ka selge ja lihtne terrorismi rahastamisele viitavate teadete esitamise süsteem.

Rahapesu Andmebüroo

Rahapesu Andmebüroole oli 2021. aasta suurte muutuste ja väljakutsete aasta. 1. jaanuarist 2021 alustati iseseiseva asutusena rahandusministeeriumi haldusalas. Enne seda oli büroo alates oma loomisest, 1. juulil 1999, toonase politseiameti, hilisema politsei- ja piirivalveameti struktuuriüksus. See tähendas, et politsei-tüüpi rahapesu andmebüroost sai administratiivne andmebüroo, millel puudub kriminaalmenetluse läbiviimise õigus, kuid mis asub lähemal erasektorile, et tõhustada koostööd just nendega.

Iseseisval asutusel on suurem otsustusvabadus, millega kaasneb ka suurem vastutus. Pikalt kestnud juhi otsingu ajal täitis juhi kohuseid Marget Lundava. 14. juunil asus andmebüroo juhina tööle Matis Mäeker. Õigusteaduste taustaga juht pühendus rahapesuvastasele võitlusele ka eelneval 10 aastal, töötades finantsinspektsioonis ja mitme rahvusvahelise organisatsiooni juures.

Andmebüroo kasvas nii töötajate arvult kui ka seetõttu, et kasvasid avaliku ja erasektori ootused. Töötajaskonna kahekordistumine on igale organisatsioonile põnev ja väljakutseid esitav aeg. Valitsemisala vahetus tõi ka identiteediküsimusi, ent kannatlikkus, missioonitunne ja teotahtelisus on suured tugevused, mis aitavad andmebürool valitudsuunas edasi liikuda.

Andmebüroo tuumfunktsioonid säilisid: andmebüroole saadetud teadete vastuvõtmine, analüüs ja rahapesu või terrorismi rahastamise kahtluse korral kuriteokahtluse kohta info edastamine õiguskaitseasutustele, samuti strateegiline analüüs. Andmebüroole tuli üle ka maailma rahapesu andmebüroode seas unikaalne kohustus teostada järelevalvet teatud turuosaliste üle, sh neile tegevuslubade andmine. Küll aga pakkusid igale andmebüroo töötajale ja rollile väljakutseid siseriikliku riskihinnangu koostamine, Euroopa Komisjoni IV rahapesu tõkestamise direktiivi rakendamise efektiivsuse hindamine, MONEYVALi hindamiseks ettevalmistamine ning mitme rahvusvahelise projekti käivitamine.

Tänu sõlmitud koostöölepetele säilis andmebüroo ligipääs varasematele andmebaasidele, mis on väga oluline, et järjepidevalt täita büroole seatud eesmärke ja peamisi ülesandeid.

Järelevalve töös lähtuti riskipõhisest lähenemisest. Tuginedes loodud riskimaatriksile ja teenusepakkujatelt kaugkontrollide käigus saadud infole, seati fookus riskantsemate sektorite teenusepakkujatele, peamiselt virtuaalvääringu teenuse pakkujatele.

Peamised tegevusloa väljastamisest keeldumise või taotluste läbivaatamata jätmise põhjused on:

- vajalike dokumentide esitamata jätmine – näiteks karistusregistri tõend ei vasta nõuetele,

sise-eeskirjad ja riskihinnang ei vasta nõuetele;
- tegevusloa taotleja ei vasta kontrollieseme asjaoludele – ettevõttega seotud isikul, näiteks juhatuse liikmel või osanikul, puudub korrektne ärialane maine, kontaktisikul puuduvad teadmised ja pädevus enda ülesannete täitmiseks, virtuaalvääringu teenuse pakkuja juhatuse asukoht ei asu Eestis.

2020. aastal alanud sammud strateegilise analüüsi viimiseks uuele tasemele said 2021. aastal veelgi hoogu juurde. Avanenud ligipääs Eesti Panga ja finantsinspektsiooni andmetele võimaldas kombinatsioonis andmebüroos kasutusel olevate teiste andmeallikatega saada parem ülevaade riigi rahapesu ja terrorismi rahastamise riskidest. Neid riske analüüsiv meeskond kasvas. Avaldati riskihinnangud virtuaalvääringute teenuse pakkujate ja äriühingu teenuse pakkujate sektoritest, millest tuleb lähemalt juttu aastaraamatu teises pooles.

Andmebüroo strateegilise analüüsi võimekuse tõstmisse panustavad ka kolm rahvusvahelist projekti. Kolleegid Ameerika Ühendriikide Rahandusministeeriumist (*US Treasury*) aitavad Eesti rahapesu ja terrorismi rahastamise tõkestamise eest vastutavatel asutustel tõsta oskuste ja teadmiste taset. Ameeriklaste osalusel on esmakordselt tegemist rahapesu valdkonnas sedavõrd süsteemse ja mastaapse koostööprojektiga.

Andmebüroo on Euroopa Nõukogu tehnilise abi projektis sisujuhi rollis. Projekti käigus analüüsitakse Eesti õiguslikku keskkonda andmete aspektist ning koondatakse rahapesu andmebüroode parim strateegilise analüüsi praktika, mida võiks ja saaks ka Eestis üle võtta. Samuti panustab projekt andmebüroo järelevalve süsteemi arendamisse.

Euroopa Liidu taastefondist eraldati Eestile enam kui 3 miljonit eurot selleks, et arendada strateegilise analüüsi funktsiooni. Eesmärgiks on rahapesu ja terrorismi rahastamise tõkestamise valdkonnas üles ehitada maailma kontekstis silmapaistval tasemel strateegilise analüüsi süsteem. See tähendab uute tehniliste lahenduste kasutuselevõttu ning tööprotsesside tõhustamist uute analüütiliste toodete abil.

Infotehnoloogia ei ole ammu enam ainuüksi ärieesmärki toetav tugifunktsioon, vaid moodustab tuumvaldkonnaga tihedalt läbipõimunud terviku, et saavutada eesmärke ja finantsilist kasu. Seetõttu toimub infotehnoloogias pidev võidurelvastumine ning iseäranis selgelt on seda näha majandusele ja finantsidele lähemal seisvates valdkondades nii heade kui ka halbade kavatsustega. Usaldusliku finantsruumi tagamisel on oluline mõista sellise võidurelvastuse tagamaid ja ära tunda infotehnoloogia pidevast arendamisest tulenevate võimalustega kaasnevaid riske. Andmebüroo on valinud infotehnoloogia selgelt enda strateegilise eesmärgi täitmise üheks vahendiks. Ühest küljest on see paratamatu trend, teisalt oleme eelisolukorras tulenevalt Eesti IKT taristust ja kuvandist. Andmebüroo infosüsteemi viimaste aastate arendustel oli näiteks suur roll, et tulla toime teadete arvu hüppelise kasvuga. Et finantsvääringud ei tunnista riigipiire, suurendab ka andmebüroo finantsruumi usalduse tagamiseks oluliselt oma infotehnoloogia kompetentsi. Olgu selleks siis andmekaeve, masinõpe või virtuaalvääringute analüüs, läbivalt ka küberturvalisus. Infotehnoloogiast tulenevaid võimalusi kavandame senisest enam kasutada ka suhtlusel ja andmevahetusel teiste osapooltega. Suhtlus Rahapesu Andmebürooga peaks olema võimalikult lihtne, kahepoolne ning andmeedastus vigade vaba.

Rahapesu Andmebüroo on kasvav ja arenev organisatsioon, mis püüdleb dialoogi, innovatsiooni ja nähtavuse poole. Ambitsiooniks ei ole vähem ega rohkem, kui olla suunanäitajaks rahapesu ja terrorismi rahastamise riskide juhtimisel. Just need, esimesel tegevusaastal iseseisva valitsusasutusena võetud suunad kinnitati 2021. aasta lõpus andmebüroo strateegiliste eesmärkidena aastateks 2022–2026. Neid eesmärke saab andmebüroo täita vaid juhul, kui töötajad on oma ala eksperdid, kes orienteeruvad hästi nii oma töösse puutuvas kui ka vastava väliskeskkonna mõjutustes.

RAHAPESU ANDMEBÜROO STRATEEGIA 2022-2026

MISSIOON: Finantsluureteavet kogudes, analüüsides ja seda jagades tagada finantstehingute läbipaistvus ja ausus, et seeläbi ennetada ja tõkestada Eesti Vabariigi rahandussüsteemi ning majandusruumi kasutamist rahapesuks, terrorismi rahastamiseks ja finantssanktsioonidest kõrvalehoidmiseks.

STRATEEGILISED EESMÄRGID missiooni täitmiseks:

I. Olla Eesti Vabariigi rahapesu ja terrorismi rahastamise riskide analüüsi keskus ja suunaandja riskide juhtimiseks riigis. Selleks Rahapesu Andmebüroo:

- **A.** arendab välja strateegilise analüüsi võimekuse ja uuendab juhtumianalüüsi võimekust;
- **B.** käivitab asjakohased analüüsid ja viib olemasolevad uuele tasemele;
- **C.** loob efektiivsuse mõõdikud riskide ja kontrollimeetmete järjepidevaks hindamiseks ning muutuste kiireks kaardistamiseks;
- **D.** rakendab ise ning annab riigis suuna riskipõhiste tegevuste teostamiseks ja meetmete rakendamiseks.

II. Võtta kasutusele intelligentsemad ja digiteadlikumad lahendused ning olla vajadusel selles vallas suunaandjaks nii avalikule kui ka erasektorile. Selleks Rahapesu Andmebüroo:

- **A.** arendab välja automaatsed ja kaasaegsed riskide analüüsimise lahendused;
- **B.** teeb koostööd avaliku ja erasektoriga, sh ülikoolide ja teadlastega.

III. Olla Eesti Vabariigi rahapesu ja terrorismi rahastamise tõkestamise kompetentsikeskus. Selleks Rahapesu Andmebüroo:

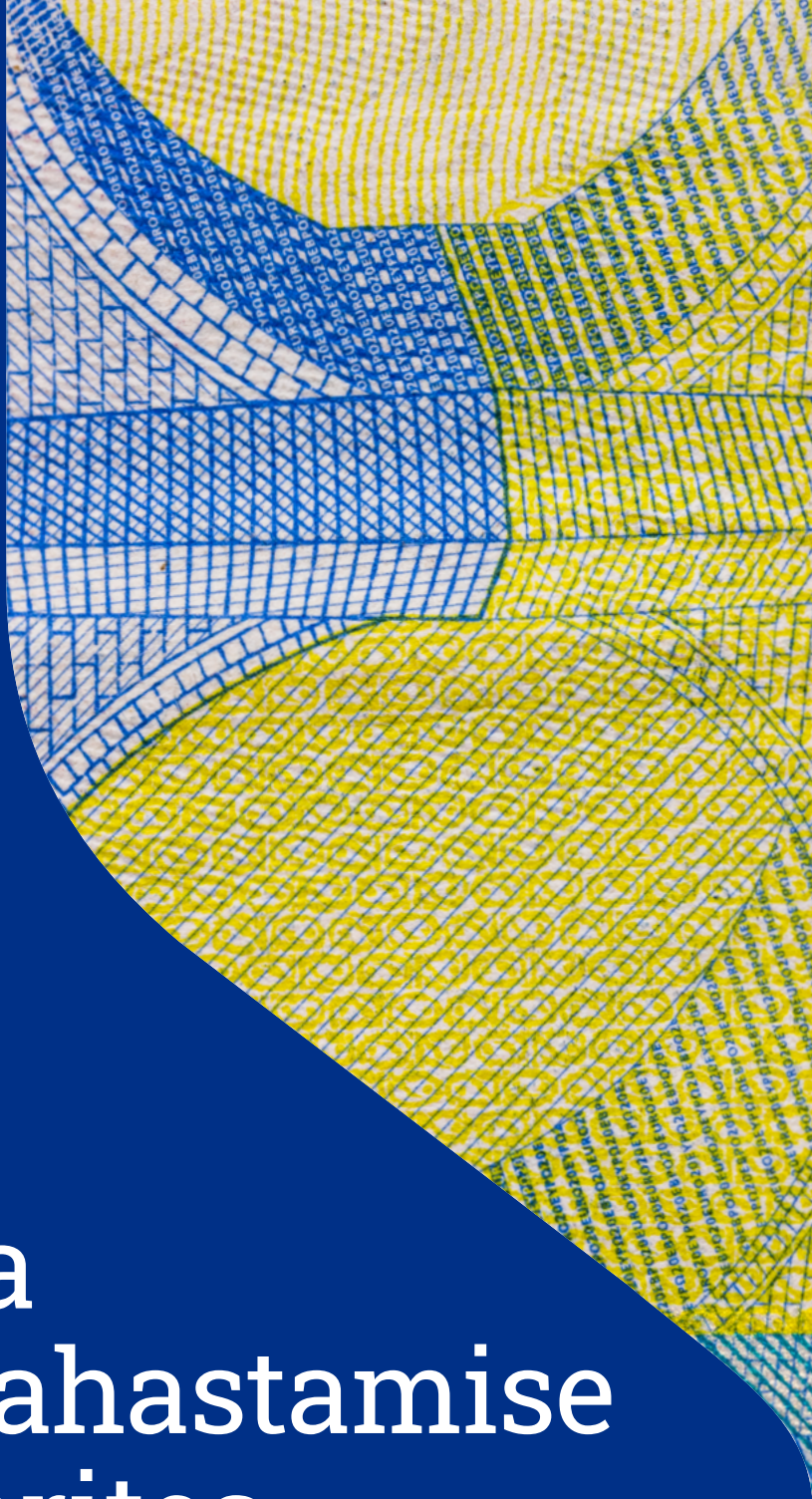
- **A.** suunab Eesti Vabariigi rahapesu ja terrorismi rahastamise tõkestamise süsteemi ülesehitamist;
- **B.** arendab pidevalt enda töötajaid ning koolitab avalikku ja erasektorit;
- **C.** informeerib avalikku ja erasektorit uutest trendidest ning tüpoloogiatest;
- **D.** loob asjakohased juhendid.

Strateegiliste eesmärkide täitmisel lähtub Rahapesu Andmebüroo järgmistest väärtustest:

1. Avatud dialoogile, suunatud innovatsioonile ning Eesti Vabariigis ja rahvusvaheliselt nähtav.

2. Töötajad on oma ala parimad eksperdid, intelligentsed suunanäitajad.

Rahapesu Andmebüroo on finantstehingute aususe valvaja.



Rahapesu ja terrorismi rahastamise riskid sektorites

Aastaraamatu esimeses pooles sedastas siseriiklik ja rahvusvahelise koostöö vaade, et rahapesu suurima riskitasemega sektoriks on *fintech* ja virtuaalvääringu teenuse pakkujad. Terrorismi rahastamise puhul on ohukohaks mittetulundussektori teadlikkuse madal tase.

Aastaraamatu teises pooles teeme sissevaate kõikidesse üheksasse sektorisse, mille turuosalised on seaduse järgi kohustatud isikuteks. Ülevaates tugineme Rahapesu Andmebüroo uuringutele, analüüsidele, igapäevasele järelevalvetööle ning riiklikule riskihinnangule sektori riskipildist koos rahapesu ning terrorismi rahastamise ohu ja haavatavuse hinnanguga.

RAHAPESU RISK SEKTORITES

sektor	oht	haavatavus	risk
Virtuaalvääringu teenuse pakkujad	3,00	4,02	suur
Kinnisvara-maaklerid	2,00	3,53	keskmine
Ühisrahastus	2,45	2,99	keskmine
Finantssektor	2,74	2,69	keskmine
MTÜd	2,00	3,38	keskmine
Äriühingu teenuse pakkujad	2,00	3,31	keskmine
Riik ja sektorid kokku	2,40	2,73	keskmine
Kauplejad	2,00	2,59	alla keskmise
Hasartmängu-sektor	1,95	2,43	alla keskmise
Professionaalid	1,31	2,50	alla keskmise

TERRORISMI RAHASTAMISE RISK SEKTORITES

sektor	oht	haavatavus	risk
Virtuaalvääringu teenuse pakkujad	5,00	3,88	suur
MTÜd	2,30	3,47	üle keskmise
Ühisrahastus	2,30	3,09	keskmine
Äriühingu teenuse pakkujad	2,30	2,76	keskmine
Finantssektor	2,14	2,75	keskmine
Riik ja sektorid kokku	2,09	2,67	keskmine
Kinnisvara-maaklerid	2,30	2,31	keskmine
Kauplejad	1,40	2,59	alla keskmise
Professionaalid	1,40	2,40	alla keskmise
Hasartmängu-sektor	1,40	2,38	väike

Siseriiklik riskihinnang 2021

Virtuaalvääringu teenuse pakkujad

Seisuga 31.12.2021 oli Eestis kehtiv tegevusluba 381 virtuaalvääringu teenuse pakkujal. Kuigi aasta-aastalt on tegevuslubade arv vähenenud (2019. aastal 1234 ja 2020. aasta lõpus 473), on mitteametlikel andmetel jätkuvalt tegemist maailma mastaabis suurima litsentside arvuga. Paljud ettevõtjad toovad Eestisse tulu ja loovad innovatsiooni, kasutades seejuures ka piisavaid riskikontrollimeetmeid, kuid suurema osa Eesti virtuaalvääringu teenuse pakkuja litsentsiomanike kohta seda öelda ei saa. Eestil tuleb nendega kaasnevaid riske jõudsalt maandada. Riskide realiseerumine tähendab siinkohal kahju inimeste varale ja Eesti mainele.

TEGEVUSLOAD VIRTUAALVÄÄRINGU TEENUSE PAKKUMISEKS 2021. AASTAL:

Esitati
347
tegevusloa taotlust, sh 161 uut ja 276 tegevusloa muutmise taotlust

Kehtetuks tunnistati
331
tegevusluba erinevate virtuaalvääringu teenuste pakkumiseks

Väljastati
86
tegevusluba

Keelduti tegevusloa väljastamisest
18
ettevõttele

57
taotlust võeti taotlejate poolt tagasi

Riikliku riskihinnangu kohaselt on peamisteks riskideks sektori läbipaistmatus, sektori täieliku riskipildi puudumine, ebapiisavad nõuded loataotlejatele, lühike kontrollaeg turule sisenemisel, kõrgendatud oht seoses e-residentidega, raskendatud kohapealne järelevalve, tegelik mitteseotus Eestiga, teenusepakkujate arvu kiire kasv, turuosaliste väga erinev hoolsusmeetmete täitmise kvaliteet.

Kuna virtuaalvääringu teenuse pakkujate ring on viimastel aastatel olnud kiires muutumises ning sektor on kiiresti arenenud, uuendas andmebüroo ka sektori riskihinnangut 2021. aastal. Uuringu peamine järeldus on, et rahapesu ja terrorismi rahastamise riskid on virtuaalvääringu teenuse pakkujate puhul jätkuvalt kõrged.

Terrorismi rahastamise vaatest on ohukohtadeks sektori suur anonüümsus ja läbipaistmatus, tõhusate seire- ja monitooringusüsteemide puudumine, ebapiisav töötajate arv ja ebapiisav hoolsusmeetmete kohaldamise tase, teenusepakkujate tegelik mitteseotus Eestiga, raskendatud kohapealne järelevalve ja andmebüroo ettekirjutustele vastamata jätmine. Lisaks sellele toimub ebaproportsionaalselt suur vara liikumine terrorismi rahastamise kõrgema riskiga riikidesse nagu Süüria ja Pakistan.

Uuringu kohaselt on enamiku Eesti tegevusloaga teenusepakkujate hoolsusmeetmete rakendamine märkimisväärselt ebapiisav. Kõrvutades seda teenuse osutamise mahtude, nõrga rahapesu ja terrorismi rahastamise tõkestamise ning finantssanktsioonide eest vastutavate töötajate oskuste ja teadmiste tasemega, viitabki see sektoris kõrgetele riskidele. Ettevõtete puhul on iseloomulik taotleda Eestist tegevusluba, kuid mitte teha samme, et olla kursis siinsete mängureeglitega või neid sisuliselt täita. Sellistel teenusepakkujatel ei peaks Eestis olema kohta. Samuti mitte ka nendel, kes kasutavad siinset jurisdiktsiooni ebaseaduslikel eesmärkidel.

Sektori üheks riskitaset tõstvaks teguriks on ka ettevõtete tegevuse vähene läbipaistvus. 2021. aastal valminud äriühinguteenuse pakkujate rahapesuriskide uuringus[IV] tõime välja, et Eesti äriühinguteenuse pakkujad reklaamivad Eesti virtuaalvääringu tegevusluba rahvusvaheliselt kui kvaliteedimärki, mis võimaldab teenusepakkujal klientidele kinnitada, et nende vara on kindlas kohas. Tegelikult on Eesti vahendite liikumisel transiitriik ning erinevad rahvusvahelised foorumid ja veebisaidid hoopis hoiatavad Eesti teenusepakkujate eest.

Mitmed siinsed äriühinguteenuse osutajad pakuvad ka virtuaalvääringu teenuse tegevuslubade ettevalmistamise teenust. Eesti valmisettevõtted, millel on virtuaalvääringu teenuse tegevusluba, on saanud müügiartikliks ka rahvusvahelistele äriteenuseid pakkuvatele ettevõtetele, kes ei tunne Eesti õigusruumi ega siinseid nõudeid. Nende äriühinguteenuse pakkujate peamine soov on teenida raha, kuid riskide juhtimine, sh andmebüroole rahapesu kahtlusega teadete tegemine, on tagaplaanil. Andmebüroole üritatakse teadlikult esitada näilikke juhatuse liikmeid, pealtnäha lugupeetud ärimeeste alalisi peatumiskohti Tallinnas või selle lähedal, kus elupinna suurus jääb alla 10m^2 jne.

Virtuaalvääringu teenuse pakkujate teatamisaktiivsus näitab paranemise märke, kuid ohumärgiks on see, et suurima käibega teenusepakkujatelt on laekunud vaid üksikud teated. Kui 2019.

253 aktiivselt tegutseval* Eestis väljaantud tegevusloaga virtuaalvääringu teenuse pakkujal on

- kokku 4,8 miljonit klienti, mis on ligi 4,5 korda rohkem kui 2019. aastal;
- käive kokku 20,3 miljardit eurot (juulist 2020 juulini 2021), millest enam kui 85% andsid 15 teenusepakkujat;
- 15 suurima käibega teenusepakkujad;
- vahendavad klientide vara, mis on peaasjalikult pärit Venemaalt, Jaapanist, Šveitsist ja nii Põhja- kui ka Lõuna-Ameerikast;
- edastavad ebaproportsionaalselt suures ulatuses vara Luxembourgi, Süüriasse, Pakistani, Kreekasse, Montenegrosse, Serbiasse ja Belize'i;
- ei ole suuremas osas esitanud ühtegi teadet rahapesu või terrorismi rahastamise kahtlusest.

** käive üle 2000 euro aastas.*

Tegevusloa tühistamine

2021. aasta sügisel tühistas andmebüroo Izibits OÜ tegevusloa virtuaalvääringu teenuse pakkumiseks.

- Ettevõte teatas 30.06.2020 majandustegevuse ajutisest loobumisest.
- Avalike allikate andmetel oli ettevõte tihedalt seotud muu hulgas Chatex kaubamärgi all opereeriva krüptovaluuta vahetusplatvormiga. Chatex püüdis jätta avalikkusele muljet, nagu tal oleks Eesti tegevusluba virtuaalvääringu teenuste pakkumiseks ja viitas oma veebilehel, et opereerib Izibits OÜ-le väljastatud tegevusloa alusel.
- Andmebüroo on seisukohal, et Eestis väljaantud tegevusluba pole lubatud edasi „laenata" ning selle alusel võib tegutseda üksnes isik, kellele on väljastatud see tegevusluba.
- Ameerika Ühendriikide ametivõimud kehtestasid finantssanktsioonid virtuaalvääringute vahetusplatvormile Chatex ning sellega seotud ettevõtetele, sh Izibits OÜ-le, seoses erinevat tüüpi kuritegevusega seotud varade vahendamisega.

aastal saatsid virtuaalvääringu teenuse pakkujad andmebüroole 400 ja 2020. aastal 530, siis 2021. aastal 1865 teadet. Teated on ajas muutunud sisukamaks ja teatajate ring on laienenud, kuid andmebüroo tehtud teadete sisuanalüüs näitas paljude turuosaliste puhul puudujääke kahtlaste tehingute väljaselgitamisel. Seda näitab ka asjaolu, et ligi pooled teadetest puudutasid kliendisuhtesse astumisest keeldumist, valdavalt seoses võltsitud dokumentide kasutamise kahtlusega.

Arvestades riskipilti, pöörati sektorile suurt tähelepanu ka järelevalvetegevuses – virtuaalvääringu teenuse pakkujate hulgas viidi läbi kõige rohkem järelevalvekontrolle. Kehtiva tegevusloaga virtuaalvääringu teenuse pakkujate osas alustati 18 järelevalvemenetlust.

Neist 14 olid kohapealsed ning neli kaugkontrolli vormis tehtud järelevalvemenetlused. Kahel juhul kontrolliti virtuaalvääringu teenuse pakkujate tegevust rahvusvahelise sanktsiooni seaduses märgitud kohustuste osas ning ülejäänud järelevalve käigus kontrolliti virtuaalvääringu teenusepakkujate tegevust kõikide rahapesu ja terrorismi rahastamise tõkestamise ja rahvusvahelise sanktsiooni seaduses märgitud kohustuste osas.

Kolme järelevalve käigus loobusid virtuaalvääringu teenusepakkujad ise tegevuslubadest. Ühe järelevalvemenetluse käigus koostas andmebüroo otsuse, mille tulemusel tunnistati virtuaalvääringu teenuse pakkuja tegevusluba kehtetuks. Antud juhul ei viinud ettevõte ennast määratud tähtajaks kooskõlla seadusest tuleneva kontrollieseme asjaoluga – virtuaalvääringu teenuse pakkujal peab olema avatud maksekonto krediidiasutuses, e-raha asutuses või makseasutuses, mis on asutatud Eestis või Euroopa Majanduspiirkonna lepinguriigis ja osutab Eestis teenuseid piiriüleselt või mis on Eestis asutanud filiaali. Kui selline maksekonto puudub, ei saa osutada virtuaalvääringu teenust Eesti litsentsiga.

Teostatud järelevalvekontrollid tuvastasid vajakajäämisi kõikides kontrollitud ettevõtetes. Peamised puudused seisnesid protseduurireeglites, riskihinnangus ning hoolsusmeetmete täitmises. Puudustest tingitud riskid vastavad andmebüroo uuringule ja riiklikule riskihinnangule.

Virtuaalvääringu teenuse pakkujate järelevalvemenetluses tuvastatud peamised puudused:

- Protseduurireeglid ei ole sageli vastavuses ettevõtte äritegevusega ning neis kirjas olev ei ole seotud virtuaalvääringu teenusepakkujatele omaste tunnustega. Turul ringlevad nö universaalsed protseduurireeglid, mis ei arvesta valdkonna spetsiifikat. Andmebüroole on see selgeks ohumärgiks, sest ettevõte, kes kasutab neid selleks, et formaalselt seaduse nõudeid täita, pole tegelikult oma protsesse ja riskijuhtimise meetmeid läbi mõelnud.

- Kontrollitud teenusepakkujate riskihinnangud ei peegeldanud ettevõtte tegelikku tegevust, ei kajastanud klientide riskiprofiile ega kliendiprofiilide kujunemise põhimõtteid või geograafilise riski vaadet.

- Hoolsusmeetmete täitmisel tuvastatud puudustest ei olnud ettevõtted seaduses nõutud määral rakendanud näiteks meetmeid kliendi isikusamasuse tuvastamisel. Sealhulgas ei olnud kogutud piisavalt dokumente kaugtuvastuse tegemisel või vaatamata seaduse nõuetele ei

olnud klienti nö näost-näkku nähtud ega tuvastatud infotehnoloogilise seadme abil. Samuti puudusid ettevõtetel tehnilised lahendused, mis võimaldaksid nõutud määral tehinguid jälgida ja tuvastada rahapesu või terrorismi rahastamise kahtlusega tehingud.

- Puudusid rahapesu riskide juhtimisega tegelevad töötajad või esinesid töötajate tegevuses huvide konfliktid. Töötajate teadmised olid tihti sisuliselt olematud, kusjuures paljudel juhtudel ei oldud nad tutvunud ettevõtte enda kirjutatud ja rakendatud protseduurireeglitega või seaduse sätetega.

Virtuaalvääringu teenusepakkujate hoolsuskohustuse, tehnilise korralduse ja riskide juhtimise üldine võimekus on tasemel, mis oli enam kui kümme aastat tagasi makseteenuse pakkujatel, kes esmakordselt makseteenuste direktiivi alusel allutati finantsjärelevalvele. Ainsaks erinevuseks on asjaolu, et rahapesu ja terrorismi rahastamise riskid, mis virtuaalvääringu teenusepakkujate sektoriga kaasnevad, on sadu või kohati tuhandeid kordi suurem kui maksevahenduse sektoris.

Andmebüroo viis virtuaalvääringu teenuse pakkujatele läbi e-koolituse, kus tutvustati sektoraalseid riske ja anti suuniseid nende juhtimiseks. Koolitus võeti turu poolt väga hästi vastu. Osalejaid oli 141 ning osalejate rahulolu koolitusega oli kõrge. Koolitustega jätkatakse, et tõsta valdkonnas tegutsevate ettevõtete riskiteadlikkust ja riskide juhtimise võimekust ning tutvustada 2022. aastal jõustuvaid muudatusi seadusandluses.

Kõnepettused ja virtuaalvääringud

2021. aastal suurenes varasemaga võrreldes kelmusjuhtumiga seotud teadete arv rohkem kui kuus korda – kokku sai andmebüroo ligi 10 000 kelmusega seotud teadet, mis on 63% kõikidest andmebüroole esitatud teadetest.

2021. aasta märksõnaks oli kõnepettus, kus kelmide peamiseks eesmärgiks oli ohvril lasta sisestada internetipanka Mobiil-ID või Smart-ID PIN-koodid, et saada ligipääs ohvri pangakontole. Samuti on levinud skeem, kus ohvril palutakse tema arvutisse alla laadida „turvaprogramm“, mis tegelikkuses on pahavara, mille abil saavad kelmid ligipääsu ohvri arvutile ja selles sisalduvale informatsioonile. Ohvritelt küsitakse sageli ka isikut tõendava dokumendi numbrit või pilti dokumendist, mida kurjategijad kasutavad hiljem ohvri nimel kiirlaenude võtmiseks ja/või ohvrite teadmata nende nimel pangakontode avamiseks.

Kelmid esitavad ohvritele erinevaid lugusid, kuid peamiselt esitletakse ennast pangatöötajana, kes palub ohvritel kahtlase tehingu tühistamiseks või väidetava varguse vältimiseks järgida helistaja juhiseid. Petturid kõnelevad enamasti vene keelt, suhtlevad oma ohvritega manipuleerivalt ja intensiivselt. Paljudel juhtudel on ohvrid kaotanud oma vara ka kelmidele, kes esitlevad ennast töötajana pangast, kus ohvril ei ole pangakontot, kuid kes osava manipulatsiooni ja veenmise tulemusel suudavad ohvri rahast ilma jätta. Kuigi petukõned on suuresti seotud Ukrainaga, ei ole Venemaa agressiooni järel petukõnede tegemine peatunud.

Ohvrite pangakontosid on kasutatud ka kõne- või muu pettuse teel omandatud raha pesemiseks ilma nende teadmata. Kelmuse teel saadud raha kantakse ohvrite pangakontole ja sealt kohe edasi, et varjata raha algset kuritegelikku päritolu. Ohvritelt välja petetud rahad võetakse sularahana makseautomaadist välja, kuid sageli saadetakse ka virtuaalvääringu teenuse pakkujate erinevatele kontodele, kus petetud raha muundatakse krüptovaluutaks.

Virtuaalvääringu teenuse pakkumisega seotud rahapesuskeemid

2021. aastal esines juhtumeid, kus Eestis registreeritud virtuaalvääringu teenuse pakkujaid kasutati rahapesuks. Virtuaalvääringu teenuse pakkujaid saab kasutada selleks, et vahetada ühte liiki vara teise vastu, näiteks kuritegelikul teel omandatud tavavaluuta vahetamiseks virtuaalvääringu vastu. Sellega soovitakse kaotada seos varasemate tehingutega ning muuta kuritegeliku päritoluga varaga tehtavate tehingute jälgimine keerulisemaks.

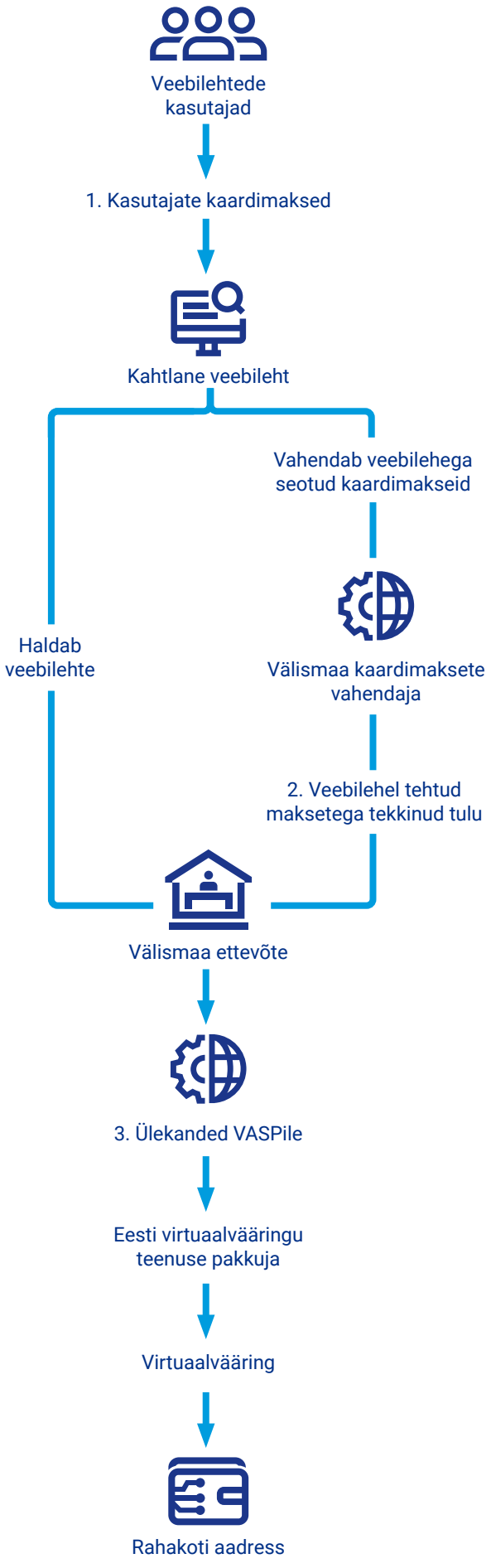
Lisaks on võimalik virtuaalvääringu teenuse pakkujate vahendusel vahetada kuritegeliku tegevuse tulemusel omandatud virtuaalvääring teist tüüpi virtuaalvääringu vastu. Ka sellise tehingu puhul katkestatakse tehingute ahel ühes süsteemis ning vara liigub edasi teise süsteemi, sest erinevad virtuaalvääringud kasutavad toimimiseks erinevaid plokiahelaid.

Näiteks, kui vahetada Bitcoin virtuaalvääringu teenuse pakkuja vahendusel Ethereumi virtuaalvääringu vastu, jääb Bitcoin virtuaalvääringu teenuse pakkujale ning teenuse kasutaja saab virtuaalvääringu teenuse pakkujalt vastu vastavas koguses Ethereumi virtuaalvääringut.

Kuritegelikku päritolu varaga on võimalik luua keerukaid rahapesuskeeme, kus kasutatakse nii finantssüsteemi kui ka virtuaalvääringutega seotud plokiahelaid. Nendes skeemides on oluline roll virtuaalvääringu teenuse pakkujatel, sest sellised platvormid on kokkupuutepunktideks erinevatele süsteemidele. Kui kuritegeliku päritoluga vara jõuab virtuaalvääringu teenuse pakkujani, on vara edasise liikumise tuvastamise ainuke viis hea koostöö teenusepakkujaga, kes vahetustehingu tegi. Virtuaalvääringu teenuse pakkuja abil saab tuvastada ka võimalikku informatsiooni kliendi kohta, kes teenuseid kasutas ning seeläbi jõuda virtuaalvääringu rahakoti aadressi omanikuni, kellele virtuaalvääringu teenuse pakkuja võis vara kanda. Mustal turul on aga võimalik osta virtuaalvääringu teenuse pakkujate platvormidel valeandmetega loodud kasutajakontosid, mida kurjategijad kasutavad oma tegeliku identiteedi varjamiseks[V].

Näide kuritegeliku raha jõudmisest virtuaalvääringusse

- Fiktiivsed kasutajad teevad kahtlase veebilehe teenuste tarbimiseks kaardimakseid kuritegelikku päritolu rahaga.
- Ettevõte, mis vahendab veebilehega seotud kaardimakseid, kannab raha firmale, mis haldab seda veebilehte.
- Firma, mis haldab veebilehte, saab väita, et tegemist on veebilehe haldamise tulemusel teenitud tuluga ja kannab raha omakorda edasi virtuaalvääringu teenuse pakkujale, et vahetada raha virtuaalvääringute vastu.
- Virtuaalvääringu teenuse pakkuja teenuste kasutamisega katkestatakse finantssüsteemis toimunud tehingute ahel, et varjata seost rahakoti aadressile jõudnud virtuaalvääringute ja varasemalt veebilehega seotud kaardimaksete vahel. Vahetustehingu tulemusena kantakse virtuaalvääring rahakotiaadressile.



Investeerimiskelmused ja virtuaalvääringud

Kõnepettuste kõrval on levinud ka investeerimiskelmused, kus potentsiaalsele ohvrile tutvustatakse „väga head, unikaalset ja personaalset investeerimisvõimalust“. Kurjategijad näitavad oma ohvrile veebilehti ja manipuleeritud graafikuid, et luua pettekujutelm mõne finantsinstrumendi kõrgest kasvust ja heast potentsiaalist ning veenda ohvrit tegema sissemakseid. Enamasti saavad ohvrid pettusest aimu alles siis, kui soovivad oma raha kätte saada, mis kahjuks enam ei õnnestu.

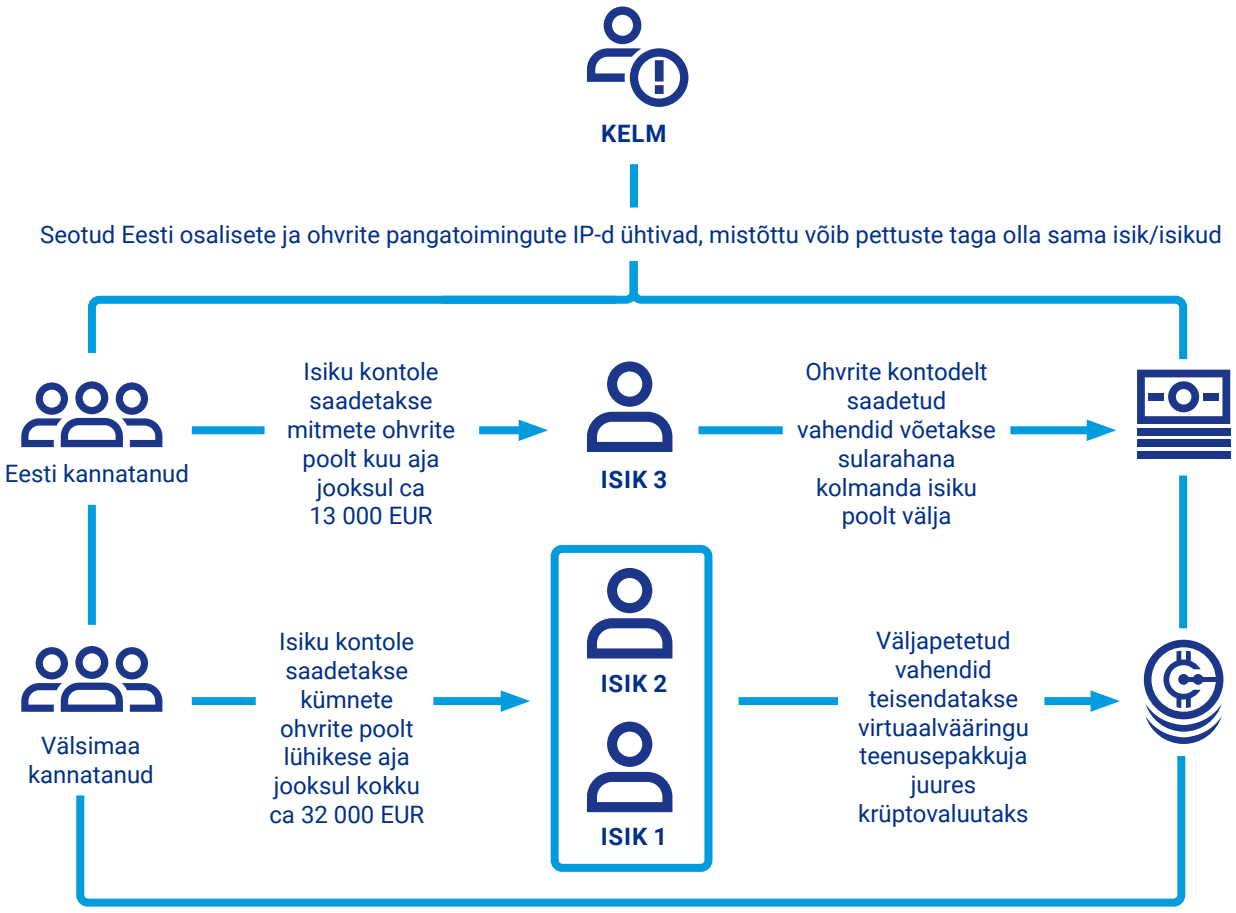
Kahju, mida kelmid võivad tekitada, kui neil on ligipääs ohvri isikuandmetele ja/või arvelduskontodele:

- Joonisel toodud kahe isiku (ISIK 1 ja ISIK 2) äsja avatud pangakontodele laekus vähem kui kuu aja jooksul kandeid kümnetelt välisriigi

kodanikelt, lisaks laekusid kontodele kontode omanike nimel võetud kiirlaenud.

- Välismaa kodanikelt laekunud ülekannete makseselgitused viitasid elektroonika ostule, mistõttu võib eeldada, et kelmus toimus veebikaubandusplatvormide kaudu.
- Kannetele järgnesid maksete tagasikutsumise avaldused.
- Väljapetetud vahendid suunati virtuaalvääringu teenuse pakkuja kontole, kus saadud vahendid konverteeriti krüptovaluutaks.
- Nii ISIK 1 kui ka ISIK 2 toimingud tehti samalt IP-aadressilt, mistõttu võis eeldada, et nimetatud isikute toimingute taga võis olla kolmas isik, kes avas antud isikutele arvelduskontod. Sama IP-aadress kattus ka ISIK 3 puhul ja isiku kontole rahalisi vahendeid kandnud kontode puhul.

Selles juhtumis olid ohvrid Eesti kodanikud, kellele avati pangas kontod, kuhu laekus esimese asjana ohvrite nimel võetud kiirlaen, mis saadeti koheselt edasi ISIK 3 kontole. ISIK 3 kontol olevad vahendid võeti sularahaautomaadist välja isiku poolt, kes ei saanud olla antud pangakonto omanik.



NFTd

2021. aastal kasvas maailmas hüppeliselt NFT (*non-fungible tokens*) populaarsus. Tegemist on plokiahelaga seotud andmeühikuga (*token*), mida on võimalik kasutada esemete unikaalse omandiõiguse iseloomustamiseks. NFT tokenitega on võimalik siduda kunstiteoseid, kinnisvara, internetidomeene, esemeid arvutimängudes jne.

Peamiselt leiab NFT kasutust digitaalsete esemete puhul. NFTd on unikaalsed ja neid ei ole võimalik muuta ega kopeerida ning sellel saab olla ainult üks omanik. NFTsid on võimalik luua ainult plokiahelates, mis võimaldavad *smart-contract* programmeerimist. Levinumad *smart-contract* standardid on ERC-721 ja ERC-1155, mis on seotud Ethereumi plokiahelaga. Näiteks on NFT kunstiteos „Everydays – The First 5000 Days", mis müüdi 2021. aastal ca 69 miljoni dollari eest, tehes sellest ühe maailma hinnalisema NFT[VI].

NFTsid nähakse maailmas ka kui uut vahendit, mis võib pakkuda huvi kurjategijatele ja rahapesijatele. Suurbritannia kaitse- ja julgeoleku mõttekoja Royal United Services Institute hinnangul on NFTsid võimalik ära kasutada erinevat tüüpi kuritegeliku tegevuse jaoks. Näiteks on võimalik NFTsid võltsida ning sisse häkkida NFT vahetusplatvormidele ja neid varastada. Varastatud NFT on võimalik maha müüa ja teenitud tulu puhtaks pesta. NFT loomise käigus on võimalik peita NFT sisse ka informatsiooni, mis tähendab, et NFTsid saab kasutada informatsiooni vahetamiseks kuritegelike osapoolte vahel[VII]. Ka Ameerika Ühendriikide Rahandusministeeriumi (*Department of Treasury*) hinnangul on NFTd seotud rahapesuriskiga ning platvorme, mis võimaldavad kaubelda NFTdega, võib teatud juhtudel, sõltuvalt konkreetsete NFTde kasutamise tüübist, käsitleda ka kui virtuaalvääringu teenuse pakkujaid[VIII].

NFTsid võidakse kasutada rahapesuks skeemis, kus kurjategija ostab kuritegeliku päritoluga vara eest NFT kunstiteose ning hakkab seejärel tegema tehinguid iseendaga seotud aadresside vahel, tekitades plokiahelasse vara müüki iseloomustavaid andmeid. Kurjategija võib lõpuks NFT müüa ka pahaaimamatule ostjale, kes maksab selle eest legaalset päritolu varaga. Lisaks saab NFT kunstiga teha tehinguid otse kahe osapoole vahel ilma vahendajata. NFTde kasutamine kurjategijate poolt võib tulevikus ka Eesti õiguskaitseasutuste tähelepanu pälvida.

Üldiselt on Europoli hinnangul virtuaalväärингute kasutamine seoses kriminaalse tegevuse ja rahapesuga kasvutrendis, kuid virtuaalväärингutes tehtud tehingute osakaal varimajanduses on võrreldes sularaha ja teiste tehingutüüpide kasutamisega veel tagasihoidlik[IX]. Avalikel andmetel võisid küberkurjategijad 2021. aastal pesta 8,6 miljardi dollari väärtuses virtuaalväärингuid. Võrreldes 2020. aastaga on kasv 30%, võttes arvesse küberkuriteod, kus vara ei vahetatud tavavaluutast virtuaalväärингuks[X].

Ameerika Ühendriikides tõsteti küberturvalisuse probleem kõrge tasemega prioriteediks pärast 2021. aastal toimunud küberrünnakuid, mis tekitasid ohtu riigi energiaga ja toiduainetega varustamisele, ja sellega seotud lunarahanõueid.

Virtuaalväärингute kasutamine ei ole aga enam kitsalt seotud küberkuritegevusega, vaid leiab järjest enam kasutust erinevat tüüpi kuritegude puhul, kus on vajalik teha tehinguid varalise väärtusega. Näiteks narkokaubandus, mõrvade tellimine tumeveebis, erinevat tüüpi kelmused, inimkaubandus jne.

Krediidi- ja finantseerimisasutused

Finantssektori turuosaliste puhul on järelevalve roll jaotatud Finantsinspektsiooni ja Rahapesu Andmebüroo vahel. 2021. aasta lõpus oli andmebüroo järelevalve all 288 kehtivat finantseerimisasutuse tegevusluba. Aasta jooksul andis andmebüroo välja 25 tegevusluba, keeldus tegevusluba väljastamast nelja ettevõtte puhul ning võttis ära 21 tegevusluba. Kokku esitati 2021. aastal 51 tegevusloa taotlust, millest 35 olid uued ning 16 tegevusloa muutmise taotlused. Tegevusluba taotlevad finantseerimisasutused võtsid ise tagasi kuus taotlust.

Krediidiasutuste saadetud kahtlaste tehingute teadete arv on viimastel aastatel olnud kasvutrendis, kuid 2021. aastal kasvas teadete arv plahvatuslikult. Kui 2019. aastal saatsid krediidiasutused andmebüroole 2905 ja 2020. aastal 4594 teadet, siis 2021. aastal enam kui 11 000 teadet. Nagu eelmises peatükis kirjeldatud, siis plahvatusliku kasvu põhjuseks olid teated kelmustest.

Finantseerimisasutuste teadete arv kasvas 2021. aastal võrreldes eelnevate aastatega samuti, kuid mitte nii drastiliselt: 2019. aastal 1188, 2020. aastal 1444 ja 2021. aastal 2088 teadet. Pooled teadetest puudutasid sularaha.

Finantssektoris on riikliku riskihinnangu kohaselt nii rahapesu kui ka terrorismi rahastamise risk keskmisel tasemel. Finantseerimisasutustega on seotud mitme teise sektori rahapesu riskid, nagu kuritegeliku raha sisenemise oht Eesti finantssüsteemi, mitteresidentidest ja e-residentidest omanikega äriühingute, maksevahendajate, virtuaalvääringute ja sularahatehingute ohud ning kliendi osas hoolsusmeetmete rakendamata jätmise oht. Finantseerimisasutustel võib olla probleeme ka mitteresidentidest klientide soovitud määral tuvastamisega ning seetõttu võib sattuda finantssüsteemi rahalisi vahendeid, mille omaniku või päritolu osas pole selgust. Nagu aastaraamatu esimeses peatükis märgitud, oli 2021. aastal andmebüroole esitatud välispäringutest arvuliselt kõige suurem rahapesu tüpoloogia kelmusest saadud vahendite kandmine välisriigi maksevahendaja või virtuaalvääringu teenusepakkuja VIBAN kontole ning edasisaatmine vastava teenusepakkuja platvormil ning see trend on ajas kasvanud. Seega on pankade jaoks üha kõrgema riskiga korrespondentsuhted makseasutustega.

Rahapesu poolelt on finantssektori haavatavad kohad järelevalve tegevusloata väikefondide valitsejate ja muude finantseerimisasutuste üle. Hoolsusmeetmete rakendamise seisukohalt on probleemne tegelike kasusaajate registri andmete usaldatavus ja juurdepääs riikliku taustaga isikute teabele nii siseriiklikult kui ka rahvusvaheliselt.

Kui 2019. aastal saatsid krediidiasutused andmebüroole 2905 ja 2020. aastal 4594 teadet, siis 2021. aastal enam kui 11 000 teadet.

Terrorismi rahastamise poolelt on keerukas töötada vastavuskontrollisüsteemidele välja spetsiifilisi stsenaariume.

Andmebüroo alustas möödunud aastal finantseerimisasutuste osas kahe järelevalvemenetlusega. Kohustatud isikute puhul vaadati kaugkontrollidega kõikide seadusest tulenevate kohustuste täitmist ehk teostati nö täiskontroll. Ühe järelevalve käigus ei vastanud finantseerimisasutus andmebüroo ettekirjutusele, mistõttu ettevõttele määrati sunniraha. Korduvate ettekirjutuste täitmata jätmiste tõttu võttis andmebüroo ühelt ettevõttelt ära tegevusloa. Teise järelevalve käigus selgus, et ettevõttel puudus protseduurireeglites juhend, kuidas ettevõte tuvastab riikliku taustaga isikuid ning nendega seotud lähikondseid. Puudusi esines ka riskihinnangus, mis ei vastanud

ettevõtte tegevuse spetsiifikale. Riskihinnang peab kajastama ettevõtte konkreetset tegevust ja sellega kaasnevaid riske, et see vastaks seaduse nõuetele ning oleks ka tõhus rahapesu ja terrorismi rahastamise riskide maandamisel.

Sektori turuosaliste teadlikkust tuleb tõsta just väiksemate turuosaliste gruppide seas, nagu tegevusloata väikefondi valitsejad ja finantseerimisasutused. Andmebüroo viis 2022. aasta alguses läbi koolituse enda järelevalve all olevatele finantseerimisasutustele, et tutvustada riiklikku riskihinnangut ning seadusest tulenevaid kohustusi rahapesu ja terrorismi rahastamise tõkestamisel. Virtuaalsel koolitusel oli 143 osalejat.

Usaldushalduse ja äriühingu teenuse pakkujad

2021. aasta lõpu seisuga oli kehtiv tegevusluba 325 usaldushalduse ja äriühinguteenuse pakkujal. Andmebüroo väljastas aasta jooksul 23 tegevusluba, keeldus tegevusloa väljastamisest kahe ettevõtte puhul ning võttis ära seitse tegevusluba. Kokku esitati 2021. aastal 50 tegevusloa taotlust, millest 31 olid uued ning 19 tegevusloa muutmise taotlused. Andmebüroo tuvastas 2021. aastal ja informeeris enda koostatud analüüsidokumendiga ka avalikkust, et Eestis pakub usaldushalduse ja äriühingu teenuseid aktiivselt 195 teenusepakkujat, kusjuures 75 teenusepakkujal puudus selleks tegevusluba. Andmebüroole ei ole peale seda esitatud tegevusloa taotlusi, samuti ei ole andmebüroo kõikide nimetatute puhul tuvastanud tegevusloata tegevuse lõpetamist. Sektori teenusepakkujad esitasid andmebüroole kuus teadet, mis on täielikus mittevastavuses sektori riskitasemega.

Riikliku riskihinnangu kohaselt on äriühinguteenuse pakkujate puhul nii rahapesu kui ka terrorismi rahastamise oht keskmine. Rahapesu vaatest on ohuks juriidiliste isikute ärakasutamine, mis on tingitud äriühingute asutamise ja vahendamise protsessi lihtsusest ja kontrollinõuetest puudustest ärisuhete loomisel. Terrorismi rahastamise vaates on riskiks juriidiliste isikute ärakasutamise oht terrorismi rahastamise skeemides ning turuosaliste madal teadlikkus nendest tüpoloogiatest.

2021. aasta teises pooles valmis andmebüroo strateegiline analüüs „Äriühinguteenuse pakkujatega seonduvad rahapesuriskid Eestis“. Järeldustes nenditakse, et nende teenuste pakkumine on Eestis väga aktiivne ja oluline osa teenuseid on suunatud rahvusvahelisele turule, kuid mitmete teenusepakkujate tegevus suurendab Eesti ärikeskkonna läbipaistmatust. Mitmed äriühinguteenuse pakkujad abistavad välismaalasi andmebüroo tegevuslubade taotlemisel, seejuures ettevõtete ja isikute tausta kontrollimata. Hoolsusmeetmete kohaldamata jätmine ettevõtte ja tegevusloa müügi protsessi käigus võimaldab ebaausatel isikutel kasutada ära Eesti ettevõtteid ja majandussüsteemi. Ettevõtted, keda andmebüroo ei tuvasta tegevusloa protsessis, on hiljem

erinevate petuskeemide või küberkuritegude tõttu taas tõusnud andmebüroo huviorbiiti. Kui äriühinguteenuse pakkuja klient paneb toime kuritegusid või vahendab kuritegelikke vahendeid, võib äriühinguteenuse pakkuja ebapiisav hoolsuskohustuse täitmine või kliendi abistamine tuua kaasa ka äriühinguteenuse pakkuja kriminaalvastutuse.

2021. aastal algatas andmebüroo neli järelevalvemenetlust usaldushalduse ja äriühinguteenuse pakkuja osas, kellel on tegevusluba. Kõik järelevalvemenetlused olid kohapealsed järelevalvekontrollid. Ühes järelevalvemenetluses kontrolliti kohustatud isiku hoolsusmeetmete täitmist ning ülejäänud kolm menetlust olid täiskontrollid, kus kontrolliti ettevõtte kõikide kohustuste täitmist seoses rahapesu ja terrorismi tõkestamise seadusega.

Kontrollitud teenusepakkujate puhul ilmnes, et nad ei suuda efektiivselt hinnata ja tuvastada sektoris esinevaid riske. Nii järelevalvetulemused, riiklik riskihinnang kui ka selle sektori osas 2021. aastal avaldatud analüüs osutavad, et äriühinguteenuse pakkujate rahapesu ja terrorismi tõkestamise alane teadlikkus on madal, riskisüsteemid puudulikud, hoolsusmeetmeid rakendatakse ebapiisavalt ja andmebüroole kahtlastest tehingutest teatamise kohustust ei täideta.

Äriühinguteenuse pakkujate puhul on väga levinud osutatav professionaalse ühingujuhi teenus. See aga kätkeb endas ohtu, et nominaaldirektoritest ja nominaalsetest osanikest „tankistid“ palgatakse kas tegelike kontrollistruktuuride varjamiseks või kasutatakse nominaaldirektoreid eesmärgiga vabaneda maksejõuetuks muutuvast ettevõttest.

Eesti ettevõtluskeskkond ja e-riigi teenused teevad Eestis äriühingute asutamise lihtsaks ja soodsaks ka mitteresidentidele ja e-residentidele. Turul tegutsevad äriühinguteenuse pakkujad müüvad mitteresidentidele ja e-residentidele valmisettevõtteid ning jätkavad neile sageli vähemalt postkasti- või kontaktisikuteenuse pakkumist, luues ja säilitades mitteresidentide kontrollitud ettevõtetele näilise sideme Eestiga.

Sõnum virtuaalvääringutega kaasnevatest rahapesu ja terrorismi rahastamise riskidest on viidud turuosalisteni ning kehtivate virtuaalvääringu teenuse tegevuslubadega ettevõtete arv Eesti turul on jõudsalt vähenenud. Vaatamata sellele tuvastas andmebüroo järelevalvet tehes, et mitmed siinsed äriühinguteenuse osutajad pakuvad endiselt virtuaalvääringu teenuse tegevuslubade ettevalmistamise teenust. See aga tähendab, et turule aidatakse tundmatu taustaga ettevõtteid, kes ei tunne Eestis kehtivaid nõudeid ega ole kättesaadavad andmebüroo järelevalvetoiminguteks.

Ettevõtted, keda andmebüroo ei tuvasta tegevusloa protsessis, on hiljem erinevate petuskeemide või küberkuritegude tõttu taas tõusnud andmebüroo huviorbiiti.

Äriühinguteenuse pakkujate seas riikliku riskihinnangu raames läbi viidud küsitluse tulemused näitasid:

- ligi 3/4 vastanutest ei osanud nimetada oma valdkonnas esinevaid rahapesu ja terrorismi rahastamise tõkestamisega seotud riskide tüpoloogiaid, mis viitab sellele, et teenusepakkujad ei tunne ega suuda efektiivselt hinnata ja tuvastada sektoris esinevaid riske;
- sektoris tegutsevad küllaltki kõrge riskiisuga teenuseosutajad.

Sellest lähtuvalt peaksid ettevõtjad tagama, et ettevõttes oleksid tegevusega kaasnevad rahapesu ja terrorismi rahastamise riskid teadvustatud, ära hinnatud ja maandatud.

Andmebüroo hinnangul on väga oluline turuosaliste teadlikkuse kasvatamine. 2021. aasta lõpus viidi äriühinguteenuse pakkujatele läbi koolitus, et suurendada arusaama võimalikest rahapesu ja terrorismi rahastamise riskidest ning anda tagasisidet järelevalvete käigus tuvastatud puudustest kohustatud isikute tegevuses. Virtuaalsel koolitusel oli reaalajas 127 osalejat.

Hasartmängusektor

Hasartmängusektori turuosaliste ring on olnud stabiilne. 2021. aasta lõpu seisuga oli väljastatud 26 tegevusluba.

2021. aastal saatsid hasartmängukorraldajad andmebüroole kahtlastest tehingutest 143 teadet, aasta varem 118. 75% neist olid seotud kasiinodega ja 60% olid sularahateated.

Riikliku riskihinnangu kohaselt on hasartmängusektori puhul nii rahapesu kui ka terrorismi rahastamise oht madal. Peamiseks probleemiks on osade turuosaliste madal riskiteadlikkus. Sellest lähtuvalt alustas andmebüroo nelja järelevalvemenetlusega hasartmängusektoris tegevusluba omava äriühingu osas. Võttes arvesse sektori madalat riski, alustati järelevalveid kaugkontrolli teel ainult hoolsusmeetmete kohaldamise osas. Need järelevalvemenetlused ei ole veel lõppfaasi jõudnud.

Peamised puudused aasta varem, 2020. aasta järelevalvete põhjal, olid sarnased teiste sektoritega: protseduurireeglite mittevastavus seaduses sätestatud nõuetele ning ettevõtte tegevusele. Suurem risk võib puudutada kaughasartmängu korraldajaid, kuid praktikas ei ole märkimisväärseid puuduseid tuvastatud.

Riikliku riskihinnangu raames tehtud küsitlusest hasartmängukorraldajate seas ilmnes:

- sektori teadlikkus rahapesu tõkestamisest on pigem kõrge. Ettevõtetes või korporatsioonides olid loodud suunised rahapesu tõkestamiseks ja olid kehtestatud rahapesu tõkestamise protseduurireeglid
- ettevõtetes on vastajate kinnitusel välja töötatud metoodika ja/või juhend rahapesu kahtlusest või ebatavalisest tehingust teatamiseks. Veidi alla poole vastanutest on kinnitanud, et praktikas on juhendit vaja läinud teate esitamiseks andmebüroole
- hoolsusmeetmete rakendamisel võib esineda varieeruvust, seda eelkõige täiendavate hoolsusmeetmete rakendamisel, mille osas on seadus jätnud kohustatud isikule võrdlemisi suure vabaduse
- turuosalised kasutavad erinevaid meetodeid kõrgema riskiga juhtumite korral rahaliste vahendite päritolu ja otstarbe tuvastamiseks. Enamasti küsitakse sellistel juhtudel enda sõnul kliendilt lisaandmeid, vaid üksikud vastajad nimetasid avalike või tasuliste andmebaaside info kasutamist ja info küsimist kolmandatelt osapooltelt

Teoreetiliselt on võimalik nii kasiinodes kui ka kaughasartmängudes pesta raha erinevate skeemide abil. Enam levinud skeemideks on kokkuleppemängud, sh meelega kaotamine ning võitude, žetoonide ja piletite ostmine, et kuritegelikul teel saadud vara näidata legitiimsena. Kasiinosid võidakse ära kasutada rahapesuks, kui raha vahetatakse ümber piletiteks ning hiljem tagasi rahaks ilma panustamiseta või panustades väikeseid summasid. Praktikas on turuosalised avastanud mitmeid sellised katseid tehingute ja teenuste jälgimisel. Vastumeetmena rakendatakse sisemisi täis- ja poolautomaatseid kontrollimehhanisme ning koolitatakse oma töötajaid ära tundma taolisi skeeme.

2021. aasta lõpus viis andmebüroo läbi koolituse hasartmängusektori turuosalistele. Koolitusel osalejatele tutvustati nii riskihinnangu olulisust kui ka seadusest tulenevaid hoolsusmeetmeid. Virtuaalsel koolitusel osales reaalajas 41 inimest.

Kauplejad

Kaupleja on kaubandustegevuse seaduse kohaselt isik või asutus, kes majandus- või kutsetegevuses pakub ja müüb kaupa või pakub ja osutab teenust. Rahapesu ja terrorismi rahasta-

mise tõkestamise seadust kohaldatakse kauplejate suhtes, kellele tasutakse või kes tasuvad sularahas üle 10 000 euro või sellega võrdväärse summa muus vääringus sõltumata sellest, kas rahaline kohustus täidetakse tehingus ühe või mitme seotud maksena kuni üheaastase perioodi jooksul. Aastaraamatus on kauplejate hulka arvestatud ka kunstiteostega kauplejad (RahaPTS § 3 lg 1 p 15). Kauplemiseks ei kohaldata reeglina loamenetlust, välja arvatud mõned erandid, näiteks alkoholimüük. Samuti ei nõua kauplemine kindlat juriidilise isiku liiki. Seetõttu ei moodusta kauplejad piiritletavat isikute rühma nagu näiteks krediidiasutused või vandeaudiitorid. Kohustatud isikuks saamine sõltub tegevusest ning makseviisist ja mahust.

Andmebüroo jaoks on kauplejate puhul kõige suuremaks väljakutseks kohustatud isikute ringi määratlemine, kuna puudub automaatne mehhanism, mis tuvastaks suuremahuliste sularahamaksete toimumist. Kohustatud isikute piiritlemisel saab andmebüroo hetkel toetuda turuosaliste enda esitatud teadetele.

Rahapesu ja terrorismi rahastamise tõkestamise seaduse kohaselt ei ole kauplejatel tegevusloa kohustust, kuid seda võib nõuda mõni eriseadus. Niisiis peavad tegevusluba taotlema väärismetalli, vääriskivide kokkuostu ning hulgimüügi pakkujad. 2021. aastal väljastati üks tegevusluba, ühe ettevõtte puhul keelduti tegevusloa väljastamisest ning andmebüroo tunnistas kehtetuks seitse tegevusluba. Kokku esitati kaheksa tegevusloa taotlust, millest kolm olid uue tegevusloa ja viis muutmise taotlused. 2021. aasta lõpu seisuga oli 102 kehtivat tegevusluba väärismetalli, vääriskivide kokkuostu ning hulgimüügi pakkumiseks.

2021. aastal saatsid väärismetallide ja vääriskividega kauplejad andmebüroole 34 teadet ning ülejäänud kauplejad 60 teadet, neist 49 sularahateadet. Valdav enamus kauplejate teateid puudutasid sõidukite oste sularahas.

Riikliku riskihinnangu kohaselt on kauplejate puhul nii rahapesu kui ka terrorismi rahastamise oht alla keskmise. Peamiseks ohuks on kohatine vähene riskiteadlikkus. Samuti puuduvad kauplejatel vajalikud teadmised nii rahapesu kui ka terrorismiga seotud nõuetest, sh teavitamiskohustusest, kohustusest teha nii kliendi kui tehingutes osalevate kolmandate osapoolte kohta sisulisem taustakontroll ja tuvastada riikliku taustaga isikud. Kauplejad ei rakenda piisavalt hoolsusmeetmeid, mis võib kaasa tuua ohu, et nende kliendid kasutavad sektorit ära. Samas enamuse kauplejate puhul ei ole oht realiseeruv, kuna nende tegevusvaldkond või -mahud klientidega ei ole nii suured. Üksikutes valdkondades, nagu näiteks hulgimüügiga tegelejad ning autode müüjad, võib oht olla pisut suurem.

Riskiteadlikkust mõjutab ka esindusorganisatsioonide tegevus. Kauplejate sektor on mitmekesine ja puudub üks enamikku kauplejaid hõlmav esindusorganisatsioon. Esindusorganisatsioone on palju ning nende kutse- ja eetikastandardite tase, aktiivsus ja alamsektori hõlmavus varieeruvad.

Andmebüroo algatas 2021. aastal neli järelevalvemenetlust kunstiteostega kauplejate osas. Kohapealse kontrolli käigus vaadati hoolsusmeetmete täitmist. Järelevalvekontrollid näitasid, et peamisteks puudusteks olid kontrollitud kauplejate protseduurireeglite puudumine, isikusamasuse tuvastamata jätmine, riskihinnangu puudumine

ja andmete säilitamata jätmine. Isikusamasus tuleb seejuures tuvastada ka juhul, kui tegemist on tuntud inimesega või vana tuttavaga.

Aastal 2022 plaanib andmebüroo viia läbi kauplejatele koolituse, et tõsta teadlikkust rahapesu ja terrorismi rahastamisega seonduvatest riskidest, sh tutvustada riikliku riskihinnangu tulemusi ning anda juhiseid seadusest tulenevate kohustuste rakendamisel.

Kinnisvaravahendajad

Kinnisvarasektor on rahapesu ja terrorismi rahastamise tõkestamise osas üks nõrgemalt reguleeritud sektoreid. Kinnisvarafirmadel ja -vahendajatel puudub turule sisenemise kontrollmehhanism ja normid tehingute vahendamiseks. Mõningal määral kompenseerib seda kinnisvaratehingute regulatsioon, kus ostu-müügi tehingud vormistatakse notariaalselt ja fikseeritakse kinnistusraamatus.

Rahapesu ja terrorismi rahastamise tõkestamise seaduse mõistes on kohustatud isikuteks need isikud, kes vahendavad kinnisasja ostu või müüki ja kinnisasja kasutustehinguid, kui tehinguga kokku lepitav kasutustasu on vähemalt 10 000 eurot kuus. Seadus paneb nendele ettevõtjatele hoolsuskohustused kliendiga ärisuhte loomisel, samuti kliendisuhte jooksul andmebüroole teatamiskohustuse kahtlastest ja ebaharilikest tehingutest.

Äriregistris oli kinnisvarabüroode tegevus 2020. aastal registreeritud enam kui 2500 ettevõtjal, kinnisvara kui põhitegevusala on registreeritud ligi 1800 ettevõtjal. Veebist võib leida umbes 160 sektoris tegutsevat ettevõtjat. Osaliselt pakub neile katusorganisatsioonina abi Eesti Kinnisvarafirmade Liit, millel on ligikaudu 60 liiget. Üksikmaakleritele pakub väljaõpet ja annab kutsetunnistusi Eesti Kinnisvaramaaklerite Koda, mis hõlmab turul tegutsejatest samuti väikest osa. Kinnisvaravahendajad on läbi aastate saatnud andmebüroole vaid üksikuid teateid. 2021. aastal oli selliseid teateid kuus.

Riikliku riskihinnangu kohaselt on kinnisvaramaaklerite puhul nii rahapesu kui ka terrorismi rahastamise oht keskmine. Peamiseks ohuks on nii rahapesu kui terrorismi rahastamise vaates turuosaliste madal teadlikkus ning korrastamata turg, mis raskendab järelevalve tegemist ja turuosaliste koolitamist. Kuigi kinnisvaravahendajate hinnangul ollakse hästi kursis neile seadusega pandud kohustusega, on tegelikkuses hoolsuskohustuse täitmine juhuslik, suhtumine seaduses ettenähtud kohustuste täitmisse pigem tõrges ning parendamist vajab oskus ohumärke ära tunda. Kinnisvaravahendajad heidavad seadusandjatele ette, et neid on koormatud kohusega, mida neil ei ole võimalik täita ja pigem ei usuta, et rahapesu oleks Eesti kinnisvara valdkonnas tõsine oht.

2021. aastal algatas andmebüroo kaks järelevalvemenetlust ettevõtete osas, kelle põhitegevusalaks oli kinnisvara vahendamine. Kaugkontrollide käigus kontrolliti hoolsusmeetmete rakendamist. Peamisteks tuvastatud probleemideks on puudused riskihinnangutes, protseduurireeglites ning hoolsusmeetmete kohaldamisel; vead isikusamasuse tuvastamisel, tegeliku kasusaaja tuvastamata jätmine, puudused riikliku taustaga isiku tuvastamisel; andmete registreerimata jätmine ning puudused andmete säilitamise osas.

Kinnisvaravahendajate hoolduskohustuse täitmine on pigem juhuslik ning oskus ohumärke näha vajab parendamist.

2021. aasta lõpus tegi andmebüroo kinnisvarasektoris tegutsevatele isikutele koolituse. Koolitusel tutvustati riikliku riskihinnangu tulemusi ning rahapesu ja terrorismi rahastamise tõkestamise seadusest tulenevaid kohustusi. Samuti toodi välja peamised puudused, mis on tuvastatud järelevalvete käigus. Virtuaalsel koolitusel osales reaalajas 170 inimest.

Pandimajad

Eestis on pandimajapidajate teenuse eripäraks asjaolu, et vähem pakutakse asjade kokkuostuteenust ning peamiselt on teenus üles ehitatud väiksemahuliste lühiajaliste laenude andmisele käsipandi tagatisel, kus laenude summad on tihti alla 200 euro.

Kokku oli 2021. aasta lõpu seisuga kehtiv tegevusluba 113 pandimaja teenuse pakkujal. Aasta jooksul väljastas andmebüroo kaks tegevusluba, kokku esitati kuus tegevusloa taotlust, millest kaks olid uued ning neli tegevusloa muutmise taotlused.

Riikliku riskihinnangu kohaselt on pandimajade puhul nii rahapesu kui ka terrorismi rahastamise oht alla keskmise.

Andmebüroo algatas 2021. aastal järelevalve viie pandimajapidaja osas. Järelevalvemenetlustest kolm olid kohapealsed kontrollid. Ühe järelevalvemenetluse puhul oli tegemist täiskontrolliga (kontrolliti kõiki RahaPTS nõudeid) ning ülejäänute puhul kontrolliti hoolsusmeetmete rakendamist ettevõttes. Ühe järelevalve käigus loobus ettevõte tegevusloast vabatahtlikult ning teise menetluse käigus tühistas andmebüroo pandimajapidaja tegevusloa, sest ettevõtte jättis andmebüroo ettekirjutused korduvalt täitmata.

Järelevalvekontrollide käigus tuvastati peamised puudujäägid protseduurireeglites ning riskihinnangus. Protseduurireeglid olid ajakohastamata ega vastanud ettevõtte spetsiifilisele äritegevusele. Sama ilmnes ka riskihinnangu osas: oli juhtumeid, kus riskihinnang puudus ja ka neid, kus riskihinnang ei vastanud ettevõtte ärispetsiifikale.

Mittetulundussektor

2021. aasta lõpu seisuga oli Eestis enam kui 23 300 mittetulundusühingut ja 818 sihtasutust.

Vabaühendused on seaduse mõttes (RahaPTS § 2 lg 3) kohustatud isikuteks, kui neile tasutakse või nad tasuvad sularahas üle 5000 euro või sellega võrdväärse summa muus vääringus sõltumata sellest, kas tasutakse ühe maksena või mitme seotud maksena kuni aastase perioodi jooksul. 15. märtsil 2022 jõustunud seadusemuudatus määratleb vabaühendused kohustatud isikutena ka juhul, kui ollakse seotud riskiriigi või -jurisdiktsiooniga.

Mittetulundussektoris on riikliku riskihinnangu kohaselt rahapesurisk keskmine ja terrorismi rahastamise risk üle keskmise. Usuühenduste ja heategevusorganisatsioonide alamsektorites on peamisteks ohukohtadeks riigi puudulik ülevaade sektorist, turuosaliste madal riskiteadlikkus, puudulik klientide ja tehingupartnerite kontroll ja turuosaliste ebapiisav sanktsiooninimekirjade kontrollimine. Lisaks ka asjaolu, et isikute ringi määratlemine lävendipõhiste sularahatehingute alusel ei vasta vabaühendustega seonduvatele riskidele. Vabaühenduste teadlikkuse tõstmise vajadust terrorismi rahastamisest järeldati ka andmebüroo 2022. aastal ilmunud uuringus „Kõrgema terrorismi rahastamise riskiga mittetulundussektori ülevaade“[XI]. Nendest tulemustest kirjutame juba järgmises aastaraamatus.

Andmebüroo tutvustas usuühendustele siseministeeriumi korraldatud koolitusel 2021. aasta lõpus terrorismi rahastamise riske. Koolitusel osales 32 inimest.

Professionaalid

Terminit „professionaalid“ kasutatakse üldnimetusena advokaatide, notarite, kohtutäiturite, pankrotihaldurite, raamatupidamisteenuse jm õigusteenuse pakkujate puhul. Notarite üle teeb järelevalvet Notarite Koda, advokaatide üle Eesti Advokatuur ning ülejäänud professionaalide osas andmebüroo.
Riikliku riskihinnangu kohaselt on professionaalide puhul nii rahapesu kui terrorismi rahastamise risk alla keskmise. Probleemiks on osade turuosaliste kohatine madal riskiteadlikkus.

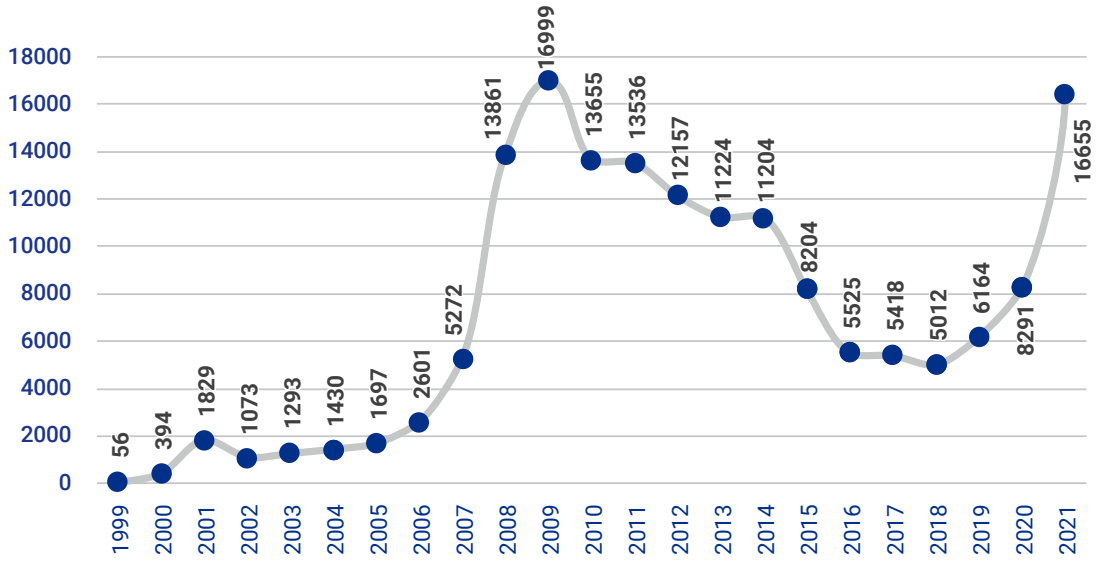
Professionaalid saatsid andmebüroole 2021. aastal 282 teadet. Sarnaselt varasemate aastatega olid aktiivseimad teataja notarid, kes edastasid 172 teadet, mis olid valdavalt seotud kinnisvaratehingutega, sh sularahas.

2021. aastal alustas andmebüroo järelevalvet üheksa pankrotihalduri osas, sh kaks järelevalvemenetlust olid kohapealsed ning seitse kaugkontrollid. Kõik järelevalvemenetlused keskendusid pankrotihaldurite teatamiskohustuse täitmisele. Puudusi tuvastati protseduurireeglites, sh ka järelevalvemenetluste eesmärgi ehk teavitamiskohustuse osas. Näiteks olid teadete esitamiseks kontaktandmed aegunud või ei olnud teate esitamiseks viidatud õigele veebilehele.

Andmebüroo koolitas 2021. aastal sektorit puudutavate riskide ning seadusest tulenevate kohustuste osas advokatuuri ning 2022. aasta alguses kohtutäitureid, pankrotihaldureid ja notareid. Kokku osales kolmel koolitustel üle 300 inimese.

2021. aasta arvudes

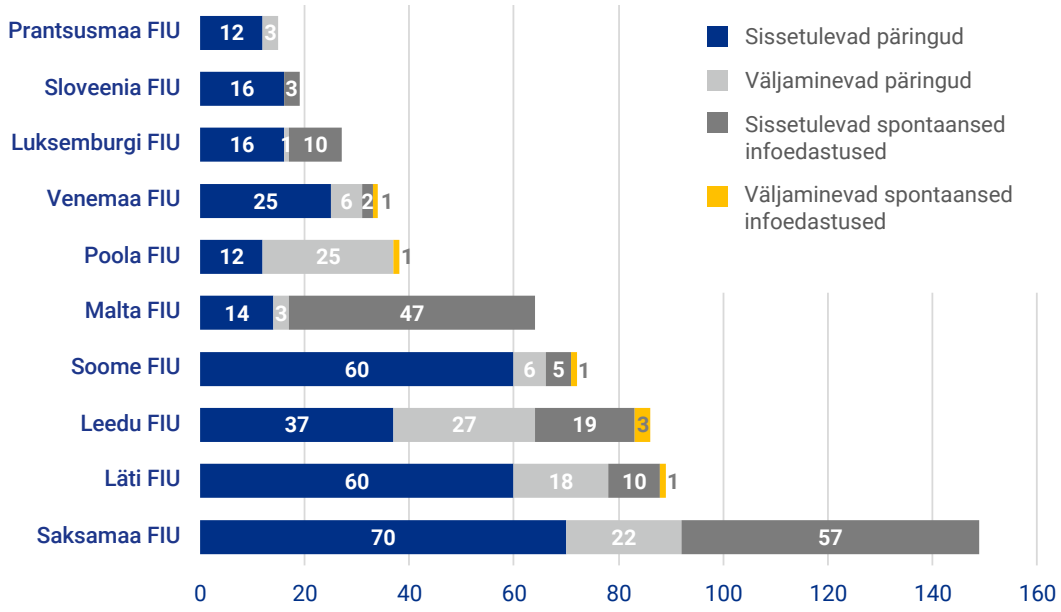
Teadete esitamine Rahapesu Andmebüroole



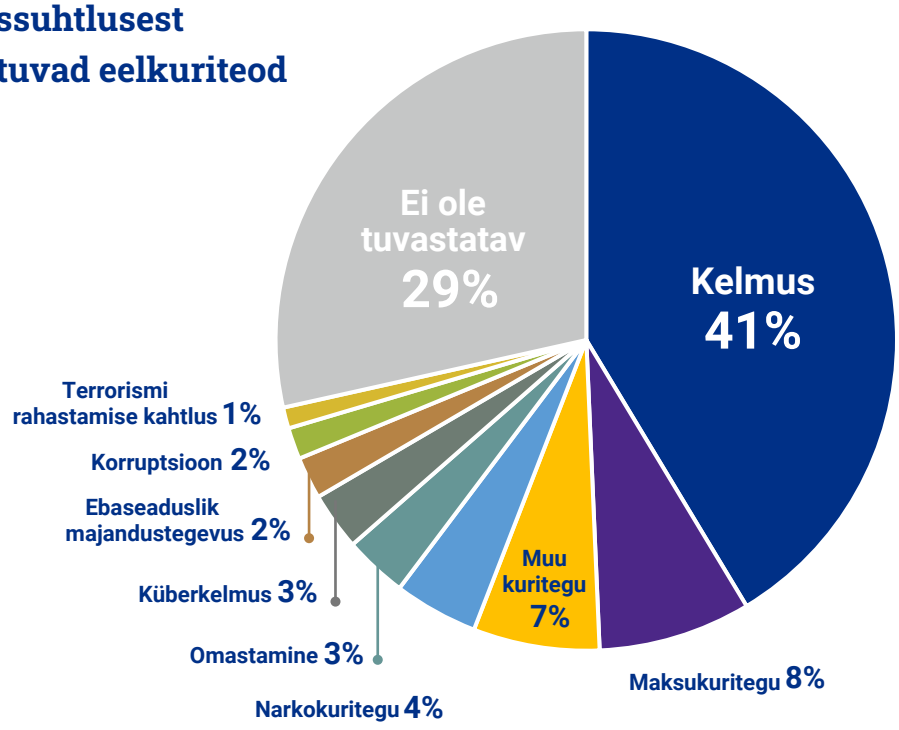
Teadete jagunemine tüübi ja esitanud sektori alusel

	Virtuaalvääringu teenusepakkujad	Krediidiasutused	Finantseerimis-asutus	Hasartmängu-sektor	Muud eraõiguslikud ettevõtjad	Professionaalid	Riigiasutused	Ei ole kohustatud subjekt	Välisriigi isikud ja asutused	KOKKU
Rahapesu kahtlusega teade (STR)	1273	10112	409	48	16	71	18	156	18	12121
Ebahariliku tegevuse teade (UAR)	253	509	253	5	2	30	9	23	14	1098
Ebahariliku tehingu teade (UTR)	255	367	151	4	11	50	5	1		844
Sularaha tehingu teade (CTR)	13	3	1049	86	74	122	12	5		1364
Rahvusvahelise sanktsiooni teade (ISR)	4	81	3		5	1	3		2	99
Terrorismi rahastamise kahtluse teade (TFR-2, end TFR)	4									4
Terrorismi rahastamise riski teade (TFR-1, end TR_UAR)	63	2	223		2	8	1			299
Päring							151		675	826
KOKKU	**1865**	**11074**	**2088**	**143**	**110**	**282**	**199**	**185**	**6485**	**16655**

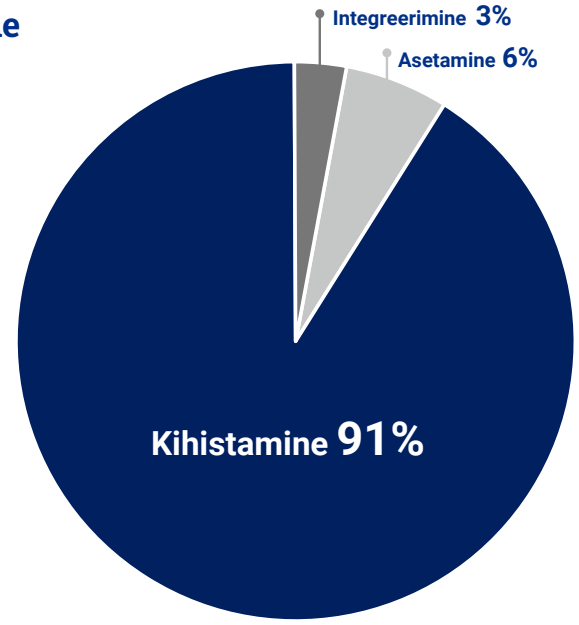
Rahapesu Andmebürooga kõige enam koostööd teinud välisriikide rahapesu andmebürood



Sissetulevast välissuhtlusest nähtuvad eelkuriteod



Toimikute jagunemine rahapesufaasides



Edastused ja käsutuspiirangud

22431
teadet

287
uurimisasutusele saadetud materjali

18 kuriteoteadet
174 materjali kriminaalasjaga liitmiseks
95 teabeks saadetud

32
käsutuspiirangut

15 30-päevast (2,22 mln €)
12 60-päevast (2,23 mln €)
5 1-aastast (20 000 €)

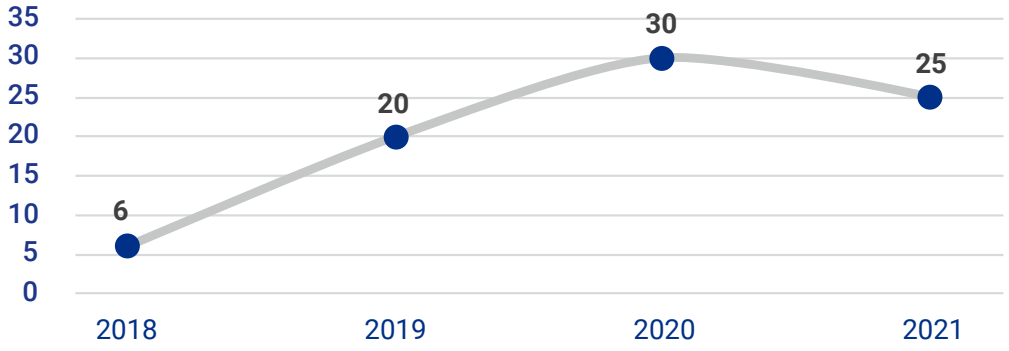
Finantssanktsiooni kohaldamine

REŽIIM	SANKTSIOONI SUBJEKT, SEOTUD ISIK	KASUTATUD MEETMED	ERAND	MEETME KUUPÄEV	SUMMA EURODES
EL nr 765/2006 Valgevene	**Alexandr Lukašenko**	ei tehtud kättesaadavaks		02.03.2021	**1363**
EL nr 269/2014 Ukraina	**Dmitry Konstantinovich Kiselyov**	külmutatud		27.04.2021	**441,58**
EL nr 269/2014 Ukraina	**Dmitry Konstantinovich Kiselyov**	külmutatud		06.05.2021	**111,36**
EL nr 765/2006 Valgevene	**Ojsc Belaz Management Company of Holding Belaz Holding**	ei tehtud kättesaadavaks		05.07.2021	**10 297,89**
EL nr 765/2006 Valgevene	**Jsc Minsk Automobile Plant-Belautomaz Holding Management Co**	vabastatud	erand	06.07.2021	**47 617,34**
EL nr 765/2006 Valgevene	**Jsc Minsk Automobile Plant-Belautomaz Holding Management Co**	ei tehtud kättesaadavaks		06.07.2021	**10 290,93**
EL nr 692/2014 Krimm	**Krimm**	ei tehtud kättesaadavaks		30.07.2021	**2,00**
EL nr 765/2006 Valgevene	**Mikhail Safarbekovich Gutseriev**	ei tehtud kättesaadavaks		02.08.2021	**94,50**
EL nr 765/2006 Valgevene	**Andrei Yurevich Pauliuchenka**	ei tehtud kättesaadavaks		01.09.2021	**1 575**
EL nr 269/2014 Ukraina	**Dmitry Konstantinovich Kiselyov**	külmutatud		30.08.20211	**245**
EL nr 765/2006 Valgevene	**Aleksandr Grigorievich Lukashenko**	ei tehtud kättesaadavaks		21.09.2021	**1 575,00**
EL nr 269/2014 Ukraina	**Dmitry Konstantinovich Kiselyov**	külmutatud		22.09.2021	**245,00**
EL nr 833/2014 Ukraina	**Gazprom Neft**	ei tehtud kättesaadavaks		29.10.2021	**609,73**
EL nr 833/2014 Ukraina	**Gazprom Neft**	külmutatud		29.10.2021	**36**
EL nr 765/2006 Valgevene	**Republican Subsidiary Unitary Enterprise Hotel Minsk**	ei tehtud kättesaadavaks		06.12.2021	**2359,98**
EL nr 765/2006 Valgevene	**Minskii Avtomobilnyi Zavod (MAZ)**	ei tehtud kättesaadavaks		17.12.2021	**400,00**
EL nr 765/2006 Valgevene	**Valgevene**	ei tehtud kättesaadavaks		30.12.2021	**500**
					73141,33

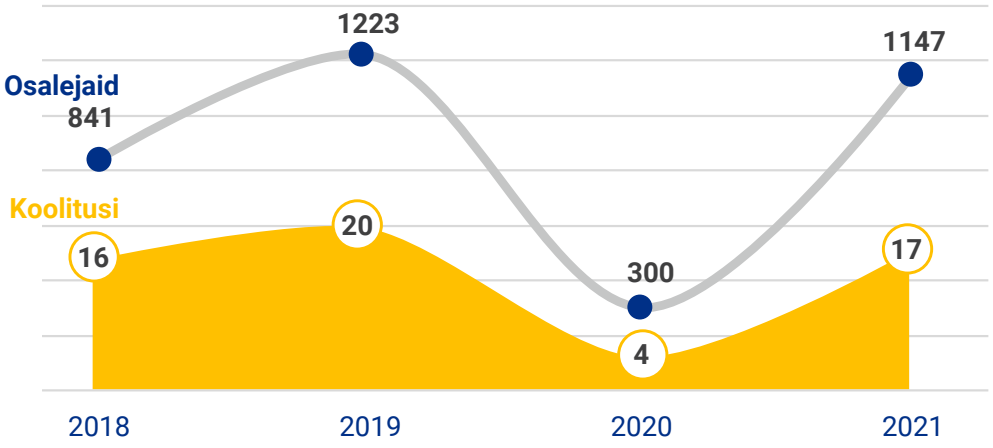
Tegevusload

	Uued taotlused		Tegevusloast keeldumine		Tagasi võetud taotlused	Tühistatud tegevusload	
	2020	2021	2020	2021	2021	2020	2021
Virtuaalvääringu teenuse pakkujad	480	161	155	18	57	1784	329
Usaldushalduse ja äriühingu teenuse pakkujad	45	31	3	2	6	3	7
Pandimajad	3	2	1				
Väärismetall	4	3		1	1		7
Finantseerimisasutused	50	35	7	4	6	17	27

Järelevalve kohapealsed kontrollid



Koolitused turuosalistele



Viiteid ja lisalugemist

I Eesti rahapesu ja terrorismi rahastamise tõkestamise siseriiklik riskihinnang. 2021. https://www.rahandusministeerium.ee/et/finants-ja-ettevotluspoliitika/rahapesu-ja-terrorismi-rahastamise-tokestamine

II Virtuaalvääringu teenuse pakkujatega seonduvad riskid Eestis. Rahapesu Andmebüroo, 2021. https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#virtuaalvringu-tee

III Kahtlaste tunnustega tehingute juhend. Rahapesu Andmebüroo, 2022. https://fiu.ee/oigusaktid-ja-juhendid/juhendid#juhend-kahtlaste-teh

IV Äriühinguteenuse pakkujatega seonduvad rahapesuriskid Eestis. Rahapesu Andmebüroo, 2021. https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#rahapesu-andmebroo-

V Baydakova, A. For $200, You Can Trade Crypto With a Fake ID. 19.10.2021. https://www.coindesk.com/policy/2021/10/19/for-200-you-can-trade-crypto-with-a-fake-id/

VI Christie's, 11.03.2021. https://onlineonly.christies.com/s/beeple-first-5000-days/beeple-b-1981-1/112924

VII Owen, A., Chase, I. NFTs: A New Frontier for Money Laundering? 2.12.2021. https://rusi.org/explore-our-research/publications/commentary/nfts-new-frontier-money-laundering

VIII Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art. Department of the Treasury, 2022. https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf

IX Europol Spotlight – Cryptocurrencies: Tracing the Evolution of Criminal Finances. Europol, 2021. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

X DeFi Takes on Bigger Role in Money Laundering But Small Group of Centralized Services Still Dominate. Chainalysis, 26.01.2022. https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/

XI Kõrgema terrorismi rahastamise riskiga mittetulundussektori ülevaade. Rahapesu Andmebüroo, 2021. https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#krgema-terrorismi-r

Rahapesu Andmebüroo

Finantstehingute aususe valvaja