

TARTU ÜLIKOOL
Sotsiaalteaduste valdkond
Johan Skytte poliitikauuringute instituut

Syrli Siimar

E-RESIDENTSUSE KAUDU ILMNEVATE FINANTSKURITEGEVUSE RISKIDE
REALISEERUMINE JA MAANDAMINE EESTI JA EUROOPA LIIDU REGULATIIVSES
RAAMISTIKUS

Magistritöö

Juhendaja: Mihkel Solvak, PhD

Tartu 2026

Autorsuse deklaratsioon

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

Töö sõnade arv: 22 480

Syrli Siimar 18.05.2026

Annotatsioon

Käesolev magistritöö uurib e-residentsusega seotud finantskuritegevuse riskide realiseerumist ja maandamist Eesti ja Euroopa Liidu regulatiivses raamistikus. Töö eesmärk on selgitada, miks ja kuidas e-residentsusega seotud riskid piiriüleses digitaalses keskkonnas avalduvad ning mil määral vastavad olemasolevad regulatiivsed ja järelevalvemehhanismid riskide tegelikule olemusele.

Teoreetiliselt tugineb töö kriminogeensete asümmeetriate teooriale, mille kaudu analüüsitakse informatsioonilisi, regulatiivseid, jurisdiktsioonilisi ja institutsionaalseid ebakõlasid. Uurimus põhineb kvalitatiivsel uurimisstrateegial, ühendades dokumendianalüüsi ning poolstruktureeritud intervjuud valdkonna ekspertidega. Analüüsis kaardistatakse empiiriliselt tuvastatud riskimustrid, seostatakse need kriminogeensete asümmeetriatega ning hinnatakse riskide ennetamise, tuvastamise ja neile reageerimise mehhanisme.

Töö tulemused näitavad, et e-residentsusega seotud finantskuritegevuse riskid ei tulene e-residendi staatusest otseselt, vaid avalduvad eelkõige Eestis registreeritud ettevõtte, digitaalse identiteedi ja piiriülese majandustegevuse koosmõjus. Peamiste riskimehhanismidena eristuvad juriidiline vorm kui „legaalne fassaad“, identiteedi ja jurisdiktsiooni kaudu loodud varjatus ning professionaalsete vahendajate roll riskide kujunemisel.

Magistritööst järeldub, et e-residentsuse riskikeskkonda iseloomustab struktuurne lahknevus piiriülese digitaalse majandustegevuse ja territoriaalselt korraldatud järelevalve vahel. Kuigi olemasolevad mehhanismid võimaldavad riske osaliselt maandada, piiravad nende toimivust eeskätt eelkontrolliks vajaliku teabe ebaühtlane kvaliteet ja kättesaadavus, rahvusvahelise infovahetuse piiratus ning professionaalsete vahendajate hoolsus- ja teatamiskohustuse ebapiisav täitmine. Seetõttu toob e-residentsuse juhtum esile Euroopa Liidu piiriülese digitaalse ettevõtluskeskkonna ja territoriaalse järelevalvemudeli süsteemsed piirangud. Laiemas tähenduses osutab töö pingele programmi majanduslike ja strateegiliste eesmärkide ning järelevalvevõimekuse vahel.

Abstract

This master's thesis examines the realisation and mitigation of financial crime risks related to e-Residency within the regulatory framework of Estonia and the European Union. The aim of the thesis is to explain why and how risks related to e-Residency emerge in a cross-border digital environment, and to assess the extent to which existing regulatory and supervisory mechanisms correspond to the actual nature of the risks.

Theoretically, the thesis draws on the theory of criminogenic asymmetries, which is used to analyse informational, regulatory, jurisdictional and institutional misalignments. The study is based on a qualitative research strategy, combining document analysis with semi-structured interviews with experts in the field. The analysis maps empirically identified risk patterns, links them to criminogenic asymmetries, and assesses the mechanisms through which risks are prevented, detected and responded to.

The findings show that financial crime risks related to e-Residency do not arise directly from e-resident status but emerge primarily through the interaction between an Estonia-registered company, digital identity and cross-border economic activity. Three main risk mechanisms are identified: the use of legal form as a “legal façade”, concealment created through identity and jurisdiction, and the role of professional intermediaries in the formation of risks.

The thesis concludes that the e-Residency risk environment is characterised by a structural misalignment between cross-border digital economic activity and territorially organised supervision. Although the existing mechanisms allow risks to be mitigated to some extent, their effectiveness is limited primarily by the uneven quality and availability of information needed for preliminary checks, the limited nature of international information exchange, and the insufficient fulfilment of due diligence and reporting obligations by professional intermediaries. The case of e-Residency therefore highlights the systemic limitations of the European Union's cross-border digital business environment and territorially based supervisory model. More broadly, the thesis points to a tension between the programme's economic and strategic objectives and the state's supervisory capacity.

Sisukord

Lühendid.....	7
Sissejuhatus	8
1. E-residentsuse programm.....	11
1.1. E-residentsuse programmi olemus.....	11
1.2. E-residentsus kui digitaaldiplomaatia ja pehme jõu instrument.....	14
1.3. E-residentsuse institutsionaalne ja regulatiivne raamistik.....	15
1.3.1. Institutsionaalse vastutuse ja järelevalve jaotus Eesti tasandil	16
1.3.2. Institutsionaalse vastutuse ja järelevalve jaotus Euroopa Liidu tasandil	19
2. Teoreetiline raamistik.....	24
2.1. Transnatsionaalne kuritegevus ja kriminogeensed asümmeetriad.....	25
2.2. Finantskuritegevuse riskid e-residentsuse kontekstis	30
2.2.1. Rahapesu olemus ja kolmeastmeline mudel	30
2.2.2. E-residentsuse programmiga kaasnevad süsteemsed riskid.....	31
2.3. Riskipõhise regulatsiooni teoreetilised alused.....	33
2.4. Analüütiline mudel: kriminogeensete asümmeetriate rakendamine e-residentsuse kontekstis	35
3. Metoodika ja andmeallikad	38
3.1. Kvalitatiivne uurimisstrateegia ja meetodite põhjendus.....	38
3.2. Uurimismeetodid	39
3.2.1. Dokumendianalüüs	39
3.2.2. Poolstruktureeritud ekspertintervjuud.....	41
3.3. Analüütiline raamistik ja metoodilised piirangud.....	43
4. Empiiriline analüüs	46
4.1. E-residentsusega seotud finantskuritegevuse riskide realiseerumine.....	47
4.1.1. Realiseerunud riskimustrid ja juhtumianalüüs.....	47
4.1.2. E-residentidega seotud välispäringute statistika	58
4.1.3. E-residendid kriminaalmenetlustes ja kohtuasjades	60
4.1.4. E-residendi staatuse omandamisega seotud realiseerunud riskid: eel- ja järelkontrolli haavatavused	61
4.2. Ekspertintervjuude tulemused	64
4.2.1. Riskide avaldumine praktikas	64
4.2.2. Koostöö ja andmevahetuse mehhanismid	67
4.2.3. Riskide maandamise strateegiad ja tulevikuvaade.....	68
4.2.4. Kriminogeensed asümmeetriad ja süsteemsed lõhed.....	69

5. Analüüs ja tulemused	73
5.1. Riskide realiseerumine ja regulatiivne vastus	74
5.1.1. Juriidiline vorm kui „leaalne fassaad“ piiriülestes skeemides	74
5.1.2. Identiteedi ja jurisdiktsiooni kaudu loodud varjatus	77
5.1.3. Professionaalsed vahendajad kui asümmeetriate kujundajad	81
5.2. Regulatiivse süsteemi toimivus ja struktuursed piirangud	83
Kokkuvõte	86
Kasutatud allikad	89
Lisad	95

Lühendid

AMLA – *Anti-Money Laundering Authority* – Euroopa Liidu rahapesu ja terrorismi rahastamise tõkestamise amet

AMLD – *Anti-Money Laundering Directive* – Euroopa Liidu rahapesu tõkestamise direktiiv

ECRIS – *European Criminal Records Information System* – Euroopa karistusregistrite infosüsteem

eIDAS – *Electronic Identification, Authentication and Trust Services Regulation* – Euroopa Liidu määrus elektroonilise identiteedi ja usaldusteenuste kohta

EIS – Ettevõtluse ja Innovatsiooni Sihtasutus

FATF – *Financial Action Task Force* – rahvusvaheline organisatsioon, mis kehtestab rahapesu ja terrorismi rahastamise tõkestamise standardeid

FI – Finantsinspektsioon

GDPR – *General Data Protection Regulation* – Euroopa Liidu isikuandmete kaitse üldmäärus

ITDS – Isikut tõendavate dokumentide seadus

KAPO – Kaitsepolitseiamet

KYC – *Know Your Customer* – kliendi tuvastamise ja tundmise põhimõte

MKM – Majandus- ja Kommunikatsiooniministeerium

MONEYVAL – *Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism* – Euroopa Nõukogu ekspertkomitee, mis hindab riikide rahapesu tõkestamise süsteeme

MTA – Maksu- ja Tolliamet

PPA – Politsei- ja Piirivalveamet

RAB – Rahapesu Andmebüroo

RahaPTS – Rahapesu ja terrorismi rahastamise tõkestamise seadus

RIA – Riigi Infosüsteemi Amet

SOCTA – *Serious and Organised Crime Threat Assessment* – Europol'i raport raske ja organiseeritud kuritegevuse trendidest

VASP – *Virtual Asset Service Provider* – virtuaalvääringu teenusepakkuja

Sissejuhatus

E-residentsuse programm on alates selle käivitamisest 2014. aastal kujunenud üheks Eesti digiriigi keskseks innovatsiooniks, mis võimaldab välisriikidest pärit isikutel kasutada Eesti e-teenuseid ning osaleda riigi ettevõtluskeskkonnas sõltumata füüsilisest asukohast. Digitaalse identiteedi kaudu loodud ligipääs riigi digitaalsele taristule on laiendanud traditsioonilist arusaama riigi piiridest, sidudes Eesti majandus- ja haldussüsteemi globaalse kasutajaskonnaga. Selline areng on toonud Eestile märkimisväärset rahvusvahelist tähelepanu ning kinnistanud selle kuvandit innovaatilise digiriigina.

Digitaalsete võimaluste laienemine ei tähenda aga üksnes uusi majanduslikke eeliseid, vaid loob ka uusi väljakutseid riigi regulatsiooni- ja järelevalvevõimekusele. E-residentsuse kaudu loodud ettevõtted tegutsevad enamasti piiriüleses keskkonnas, kus majandustegevus, juhtimine ja rahavood paiknevad erinevates jurisdiktsioonides. Selline hajutatuse muudab nii riskide tuvastamise kui ka nende maandamise keerukamaks ning paneb proovile riigi suutlikkuse tagada oma digitaalse infrastruktuuri usaldusväärsus.

Seda kinnitavad ka erinevad analüüsid ja hinnangud, mis viitavad sellele, et e-residentsusega seotud riskid ei ole pelgalt teoreetilised, vaid on ka praktikas avaldunud. Riigikontrolli audit tõi juba 2020. aastal esile puudujääke e-residentide taustakontrollis ja järelkontrollis, viidates olukordadele, kus e-residenti staatuse on saanud isikud, kelle taust oleks pidanud seda välistama. Kaitsepolitseiamet (KAPO) on tuvastanud e-residentsusega seotud julgeolekuriske, sealhulgas äärmuslusega seotud isikute osalust programmis. Rahapesu Andmebüroo (RAB) ning Rahandusministeeriumi analüüsid osutavad omakorda sellele, et e-residentsuse kaudu loodud ettevõtteid kasutatakse piiriülestes finants skeemides, sealhulgas rahapesuks, maksupettusteks ja sanktsioonide rikkumiseks. Ka rahvusvahelised hinnangud, näiteks Euroopa Nõukogu rahapesu ja terrorismi rahastamise vastaste meetmete hindamise ekspertkomitee Moneyvali raport, rõhutavad, et e-residentsuse programmiga kaasnevad süsteemsed haavatavused, eeskätt tegelike kasusaajate tuvastamise ja järelevalve osas.

Hoolimata eelnevates raportites esile toodud riskidest on e-residentsuse programmi käsitletud eelkõige digitaalse innovatsiooni, majandusliku mõju ning digitaaldiplomaatia ja pehme jõu perspektiivist (Hoffmann & Solarte-Vasquez, 2022; Nye, 2004). Senistes käsitlustes on tähelepanu koondunud eeskätt programmi toimimisele ja mõjudele, kuid vähem on käsitletud e-residentsusega seotud finantskuritegevuse riskide praktilist realiseerumist ning olemasolevate regulatiivsete ja järelevalvemehhanismide suutlikkust neid riske maandada. Eriti oluline on see

Euroopa Liidu (EL) kontekstis, kus e-residentsuse kaudu loodud ettevõtted saavad ligipääsu siseturule ning võivad seeläbi mõjutada laiemat finantskeskkonda ja selle usaldusväärsust.

Nende riskide mõistmiseks tuleb e-residentsust vaadelda EL-i mitmetasandilises regulatiivses raamistikus toimiva riikliku haldusmeetmena, mille normatiivset keskkonda kujundavad EL-i tasandi õigusaktid ja institutsioonid, kuid mille riskide tuvastamine ja järelvalve realiseeruvad valdavalt riiklike institutsioonide tasandil. Käesolevas magistritöös käsitletakse regulatiivset raamistikku laiemas tähenduses, hõlmates lisaks õigusnormidele ka institutsionaalset korraldust, järelvalvemehhanisme ning nende praktilist rakendamist. Selline lähenemine võimaldab analüüsida mitte üksnes regulatsiooni formaalset olemasolu, vaid ka selle tegelikku toimimist ja tõhusust ning käsitleda e-residentsusega seotud riske laiemas piiriülese kuritegevuse kontekstis.

Käesoleva magistritöö uurimisprobleem seisneb selles, et e-residentsus on loonud piiriülese majandus- ja regulatiivse keskkonna, kus finantskuritegevuse riskide avaldumine ja maandamine ei piirdu ühe riigi tasandiga. Samal ajal on olemasolevad regulatiivsed ja järelvalvemehhanismid hajutatud erinevate institutsioonide ja tasandite vahel ega pruugi olla täielikult kohandunud e-residentsusega seotud riskide piiriülese ja digitaalse olemusega.

Töö eesmärk on seostada empiiriliselt tuvastatud e-residentsusega seotud finantskuritegevuse riskimustrid ja institutsionaalsed praktikad kriminogeensete asümmeetriate teooriaga, et hinnata, mil määral vastavad Eesti ja EL-i regulatiivsed ning järelvalvemehhanismid nende riskide tegelikule olemusele ning millised struktuursed tegurid piiravad nende toimivust piiriüleses digitaalses keskkonnas.

Sellest tulenevalt on tööl kaks uurimisküsimust:

1. Miks ja kuidas realiseeruvad e-residentsusega seotud finantskuritegevuse riskid kriminogeensete asümmeetriate kontekstis?
2. Milliste regulatiivsete ja järelvalvemehhanismide kaudu neid riske Eesti ja EL-i raamistikus maandatakse ning mil määral vastavad need riskide tegelikule olemusele?

Uurimisküsimustele vastamiseks kasutatakse kvalitatiivset uurimisstrateegiat, mis põhineb dokumendianalüüsil ja poolstruktureeritud ekspertintervjuudel. Dokumendianalüüsi käigus kaardistatakse e-residentsusega seotud finantskuritegevuse riskide avaldumisvormid ja korduvad riskimustrid, tuginedes riiklikele ja rahvusvahelistele raportitele, riskihinnangutele

ning juhtumipõhiste allikatele. Ekspertintervjuud võimaldavad täiendada dokumendianalüüsi praktikatasandi hinnangutega selle kohta, kuidas riskid avalduvad, milliste mehhanismide kaudu neid maandatakse ning milliseid regulatiivseid ja järelevalvelisi kitsaskohti institutsioonid praktikas tajuvad. Selline meetodite kombinatsioon võimaldab siduda dokumentides tuvastatud riskimustrid ekspertide hinnangutega ning tõlgendada neid töö teoreetilise ja analüütilise raamistiku abil, andes tervikliku hinnangu süsteemi toimimisele.

Töö on üles ehitatud järgmiselt. Esimeses peatükis antakse ülevaade e-residentsuse programmi olemusest ja toimimisest, käsitletakse selle rolli digitaaldiplomaatia ja pehme jõu instrumendina ning kaardistatakse programmi institutsionaalne ja regulatiivne raamistik nii Eesti kui ka EL-i tasandil. Teises peatükis esitatakse töö teoreetiline raamistik, keskendudes transnatsionaalse kuritegevuse, kriminogeensete asümmeetriate, finantskuritegevuse ning riskipõhise regulatsiooni käsitlestele. Kolmandas peatükis kirjeldatakse uurimismetoodikat ja andmeallikaid. Neljandas peatükis esitatakse empiiriline analüüs, kus kaardistatakse e-residentsusega seotud riskide realiseerumine ning analüüsitakse ekspertintervjuude tulemusi. Viiendas peatükis sünteesitakse tulemused, seostatakse empiirilised riskimustrid kriminogeensete asümmeetriatega ning hinnatakse regulatiivsete ja järelevalvemehhanismide toimivust riskide maandamisel. Töö lõpetab kokkuvõtte, kus esitatakse peamised järeldused ja võimalikud edasiarendused.

1. E-residentsuse programm

1.1. E-residentsuse programmi olemus

E-residentsuse programm loodi 2014. aasta 1. detsembril eesmärgiga pakkuda välisriikide kodanikele turvalist ligipääsu Eesti e-teenustele ning võimalust osaleda Eesti ettevõtluskeskkonnas. E-residentsuse programmi ametliku veebilehe järgi on Eesti „esimene riik maailmas, mis pakub väliskodanikele võimalust e-residendina osa saada oma arenenud digiriigi e-teenustest ning asutada EL-i ettevõtte 100% kaugteel ja asukohast sõltumata“ (E-Residency, s.a.).

Programmi algse kontseptsiooni kohaselt nähti e-residentsust vahendina, mis võimaldab laiendada Eesti digiriigi teenuseid üle territoriaalsete piiride ning kujundada transnatsionaalset digitaalse ettevõtluse keskkonda, kus ettevõtjad saavad osaleda sõltumata füüsilisest asukohast (Kotka jt., 2015, lk 4). Programmi üheks keskseks eesmärgiks on soodustada Eesti majanduse, teaduse, hariduse ja kultuuri arengut (Isikut tõendavate dokumentide seadus, 1999/2025).

E-residentsuse keskmeks on riiklikult väljastatud digitaalne identiteet, mis võimaldab kasutajal end Eesti e-teenustes turvaliselt autentida ja kasutada elektroonilise allkirja funktsiooni. Selle identiteedi tehniliseks kandjaks on e-residendile väljastatav digitaalne isikutunnistus (digi-ID), mida kasutatakse üksnes elektroonilistes keskkondades. See võimaldab e-residendil Eesti e-teenustes oma isikut turvaliselt tõendada, kuid ei anna õigust füüsiliseks riigis viibimiseks ning ei kaasa kodakondsust, maksuresidentsust ega elamisluba. Digi-ID kehtivusaeg on viis aastat, pärast mida tuleb taotleda uue kaardi väljastamist (E-Residency, s.a.).

Lisaks riiklikele digiteenustele toimib e-residentsus ka laiemas ettevõtlusökosüsteemis, mida toetab ulatuslik erasektori teenusepakkujate võrgustik (*marketplace*). Selles võrgustikus tegutseb üle 150 rahvusvahelise teenusepakkuja, kes pakuvad e-residentidele muu hulgas raamatupidamis-, juriidilisi ja ettevõtte haldamise teenuseid. Nende hulka kuuluvad ka äriühinguteenuse pakkujad, kelle teenused hõlmavad ettevõtete asutamist, juhtimis- ja kontaktisikuteenuseid. (E-Residency, s.a.)

Alates 2014. aasta 1. detsembrist on e-residendiks saanud üle 135 000 inimese (v.a tühistatud staatus) 185 erinevast riigist. Ligikaudu 50% e-residentidest on pärit EL-i riikidest. 2026. aasta alguses on kehtivaid e-residendi digi-ID kaarte käibel üle 63 000 ja 2025. aastal lisandus e-residente juba 20% rohkem kui 2024. aastal. Enim e-residentsuse taotlusi tuli Saksamaalt, Prantsusmaalt ning Ukrainast. Taotluste arvu poolest on olulisteks kasvuturgudeks ka Itaalia, Ühendkuningriik ning Ladina-Ameerika riigid. (Ristoja, 2026)

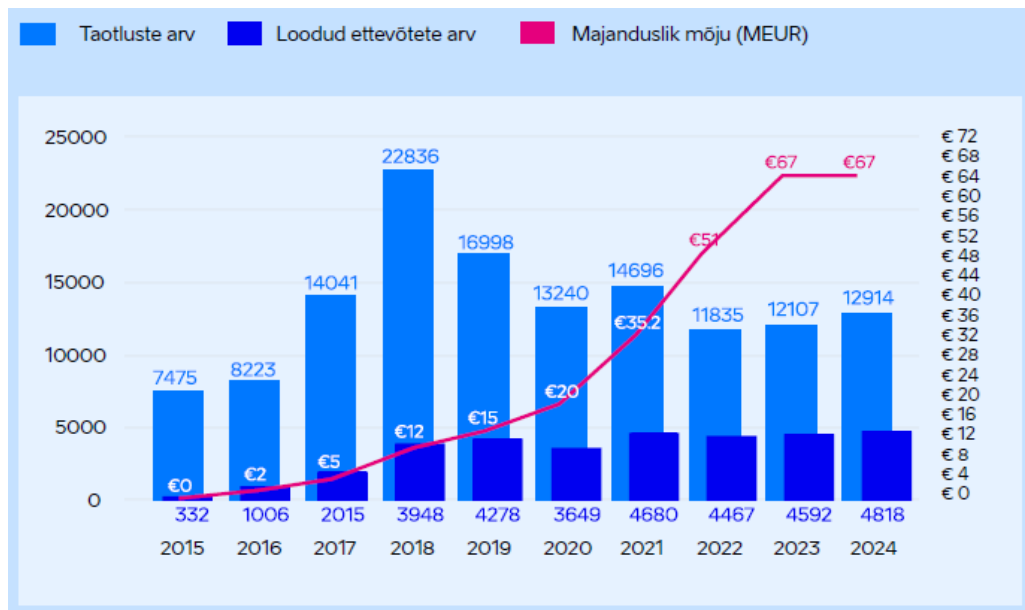
Märkimisväärse osa e-residentidest moodustavad EL-i väliste ehk kolmandate riikide kodanikud. Enim taotlusi kolmandatest riikidest tuleb Ukrainast, Türgist, Hiinast, Indiast ja Pakistanist, mis moodustavad 21% kõigist taotlejatest (EIS, 2025). Kuni 2022. aastani olid ka Venemaa kodanikud püsivalt taotlejate esiviisikus, kuid 2022. aasta märtsis lõpetati Venemaa ja Valgevene kodanikele uute e-residendi digi-ID-de esmane väljastamine (EIS, 2025; Rahandusministeerium, 2025).

E-residendi digi-ID taotlemisel on taotlejad märkinud valdavaks põhjuseks Eestis ettevõtte loomise (73,1%). Samas omab ettevõtlusseost ligikaudu 34% kehtivatest e-residentidest ja e-residentide asutatud ettevõtetest olid aktiivsed omakorda umbes 53% (Rahandusministeerium, 2025). E-residendid asutavad iga viienda uue Eesti ettevõtte aastas: läbi aegade on e-residendid loonud üle 39 000 Eesti ettevõtte. 2025. aastal asutasid kõige enam uusi Eesti ettevõtteid Ukraina, Hispaania, Türgi, Saksamaa ja Prantsusmaa kodakondsusega e-residendid. (Ristoja, 2026)

Suur osa e-residentide loodud ettevõtetest tegutseb digitaalses või teenuspõhises majanduses, näiteks tarkvaraarenduse, konsultatsiooni ja juhtimisteenuste valdkonnas, mis võimaldab ettevõtlustegevust korraldada asukohast sõltumatult. Nendele järgnevad tegevusalad nagu jaekaubandus, turundus- ja reklaamiteenused, finants- ja investeerimistegevus ning muud kutse- ja tehnilised teenused. (E-Residency dashboard, s.a.)

Programmi majandusliku mõju mõõtmise aluseks on riiklikult kinnitatud mudel, mis võtab arvesse e-residentide Eesti ettevõtete tasutud tööjõumakse ja erijuhtude tulumaksu (valdavalt dividendidelt). E-residentsuse majanduslik mõju on Ristoja (2026) sõnul läbi aegade olnud ligi 400 miljonit eurot. 2025. aastal hinnati e-residentsuse programmi majanduslikku mõju riigile kokku 124,9 miljonit eurot. Sellest ligikaudu pool moodustasid erijuhtude tulumaks, veidi alla poole tööjõumaksud ning väiksema osa e-residentsuse taotlemise ja ettevõtte asutamise riigilõivud (Ristoja, 2026).

Joonisel 1 on esitatud e-residentsuse programmi arengunäitajad aastatel 2015–2024. Taotluste arv, loodud ettevõtete arv ja majanduslik mõju kajastavad vastava aasta näitajaid. Majanduslik mõju tähistab programmi hinnangulist iga-aastast majanduslikku tulemust ja maksutulu, mitte programmi algusest arvutatud kumulatiivset kogumõju.



Joonis 1. E-residentsuse programmi tulemused 2018–2024 (EIS, jätkustrateegia, 2025)

Kui veel 2020. aastal juhtis Riigikontroll tähelepanu sellele, et e-residentsuse majandusliku mõju hindamisel võis probleemiks olla e-residentide loodud ettevõtete ja laiemalt e-residentidega seotud ettevõtete ebapiisav eristamine (Riigikontroll, 2020), siis hiljem on programmi maksutulu hindamise metoodikat täpsustatud. E-residentsuse programm eristab nüüd otsesemat ja kaudsemat majanduslikku mõju ning seob maksutulu arvestuse kitsamalt e-residentide loodud ettevõtetega (Ristoja, 2026).

Kuigi metoodika täpsustamine muudab majandusliku mõju arvestuse varasemast kitsamaks ja täpsemaks, jääb probleemiks näitajate piiratud läbipaistvus ning e-residentidega seotud ettevõtete tegelik majanduslik aktiivsus. Riigikontroll märkis 2020. aastal, et makse maksis vaid 6% e-residentide loodud ettevõtetest, Moneyvali 2022. aasta hindamisaruande järgi ei olnud ligikaudu 80% e-residentide asutatud ettevõtetest Eestis majanduslikult aktiivsed ning 2025. aastal asutatud ettevõtetest tasus makse vaid 17% (Riigikontroll, 2020; Moneyval, 2022; Ristoja, 2026). Ka RAB-i 2024. aasta analüüs, mille kohaselt kustutati äriregistri korrastamise käigus 24% ajalooliselt e-residendi seost omanud ettevõtetest, viitab sellele, et märkimisväärne osa sellistest ettevõtetest ei ole olnud sisuliselt aktiivsed (RAB, 2024b).

Ka e-residentsuse jätkustrateegia 2026–2029 nendib, et e-residentsus on olnud atraktiivne eelkõige mikroettevõtetele, mis ei ole toonud riigile oodatud maksutulu, mistõttu on programmi uus fookus seatud nn „tuleviku suurtele ettevõtetele“ (*future large businesses*), kellel on pikemas perspektiivis suurem maksutulu potentsiaal (EIS, 2025). See viitab, et senine mudel ei ole toonud oodatud majanduslikku tulemust ning programm püüab seda korrigeerida.

1.2. E-residentsus kui digitaaldiplomaatia ja pehme jõu instrument

E-residentsuse loomine 2014. aastal oli osa Eesti strateegilisest eesmärgist laiendada digitaalse riigi infrastruktuuri kasutamist ka väljapoole riigi territoriaalseid piire (Kotka jt., 2015). Selline lähenemine laiendab riigi toimimise traditsioonilist territoriaalset loogikat, kuna digitaalne identiteet võimaldab osaleda riigi majandus- ja haldussüsteemis ilma füüsilise kohalolekuta (Kotka jt., 2016). E-residentsuse programmi on seetõttu käsitletud ka kui Eesti digiriigi kuvandi kujundamise vahendit, mis toetab laiemat „e-Estonia“ narratiivi ning aitab positsioneerida Eestit rahvusvaheliselt innovaatilise ja tehnoloogiliselt arenenud riigina (Tamppuu & Masso, 2018; Hoffmann & Solarte, 2022). Väikeriigi kontekstis võimaldab selline strateegiline narratiiv suurendada riigi nähtavust ja mõju, demonstreerides Eesti digivalitsemise lahendusi rahvusvahelisele publikule (Hardy, 2023).

Samas ei saa e-residentsust käsitleda üksnes tehnilise digitaalse identiteedilahendusena, vaid seda tuleb mõista ka laiemalt institutsionaalse ja organisatsioonilise süsteemina, mis hõlmab erinevaid avaliku ja erasektori osapooli ning nendevahelisi koostoimeid. Selline käsitus võimaldab analüüsida e-residentsust mitte ainult üksikute teenuste kogumina, vaid tervikliku ökosüsteemina, mille toimimine sõltub nii tehnoloogilisest kui ka institutsionaalsest disainist. (Sallam jt., 2022)

Rahvusvaheliste suhete teooria perspektiivist võib e-residentsust käsitleda ka digitaaldiplomaatia ja pehme jõu instrumendina. Pehme jõud põhineb riigi võimel mõjutada teisi läbi ideede, väärtuste ja institutsioonide atraktiivsuse, mitte sõjalise või majandusliku surve kaudu (Nye, 2004). Sellest lähtuvalt on e-residentsus käsitletav mehhanismina, mille kaudu Eesti püüab kujundada rahvusvahelist kuvandit ja suurendada oma mõjukust digitaalses keskkonnas, omades seejuures ka laiemat poliitilist ja strateegilist tähendust riigi välissuhtluses (Hoffmann & Solarte, 2022). Empiiriline analüüs kinnitab selle lähenemise paikapidavust: Blue (2020) näitab, et e-residentsuse kasutamine muudab e-residentide hoiakuid Eesti suhtes märgatavalt positiivsemaks ning seob nad riigi väärtuste ja digitaalse identiteediga (Blue, 2020).

E-residentsus ei toimi seega üksnes kuvandiloome vahendina, vaid loob välisriikide ettevõtjatele ja spetsialistidele praktilise kokkupuute Eesti digitaalse ökosüsteemiga (Kimmo, Pappel & Draheim, 2018). Selle kaudu kujuneb rahvusvaheline e-residentide kogukond, mida võib käsitleda Eesti pehme jõu võrgustikuna: e-residendid mitte ainult ei vahenda Eesti digiriigi kuvandit, vaid osalevad selle kaasloomes oma igapäevase tegevuse kaudu (Blue, 2020).

Kuigi e-residentsus loob Eestile pehme jõu kaudu märkimisväärsed rahvusvahelist nähtavust, kaasneb digitaalse infrastruktuuri avamisega rahvusvahelisele kasutajaskonnale vajadus tasakaalustada avatust ja turvalisust, kuna sellega seotud riskid võivad mõjutada nii programmi usaldusväärsust kui ka riigi mainet. Digitaalne identiteet ja piiriülene ettevõtlus võivad luua võimalusi väärkasutuseks, mistõttu sõltub programmi usaldusväärsus tõhusatest regulatiivsetest ja järelevalvemehhanismidest. Seejuures võib tekkida pinge e-residentsuse kaudu kujundatud kuvandi ning tegelike riskide vahel, mis viitab sellele, et e-residentsus ei ole üksnes pehme jõu instrument, vaid ka kompleksne poliitikainstrument, kus põimuvad riigi kuvand, majandushuvid ja regulatiivsed riskid.

Need küsimused muutuvad eriti oluliseks piiriülese majandustegevuse kontekstis, kus digitaalse identiteedi abil loodud ettevõtted võivad tegutseda samaaegselt mitmes jurisdiktsioonis ning kus regulatiivne killustatus loob täiendavaid riske. Sellises keskkonnas võivad erinevused riikide regulatsioonides, järelevalvesüsteemides ja institutsionaalses pädevuses luua võimalusi kuritegelikuks tegevuseks (Masso jt., 2024; Sullivan & Burger, 2017).

1.3. E-residentsuse institutsionaalne ja regulatiivne raamistik

Eeltoodust tulenevalt käsitletakse e-residentsust käesolevas töös piiriülese majandus- ja haldusruumina, mille toimimine sõltub digitaalsest taristust, ettevõtlusökosüsteemist ning riiklikest ja EL-i tasandi järelevalvemehhanismidest.

Piiriüleste e-teenuste ja digitaalsete identiteetide areng on toonud kaasa olulisi muutusi selles, kuidas riigid ja supranatsionaalsed organisatsioonid teostavad regulatiivset järelevalvet ning määratlevad institutsionaalset vastutust. Erinevalt traditsioonilistest territoriaalsetest regulatsioonimudelitest toimivad digitaalsed identiteediraamistikud mitmetasandilistes ja jurisdiktsioonide ülestes keskkondades, kus vastutus, pädevused ja järelevalvemehhanismid on sageli killustunud mitme institutsiooni vahel (Lips, Bharosa & Draheim, 2020). Selline struktuur tõstatab küsimuse, kas ja mil määral on olemasolevad institutsionaalsed lahendused võimelised tagama tõhusa kontrolli, läbipaistvuse ja vastutuse olukordades, kus õiguslikud, tehnilised ja organisatsioonilised süsteemid ristuvad.

E-residentsuse programmi riskide haldamine toimub regulaarselt ja riigiasutuste ülese koordineerimise vormis. Sellesse on kaasatud kõik peamised programmiga seotud osapooled ja järelevalveasutused (EIS, 2025). Isikut tõendavate dokumentide seaduse kohaselt teostavad e-

residendi digitaalse isikutunnistuse kasutamise üle oma pädevuse piires riiklikku järelevalvet Politsei-ja Piirivalveamet (PPA), Maksu-ja Tolliamet (MTA), KAPO, RAB ning järelevalveprotsessi on kaasatud ka Riigi Infosüsteemi Amet (RIA), kes hindab digitaalse dokumendi andmekandja vastavust tehnilistele nõuetele (ITDS, 1999/2025). Kaudselt panustab riskide maandamisse ka Finantsinspeksioon (FI), teostades rahapesu ja terrorismi rahastamise tõkestamise järelevalvet finantssektori kohustatud isikute üle, kes osutavad e-residentidele finantsteenuseid ja tuginevad kliendi tuvastamisel digi-ID-le (Rahapesu ja terrorismi rahastamise tõkestamise seadus (RahaPTS), 2007/2025).

Supranatsionaalsel tasandil täiendavad riiklikku raamistikku EL-i institutsioonid, õigusaktid ja koostöömehhanismid, mille eesmärk on hallata piiriüleseid riske ning tagada siseturu toimimine valdkondades, mis on otseselt seotud e-residentsuse põhielementidega. Kuigi EL ei teosta otsest järelevalvet e-residentsuse programmi kui riigisisese haldusmeetme üle, kujundab see siduvate määruste ja direktiivide kaudu programmi normatiivset keskkonda, reguleerides digitaalse identiteedi vastastikust tunnustamist, isikuandmete kaitset ning rahapesu ja terrorismi rahastamise tõkestamist.

Käesolevas peatükis kaardistatakse institutsionaalse vastutuse ja regulatiivse järelevalve jaotuse Eesti ja EL-i tasandil, keskendudes vastutuse ja volituste jaotusele ning koostöömehhanismidele. Alapeatüki eesmärk on luua institutsionaalne lähtekoht, mille alusel hinnata nende struktuuride võimalikke kitsaskohti ja järelevalveriske edasises analüüsis.

1.3.1. Institutsionaalse vastutuse ja järelevalve jaotus Eesti tasandil

E-residentsuse programmi haldamise eest vastutab Ettevõtluse ja Innovatsiooni Sihtasutus (EIS), mis tegutseb Majandus- ja Kommunikatsiooniministeeriumi (MKM) valitsemisalas. MKM-i roll piirdub strateegilise suunamise ja haldusliku vastutusega ega hõlma otsest regulatiivset järelevalvet e-residentide või digitaalse identiteedi kasutamise üle (Riigikontroll, 2020).

PPA on e-residentsuse programmi keskne haldus- ja järelevalveasutus Eesti tasandil, kelle ülesanne on tagada programmi õiguspärane toimimine, usaldusväärsus ning riskide maandamine nii riigisiseses kui ka rahvusvahelises kontekstis.

PPA-l on isikut tõendavate dokumentide seadusest tulenev otsene pädevus digi-ID ja identiteedi järelevalve teostamiseks (ITDS, 1999/2025). PPA roll hõlmab isikusamasuse tuvastamist ning haldusotsuste tegemist digi-ID väljastamise, uuendamise, peatamise või kehtetuks tunnistamise

üle vastavalt ITDS-is sätestatud alustele. Kuigi PPA-l on seadusjärgne lõppvastutus ja kaalutusõigus e-residendi digi-ID staatuse üle otsustamisel, tugineb menetlusprotsess riigiasutuste ülesele koordineerimisele ja teabevahetusele. Sellesse võrgustikku on kaasatud KAPO, MTA ning RAB, kes edastavad PPA-le operatiivset sisendit ja riskihinnanguid riikliku julgeoleku, maksukuulekuse ning rahapesu ja terrorismi rahastamise riskide kohta. Selline koostööraamistik võimaldab PPA-l langetada põhistatud haldusotsuseid dokumendi väljastamise, peatamise või kehtetuks tunnistamise üle, arvestades programmi usaldusväärsust mõjutavaid riske. (Riigikontroll, 2020; Moneyval, 2022)

Lisaks vastutab PPA isikut tõendavate dokumentide andmekogu ning automaatse biomeetrilise isikutuvastuse süsteemi (ABIS) haldamise eest, tagades e-residentidelt kogutud biomeetriliste andmete (sõrmejäljed, näokujutised) turvalise töötlemise ja kaitse (ITDS, 1999/2025).

PPA ülesanne on ka iga taotleja suhtes põhjaliku eel- ja järelkontrolli kontrolli teostamine, mille eesmärk on hinnata võimalikke ohte avalikule korrale ja riigi julgeolekule. Kontroll hõlmab andmete võrdlemist riiklikes ja rahvusvahelistes andmebaasides ning koostööd teiste pädevate asutustega (Riigikontroll, 2020). Alates 2022. aastast rakendatakse automatiseeritud järelkontrolli lahendust, mis võimaldab regulaarselt seirata e-residentidega seotud riskiinfot Eesti sisestest ja EL-i andmekogudest. Riskiprofiilide kasutamine toetab kõrgendatud riskiga juhtumite tuvastamist ning võimaldab vajaduse korral alata menetluse digi-ID peatamiseks või kehtetuks tunnistamiseks. (Rahandusministeerium, 2025)

Rahvusvahelises koostöös on PPA keskne kontaktasutus välisriikide õiguskaitseorganite päringute ja õigusabitaotluste menetlemisel, mis puudutavad e-residente või nendega seotud ettevõtteid. Teabevahetus toimub turvaliste kanalite kaudu, sealhulgas Europol SIENA süsteemi ja Interpoli võrgustike vahendusel. (Riigikontroll, 2020; Moneyval, 2022)

KAPO teostab seaduse alusel riiklikku järelevalvet e-residendi digi-ID kasutamise üle, keskendudes julgeolekuohtude tuvastamisele ning terrorismi ja selle rahastamise tõkestamisele (KAPO, 2025). KAPO pädevus tuleneb Julgeolekuasutuste seadusest (JAS, 2000/2023) ning KAPO põhimäärusest (2014/2025), mis määratlevad ameti ülesanded riigi julgeoleku kaitsel, sealhulgas vastuluure- ja terrorismivastase tegevuse valdkonnas. KAPO roll e-residentsuse programmis on analüütiline ja ennetav: amet tuvastab julgeolekukriitilist teavet ning on seadusega kohustatud edastama selle PPA-le, kellel on ainupädevus langetada haldusotsuseid digi-ID staatuse üle (ITDS, 1999/2025, KAPO, 2025).

Rahapesu ja terrorismi rahastamise tõkestamise keskne riiklik asutus on RAB, mis tegutseb autonoomselt Rahandusministeeriumi valitsemisalas. RAB-i pädevus ja ülesanded tulenevad eeskätt rahapesu ja terrorismi rahastamise tõkestamise seadusest (RahaPTS, 2007/2025), mis sätestab nii rahapesu ja terrorismi rahastamise tõkestamise institutsionaalse raamistiku kui ka andmevahetuse mehhanismid pädevate asutuste vahel. RahaPTS-i kohaselt on RAB-i ülesandeks rahapesu ja terrorismi rahastamise kahtluste vastuvõtmine, analüüsimine ning asjakohase teabe edastamine uurimisasutustele ja teistele pädevatele asutustele.

Kuigi e-residendi digitaalse isikutunnistuse väljastamise ja kehtivuse üle otsustab PPA vastavalt isikut tõendavate dokumentide seadusele (ITDS, 1999/2025), on RAB volitatud edastama PPA-le teavet ja riskihinnanguid, kui see on vajalik rahapesu või terrorismi rahastamise tõkestamiseks (RahaPTS, 2007/2025, § 60). Seega võib RAB-i analüütiline hinnang olla sisuliseks aluseks PPA haldusotsusele digi-ID väljastamises, peatamises või kehtetuks tunnistamises, kuigi RAB-il endal puudub haldusõiguslik otsustusõigus digi-ID staatuse üle.

Lisaks avaldub RAB-i roll e-residentsuse kontekstis järelevalves kohustatud isikute üle. RahaPTS § 2 kohaselt kuuluvad kohustatud isikute hulka muu hulgas usaldushalduse ja äriühinguteenuse pakkujad, kes võivad e-residentide jaoks olla keskseks vahendajaks Eesti ettevõtte asutamisel, aadressi- ja kontaktisikuteenuse kasutamisel ning ettevõtte haldamisel (RahaPTS, 2007/2025). Seetõttu on RAB-i järelevalve oluline ka professionaalsete vahendajate kaudu tekkivate rahapesu- ja finantskuritegevuse riskide maandamisel.

Ehkki RAB-i pädevus tuleneb siseriiklikust seadusest (RahaPTS), on tema järelevalvemudel ja koostöömehhanismid kujundatud EL-i õigusraamistikus, mida käsitletakse järgmises alapunktis.

MTA otsene ülesanne e-residentsuse menetluses on taotleja maksualase tausta eelkontroll, mille käigus hinnatakse tema seoseid Eestis registreeritud ettevõtetega ning maksukuulekust, sh maksuvõlgade olemasolu, deklaratsioonide ja aruannete esitamise korrektsust, ärikeelu puudumist ning varasemaid tuvastatud õigusrikkumisi (Riigikontroll, 2020). MTA pädevus sellise kontrolli teostamiseks tuleneb Maksukorralduse seadusest (2002/2025). Eelkontroll toimub valdavalt automatiseeritult massandmete alusel, kuid vajaduse korral kaasatakse analüüsi teabe- ja maksuauditi üksuste ametnikud, kes annavad PPA-le kooskõlastuse, teevad ettepaneku e-residentsusest keeldumiseks või esitavad tingimusliku kooskõlastuse koos nõuetega puuduste kõrvaldamiseks (Riigikontroll, 2020).

Finantsinspeksioon teostab rahapesu ja terrorismi rahastamise vastast järelevalvet finantssektori ja finantsteenuste osutajate üle, sealhulgas nende teenuste kontekstis, mida võivad kasutada e-residentidest kliendid (Moneyval, 2022). FI pädevus tuleneb Finantsinspeksiooni seadusest (2001/2025) ning RahaPTS ning on suunatud eelkõige finantssektori kohustatud isikutele, näiteks pankadele, makseasutustele ja teistele finantsteenuse osutajatele, mitte e-residentidele endile. Sarnaselt RAB-ile rakendab ka FI riskipõhist kontrolli, mille käigus järelevalve intensiivsus sõltub hinnatud riskitasemest. (RAB, 2025; Moneyval, 2022)

RIA roll e-residentsuse programmi institutsionaalses ja regulatiivses raamistikus on olemuselt tehniline ja taristupõhine, keskendudes riikliku infosüsteemi arendamise koordineerimisele, digitaalse identiteedi turvalisuse tagamisele ja küberkaitsele (Kotka jt, 2016). RIA roll piirdub e-residendi digi-ID kui tehnilise vahendi turvalisuse ja standarditele vastavuse hindamisega, digi-ID kasutamise õiguspärasuse hindamine kuulub seaduse alusel teiste pädevate asutuste ülesannete hulka (ITDS, 1999/2025).

Riigisisel tasandil võib sellist pädevuste jaotust käsitleda mitmetasandilise või funktsioonipõhise valitsemise loogikana, kus otsustus-, analüüsi- ja tehnilised funktsioonid on institutsionaalselt eristatud (Bache, 2012). Selline spetsialiseerumine võib suurendada kompetentsipõhist tõhusust ja riskide diferentseeritud käsitlemist, kuid samal ajal hajutada vastutust ning raskendada tervikliku järelevalve tagamist.

1.3.2. Institutsionaalse vastutuse ja järelevalve jaotus Euroopa Liidu tasandil

EL-i tasandil ei eksisteeri e-residentsuse programmi suhtes eraldiseisvat regulatiivset ega järelevalveasutust, kuid programmi põhielemendid - digitaalne identiteet, isikuandmete töötlemine ning finantskuritegude tõkestamine - alluvad EL-i õigusele ja mitmetasandilisele institutsionaalsele järelevalveraamistikule, kus kontroll on korraldatud sektori- ja riskipõhiselt.

Analüütiliselt võib selle pädevusjaotuse jagada kolmeks funktsionaalseks kihiks: seadusandlik tasand, kus kujundatakse horisontaalsed normid; regulatiivne ja järelevalveline tasand, kus liikmesriikide pädevaid asutusi toetavad ja koordineerivad EL-i tasandi organid; ning operatiivtasandi õiguskaitsekoostöö, kus piiriüleste süütegude tuvastamiseks ja uurimiseks kasutatakse Europolit, Eurojusti ja EPPO tuge (Rahapesu tõkestamise direktiiv (AMLD VI), EL 2024/1640; Isikuandmete kaitse üldmäärus (GDPR) EL 2016/679).

Seadusandlik tasand

Seadusandlik funktsioon EL-i tasandil koondub institutsioonidevahelisse menetlusse, kus Euroopa Komisjon omab algatusõigust ning Euroopa Parlament ja Euroopa Liidu Nõukogu kujundavad õigusaktide lõpliku sisu. E-residentsuse programmi seisukohalt ei reguleeri EL konkreetset riiklikku lahendust, vaid kehtestab horisontaalsed normid, mis määratlevad õigusliku ja tehnilise raamistiku, mille piires liikmesriik võib oma digitaalse identiteedi süsteemi ja ettevõtluskeskkonda kujundada. Seeläbi struktureerib EL-i tasandi normiloomel liikmesriigi diskretsiooni ning tagab õiguse ühetaolise kohaldamise ja siseturu toimepidevuse.

Digitaalse taristu normatiivne alus tuleneb e-identimise ja e-tehingute jaoks vajalike usaldusteenuste (eIDAS) määrusest (EL 910/2014), mis sätestab elektroonilise identimise vahendite usaldusväarsuse tasemed, usaldusteenuste nõuded ning vastastikuse tunnustamise põhimõtte. See on õiguslik eeldus, mis võimaldab e-residenti digi-ID-l toimida piiriüleselt ning tagab kvalifitseeritud e-allkirjade kehtivuse kogu EL-is. Antud raamistiku edasiarendusena vastu võetud eIDAS 2.0 määrus (EL 2024/1183) loob Euroopa digiidentiteedikukru kontseptsiooni. Eesti tasandil tagab RIA, et e-residenti digi-ID ja sellega seotud usaldusteenused vastavad nendele tehnilistele ja õiguslikele standarditele, mis omakorda kindlustab lahenduse kooskõla liidu õigusega (Kotka, Vargas Alvarez del Castillo & Korjus, 2016; ITDS, 1999/2025).

Empiirilised uuringud osutavad siiski, et eIDAS-e normatiivne ühtlustamine ei ole praktikas täielikult kõrvaldanud liikmesriikide vahelist killustatust. Lips, Bharosa ja Draheim (2020) näitavad, et erinevad tõlgendus- ja järelevalvepraktikad ning ühtse testimisraamistiku puudumine on tekitanud rakenduslikke koordineerimisprobleeme (Lips, Bharosa & Draheim, 2020). Lips jt (2022) rõhutavad, et just need puudujäägid tingisid eIDAS 2.0 reformi, mille eesmärk on tehniliste ja õiguslike standardite tugevam ühtlustamine, et vähendada piiriüleseid turva- ja regulatsioonilünki (Lips jt, 2022).

Isikuandmete töötlemise õiguslik raamistik tuleneb Isikuandmete kaitse üldmäärusest (GDPR) (EL 2016/679), mis kaitseb füüsiliste isikute põhiõigusi ja -vabadusi isikuandmete töötlemisel. Kuna e-residentsuse menetluses töödeldakse isikuandmeid avaliku võimu teostamise ja avalikes huvides oleva ülesande täitmise raames, peab andmetöötlus vastama määruses sätestatud õiguslikele nõuetele. Programmi piiriülese iseloomu tõttu on eriti olulised automatiseeritud töötlusel põhinevaid üksikotsuseid ning isikuandmete kolmandatesse riikidesse või rahvusvahelistele organisatsioonidele edastamist puudutavad nõuded (EL 2016/679).

Finantskuritegude tõkestamise valdkonnas kujundab liikmesriikide kohustusi direktiivide ja määruste kaudu ühtlustatud riskipõhine järelevalveraamistik, mille eesmärk on vähendada regulatiivseid erinevusi ning tugevdada piiriüleste riskide käsitlemist. Riskipõhise lähenemise kohustus sätestati esmalt Euroopa Parlamendi ja nõukogu rahapesu tõkestamise direktiivis EL 2015/849 (IV AMLD), mida täiendati direktiiviga EL 2018/843 (V AMLD). Need direktiivid kohustasid liikmesriike rakendama riskipõhist järelevalvemudelit, mille kohaselt kontrollimeetmete intensiivsus peab vastama tuvastatud rahapesu ja terrorismi rahastamise riskide tasemele. 2024. aastal võeti vastu uus õigusraamistik, mille keskseks osaks on direktiiv EL 2024/1640 (VI AMLD), mis tunnistab direktiivi 2015/849 alates 2027. aastast kehtetuks ning süvendab riskipõhist lähenemist, täpsustades järelevalveasutuste ülesandeid, koostöömehhanisme ja teabevahetust liikmesriikide vahel.

Seega ühtlustab EL seadusandlikul tasandil e-residentsuse jaoks olulisi digitaalse identiteedi, andmekaitse ja rahapesu tõkestamise norme, kuid ei reguleeri ega kontrolli e-residentsuse programmi kui konkreetset riigisisest haldusmeedet.

Regulatiivne ja järelevalveline tasand

Regulatiivne ja järelevalveline tasand moodustab EL-i ülese integreeritud järelevalvemehhanismi, kus liikmesriikide pädevad asutused teostavad vahetut kontrolli, tuginedes EL-i tasandi organite koordineerimisele ja ühtsetele metoodikatele.

Finantskuritegude tõkestamise valdkonnas on selle süsteemi keskseks lüliks 2024. aasta rahapesu paketiga loodud Rahapesu ja Terrorismi Rahastamise Tõkestamise Amet (AMLA). AMLA ülesandeks on teostada otsest järelevalvet teatud kõrge riskiga piiriüleste finantsasutuste üle ning koordineerida riiklike järelevalveasutuste tegevust, vähendades liikmesriikide vahelisi regulatiivseid erinevusi (EL 2024/1620; EL 2024/1640). AMLA loomine tähistab EL-i tasandil järelevalve osalist tsentraliseerimist valdkonnas, kus e-residentsuse kaudu asutatud ettevõtete piiriülene tegevus võib tekitada kõrgendatud rahapesuriske.

Andmekaitse valdkonnas täidab sarnast koordineerivat rolli Euroopa Andmekaitse-nõukogu, mis tagab isikuandmete kaitse üldmääruse (GDPR) ühtse kohaldamise, andes välja suuniseid ja lahendades liikmesriikide vahelisi erimeelsusi (EL 2016/679).

Lisaks vahetutele valdkondlikele koordineerijatele mõjutavad e-residentsuse regulatiivset keskkonda ka EL-i finants- ja küberturvalisuse valdkonna institutsioonid, kes kujundavad standardeid Eesti riigiasutustele ja e-residente teenindavatele erasektori partneritele. Euroopa

Keskpank (ECB) ja Euroopa Pangandusjärelevalve (EBA) kujundavad EL-i finantssüsteemi stabiilsuse ja riskijuhtimise standardeid, sealhulgas pankade hoolsus- ja isikutuvastusprotsesse, mille kaudu e-residendid Eesti ettevõtlus keskkonnale ligi pääsevad. (Rahandusministeerium, 2025; Moneyval, 2022) Samal ajal suunab EL Küberturvalisuse Amet (ENISA) programmi tehnilist vundamenti, osaledes Euroopa küberturvalisuse sertifitseerimise kavade haldamisel ning analüüsides e-identimise süsteemide ja usaldusteenustega seotud küberohte, nõrkusi ning turvaintsidentidest teavitamise poliitikat (EL 2024/1183).

Seega jääb vahetu järelevalve valdavalt liikmesriikide pädevusse, samas kui EL-i tasandi institutsioonid kujundavad standardeid, koordineerivad järelevalvepraktikat ning püüavad vähendada liikmesriikide vahelisi erinevusi.

Operatiivtasandi õiguskaitsekoostöö

EL-i õiguskaitseasutuste vaheline operatiivkoostöö on e-residentsuse programmi piiriüleste riskide maandamisel kriitilise tähtsusega, pakkudes raamistikku teabevahetuseks ja ühistegevuseks. Europol pakub EL-i tasandil operatiivset ja analüütilist tuge liikmesriikide õiguskaitseasutustele raskete rahvusvaheliste kuritegude, sealhulgas rahapesu, küberkuritegevuse ja majandussüütegude uurimisel (Moneyval, 2022). Europoli roll seisneb teabe koondamises, piiriüleste ohumustrite analüüsimises ning liikmesriikide vahelise operatiivkoostöö hõlbustamises (Europol, 2025). RAB osaleb ka Europoli finantsteabe partnerluses (EFIPPP), mis on ühine platvorm avaliku ja erasektori vaheliseks teabevahetuseks, võimaldades riikidel operatiivsemalt reageerida uutele finantskuritegevuse suundumustele. Operatiivse infoliikumise tagamiseks on PPA-l ning MTA-l Europoli juures alalised sideohvitserid, kelle kaudu vahendatakse teavet nii süüteo- kui ka haldusmenetlustes. (Rahandusministeerium, 2025)

Kuna e-residendid asutavad Eestis ettevõtteid, mis on osa EL-i ühest majandusruumist, omavad Euroopa Prokuratuur (EPPO) ja Euroopa Pettustevastane Amet (OLAF) pädevust uurida nende üksustega seotud võimalikke EL-i finantshuve kahjustavaid pettusi ja korruptsiooni. Uue rahapesuvastase direktiivi (EL 2024/1640) kohaselt on neil institutsioonidel oma ülesannete täitmisel otsene juurdepääs tegelike kasusaajate andmetele, et toetada riiklikke uurimisi. Keerukate ja mitut jurisdiktsiooni hõlmavate juhtumite lahendamisel pakub liikmesriikide asutustele menetluslikku ja operatiivtuge Eurojust, koordineerides koostööd ning hõlbustades ühiste uurimisrühmade tegevust. Operatiivseks teabevahetuseks kasutatakse

seejuures turvalisi sidekanaleid nagu SIENA, mis tagab, et tundlik info on kättesaadav vaid asjakohasele juurdepääsuõigusega personalile. (Rahandusministeerium, 2025; EL 2024/1640)

Operatiivtasandil sõltub e-residentsusega seotud riskide tuvastamine ja menetlemine seega eeskätt sellest, kui kiiresti ja tõhusalt liigub teave liikmesriikide ning EL-i koostöökanalite vahel.

Kokkuvõttes ei toimi e-residentsus EL-i tasandil iseseisva regulatiivse objektina, vaid on lõimitud EL-i mitmetasandilisse normatiiv- ja järelevalvestruktuuri. Bache'i mitmetasandilise valitsemise käsitluse kohaselt ei ole pädevus koondunud ühele territoriaalsele tasandile, vaid jaguneb nii üldpädevusega institutsioonide kui ka ülesandespetsiifiliste ja funktsioonipõhiste üksuste vahel (Bache, 2012). E-residentsuse regulatiivne keskkond peegeldab seda loogikat: normilooma ja strateegiline suunamine toimuvad ühel tasandil, samas kui riskihindamine, järelevalve ja tehniline kontroll on delegeeritud mitmele spetsialiseerunud institutsioonile. Selline struktuur võib suurendada koordineerimist ja standardite ühtlustamist, kuid samal ajal hajutada vastutust ning tekitada institutsionaalseid pingeid.

Seetõttu ei piisa e-residentsuse mõistmiseks üksnes õigusliku ja institutsionaalse raamistiku kirjeldamisest, vaid vaja on ka teoreetilist käsitlust, mis võimaldab analüüsida, kuidas piiriülese digitaalse ettevõtluse, territoriaalse järelevalve ja hajutatud vastutuse koosmõjus võivad kujuneda finantskuritegevust soodustavad struktuursed tingimused.

2. Teoreetiline raamistik

E-residentsuse programm toimib olemuselt globaalses digitaalses keskkonnas, kus majandustegevus, ettevõtlus ja teenused ei ole enam seotud ühe konkreetse territooriumiga. Sellised piiriülesed digitaalsed infrastruktuurid loovad uusi võimalusi majandustegevuseks, kuid võivad samal ajal avada ka uusi kanaleid rahvusvahelise kuritegevuse organiseerimiseks ja varjamiseks. Seetõttu käsitletakse antud töös e-residentsuse süsteemiga seotud riskide mõistmiseks laiemat nähtust - transnatsionaalset kuritegevust - ning neid struktuurseid tegureid, mis võivad selle kujunemist soodustada.

Transnatsionaalset kuritegevust on teaduskirjanduses käsitletud kui nähtust, mille kujunemist mõjutavad globaliseerumine, rahvusvahelised finantsvood, tehnoloogiline areng ning riikidevahelised regulatiivsed erinevused. Albanese (2012) määratleb transnatsionaalset kuritegevust kui seaduserikkumist, mille planeerimine, toimepanemine või mõju ulatub üle ühe riigi piiri, eristades seda seeläbi traditsioonilisest riigisisest kuritegevusest. Autor käsitleb seda kui organiseeritud kuritegevuse globaalset avaldumist, mille keskmes on kasumile suunatud ebaseaduslikud turud ja piiriülesed kuritegelikud tegevused. (Albanese, 2012) Boisteri järgi võib transnatsionaalset kuritegevust käsitada katusmõistena, mis hõlmab käitumist, millel on tegelik või potentsiaalne piiriülene mõju ning mis tekitab nii riiklikku kui ka rahvusvahelist regulatiivset huvi (Boister, 2003).

Sellise piiriülese kuritegevuse kujunemise mõistmiseks ei piisa üksnes nähtuse kirjeldamisest, vaid vajalik on ka analüütiline raamistik, mis selgitaks, millised struktuursed tingimused võimaldavad selle tekkimist ja levikut. Käesolevas töös kasutatakse nende tingimuste analüüsimiseks Nikos Passase kriminogeensete asümmeetriate teooriat. Passase (2003) käsitus keskendub sellele, kuidas globaliseerumisest tulenevad poliitilised, majanduslikud ja õiguslikud erinevused loovad keskkonna, kus piiriülene kuritegevus saab tekkida ja areneda. Selline lähenemine võimaldab käsitleda e-residentsuse programmi mitte üksnes tehnilise või õigusliku lahendusena, vaid osana laiemast globaalsest regulatiivsest ja majanduslikust süsteemist, milles võivad avalduda ka kriminogeensed riskid.

2.1. Transnatsionaalne kuritegevus ja kriminogeensed asümmeetriad

Nikos Passas esitas juba 2003. aastal transnatsionaalse kuritegevuse analüüsimiseks teoreetilise käsitluse, mille kohaselt globaliseerumisest tulenevad poliitilised, majanduslikud ja õiguslikud asümmeetriad – sh regulatiivsed erinevused ja kontrollimehhanismide killustatus – loovad kriminogeenseid struktuurseid tingimusi. Need struktuursed ebakõlad soodustavad seaduslike ja ebaseaduslike struktuuride põimumist ning avavad seeläbi võimalused kuritegude toimepanekuks piiriüleses mõõtnes. Passas (2003) suhtub kriitiliselt tavapärasesse „organiseeritud kuritegevuse“ mõistesse, mis käsitles seda autonoomse ja selgelt eristuva „allilma“ probleemina. Autor näitab, et selline dualistlik käsitlus on ebapiisav, kuna piiriülene kuritegevus kujuneb ja toimib tihedas seoses legaalses majanduslikes, poliitilistes ja institutsionaalsetes struktuuridega. (Passas, 2003)

Passas pakub välja definitsiooni, mille kohaselt on piiriülene kuritegevus käitumine, mis ohustab õiguslikult kaitstud huve rohkem kui ühes riiklikus jurisdiktsioonis ja on kriminaliseeritud vähemalt ühes asjaomases riigis. Selline lähenemine võimaldab uurida transnatsionaalset kuritegevust laiemalt kui vaid rangelt juriidiliste määratluste kaudu, võttes arvesse ka globaalse ühiskonna mitmekesisust ja huve.

Passase teooria keskseks argumendiks on kriminogeensete asümmeetriate mõiste, mille all autor peab silmas poliitilisi, majanduslikke, kultuurilisi ja õiguslikke struktuurseid ebakõlasid ning ebavõrdsusi. Need asümmeetriad loovad nõudluse ebaseaduslike kaupade ja teenuste järele, pakuvad osapooltele stiimuleid ebaseaduslikes tehingutes osalemiseks ning nõrgestavad riikide võimekust piiriülest kuritegevust tõhusalt kontrollida. Samuti võivad neid asümmeetriaid võimendada majanduslikud ja poliitilised stiimulid olukorras, kus majandustegevuse soodustamine ei ole tasakaalus järelevalvevõimekusega. Globaliseerumise tingimustes see lõhe süveneb, kuna majandustegevus on muutunud piiriüleseks, samas kui järelevalvemehhanismid jäävad territoriaalseks, võimaldades kurjategijatel kasutada ära riikidevahelisi regulatiivseid erinevusi.

Passase käsitluses süvendab globaliseerumine kriminogeenseid asümmeetriaid, sest piiriülene majandustegevus võimaldab ära kasutada eri jurisdiktsioonide õiguslikke ja järelevalvelisi erinevusi. Ta kirjeldab seda „jurisdiktsiooni šoppamisena“, mille puhul otsitakse või kombineeritakse selliseid õigusruume, kus teatud tegevused ei ole kriminaliseeritud või kus järelevalve on nõrgem. See võimaldab kurjategijatel distantseerida kriminaalset mõtet selle teostusest, kasutades tehnoloogiat ja varifirmasid tegevuse hajutamiseks üle maailma. Passas toob välja, et teatud jurisdiktsioonid ja seaduslikud struktuurid toimivad nendes skeemides kui

„mustad kastid“, pakkudes anonüümsust ja varjates globaalsete õiguserikkujate jälgi. Sellised mustad kastid on kriitiliseks instrumendiks, et varjata kuritegelikku päritolu vara ja takistada uurijatel tegelike kasusaajate tuvastamist.

Passas seab kahtluse alla ka traditsioonilise jaotuse seaduskuuleka ühiskonna (*upperworld*) ja kuritegeliku „allilma“ (*underworld*) vahel, rõhutades, et piir seadusliku ja ebaseadusliku vahel on sageli hägune. Tema käsitluses võivad legaalsed äristruktuurid teadlikult või teadmatult teenindada kuritegelikke eesmärke, toimides seeläbi legaalse ja illegaalse sfääri liidesena (liides ehk *interface*). Selliste sümbiootiliste suhete puhul toob Passas esile nn ülesannete delegeerimise mehhanismi, mille korral seaduslikud osapooled annavad probleemset, ebaeetilised või ebaseaduslikud tegevused üle välistele tegijatele. Selline organisatsiooniline ja globaalselt hajutatud struktuur võimaldab seeläbi lahutada „kuritegeliku käe“ (täideviija) „kuritegelikust mõistusest“ (organiseerija), pikendades vastutusahelat üle mitme jurisdiktsiooni ning muutes seoste tuvastamise keerukaks.

Selline vastutuse struktuurne hajumine loob olukorra, kus juriidilised isikud ning professionaalsed vahendajad, näiteks juristid, raamatupidajad, konsultandid või finantsteenuste osutajad, toimivad puhvritena, pakkudes otsustajatele usutavat eitust (*plausible deniability*). Vahendajad võivad osaleda tehingutes ilma klientide tegelikku identiteeti või lõppeesmärki täielikult teadmata, mistõttu killustub nii informatsioon kui ka õiguslik vastutus. Passase käsitluses suunab see tähelepanu üksikutele täideviijatele, jättes tahaplaanile süsteemsed asümmeetriad ja institutsionaalsed korraldused, mis võimaldavad tegelikel kasusaajatel jääda õiguslikult kättesaamatuks ning tegutseda legaalse majanduse sees selle infrastruktuuri varjus.

Samuti toob autor välja süsteemse sünergia (*systemic synergy*) mõiste, mis võimaldab nii seaduslikel kui ka ebaseaduslikel osapooltel kasu lõigata ilma otsese vandenõuta. Näiteks saavad finantsinstitutsioonid kasu, teadlikult või teadmatult, kuritegeliku tegevuse tulemusel tekkivatest kapitalivoogudest, mida nad oma tavapärase äritegevuse käigus teenindavad, sageli seetõttu, et eelnevad tehingud on ebaseaduslikkuse jäljed varjanud. Selles protsessis mängivad samuti olulist rolli professionaalsed hõlbustajad, kes pakuvad kuritegelikele võrgustikele vajalikku infrastruktuuri ja nõustamist, moodustades varifirmasid ja hallates tehinguid diskreetsetes jurisdiktsioonides. Passas osundab, et legaalsed osapooled võivad ise toimida kriminaalsete osapooltena, pakkudes seaduslikke kaupu ja teenuseid, mis on muudetud konkurentsivõimeliseks läbi süsteemse pettuse või maksudest hoidumise. Seetõttu ei saa transnatsionaalset kuritegevust käsitleda kui välist vandenõud, vaid kui nähtust, mis on lahutamatult põimunud legaalse majandussüsteemi ja selle regulatiivsete ebakõladega.

Kui Passas (2003) käsitleb kriminogeenseid asümmeetriaid globaliseerumise struktuurse kõrvalmõjuna, siis väikeriikide vaates ei ole selline keskkond üksnes riskiallikas, vaid ka strateegiline võimalus. Hardy (2023) varjupaigateooria kohaselt võivad väikeriigid otsida poliitilist ja majanduslikku varju globaalses võrgustikuühiskonnas, kasutades innovatsiooni ja digitaalset lahendusi oma mõju suurendamiseks. Eesti puhul ei ole digitaalne innovatsioon, sh e-residentsus, pelgalt tehnoloogiline areng, vaid teadlik strateegia riigi digitaalse ulatuse laiendamiseks ja institutsionaalse usalduse eksportimiseks. (Hardy, 2023) Seega võib Passase kirjeldatud kriminogeensete asümmeetriate teke olla riigi poolt teadlikult aktsepteeritud risk: riik on valmis looma asukohasõltumatut majandusruumi ja eksportima institutsionaalset usaldust (digi-ID), et saavutada pehme jõu kaudu poliitiline julgeolek ja suurendada oma majanduslikku baasi.

Passase käsitlus annab käesolevale tööle keskse raamistiku, võimaldades analüüsida, kuidas regulatiivsed, institutsionaalsed ja jurisdiktsioonilised ebakõlad loovad finantskuritegevust soodustavaid tingimusi. Samas ei selgita Passase teooria üksinda piisavalt seda digitaalset ja ruumilist keskkonda, milles need asümmeetriad e-residentsuse puhul avalduvad. Seetõttu kasutatakse töös täiendavalt Castellsi (2010) võrgustikuühiskonna käsitlust, mis aitab mõtestada piiriülese digitaalse majandustegevuse ja territoriaalselt korraldatud järelevalve vahelist pinget (Castells, 2010). Kui Passas aitab selgitada, miks regulatiivsed ja institutsionaalsed lõhed muutuvad kriminogeenseks, siis Castells aitab selgitada, kus ja kuidas need lõhed digitaalses võrgustikulises keskkonnas avalduvad.

Castells eristab kaasaegses ühiskonnas kahte ruumilist loogikat: „paikade ruumi“, mis põhineb territoriaalsel kohalolul ja riiklikul jurisdiktsioonil ning „voogude ruumi“, mis koosneb digitaalsetest, finants- ja informatsioonivoogudest ning mille toimimine ei ole seotud konkreetse geograafilise asukohaga (Castells, 2010, lk 453). Kaasaegne majandus ja võimustruktuurid organiseeruvad üha enam voogude ruumis, samal ajal kui õigussüsteemid ja järelevalveinstitutsioonid toimivad endiselt paikade ruumi loogikas. Kui Passas keskendub riikidevahelistele regulatiivsetele erinevustele ja jõustamisvõimekuse ebavõrdsusele, siis Castells näitab, miks digitaalne võrgustikuline keskkond neid erinevusi võimendab: majandustegevus, kapital ja informatsioon liiguvad piiriüleselt kiiremini, kui territoriaalsed kontrollimehhanismid suudavad reageerida.

E-residentsuse puhul avaldub see pinge eeskätt distantsjuhtimises: ettevõtte on formaalselt registreeritud Eestis, kuid selle juhtimine, majandustegevus ja riskikäitumine paiknevad teistes jurisdiktsioonides, mis muudab territoriaalse järelevalve killustunuks ning sõltuvaks

rahvusvahelisest koostööst. Võrgustikuühiskonnas kasutavad nii seaduslikud ettevõtted kui ka kuritegelikud rühmitused samu digitaalseid infrastruktuure ja finantssüsteeme. See muudab kuritegevuse paindlikumaks ja hajusamaks ning lihtsustab jurisdiktsiooniliste lõhede ärakasutamist. Riigid on küll olnud globaliseerumise ja digitaalse arengu edendajad, kuid nende suutlikkus piiriüleseid infovooge täielikult kontrollida on piiratud. (Castells, 2010) Seetõttu ei loo võrgustikuühiskond transnatsionaalset kuritegevust, kuid loob tingimused, milles see saab hõlpsamini areneda.

Tammpuu ja Masso (2019) analüüs e-residentsusest näitab, et transnatsionaalne digitaalne identiteet toimib osana globaalsest digitaalsest infrastruktuurist, mis võimaldab majandustegevust üle riigipiiride. Kuigi e-residentsus on formaalselt kõigile avatud, sõltub selle tegelik kasutus riikide digitaalse ja majandusliku arengutasemest. See tähendab, et digitaalne identiteet ei ole pelgalt tehniline vahend, vaid mehhanism, mis kujundab ligipääsu globaalsele majandusele ning võib teatud juhtudel nii vähendada kui ka taastoota arengulisi erinevusi. (Tammpuu & Masso, 2019)

Need arengulised erinevused ja Castellsi kirjeldatud kontrollivõimekuse piiratus realiseeruvad praktikas läbi andmevahetuse lünkade, mis muudavad piiriülese kontrolli tehniliselt keerukaks. Seda pinget Castellsi piirideta voogude ja territoriaalse riikliku järelevalve vahel analüüsivad Masso jt (2024), näidates, et kuna ametlikud andmevood riikide vahel sageli ei toimi, peavad Eesti ametiasutused kolmandate riikide taotlejate puhul toetuma internetist leitud infole, mis on ebakvaliteetne ja ebausaldusväärne (Masso jt, 2024). Selline olukord võib Passase käsitluses sarnaneda „musta kasti“ efektiga, kus ametlikult väljastatud usaldusmärk (digi-ID) põhineb andmetel, mille kvaliteet ja kättesaadavus varieerub jurisdiktsiooniti. Tulemuseks võivad olla uued digitaalsed barjäärid, kus vähem arenenud andmetaristuga riikide kodanikud on juba eos riskantsed subjektid, kuna nende kohta puuduvad usaldusväärsed andmevahetuskanalid.

Kriminoloogilisest vaatenurgast tähendab see, et andmete kättesaadavuse ja kvaliteedi erinevused riikide vahel ei mõjuta üksnes teenuste toimivust, vaid kujundavad ka digitaalseid piire, mille kaudu otsustatakse, kes on usaldusväärne ja kes riskantne. Nagu Masso jt (2024) näitavad, võib andmestatud kontroll legitimeerida ja taastoota globaalseid ebavõrdsusi, kuna taotlejate hindamine sõltub nende päritoluriigi andmekoostööst ja kontrollivõimekusest (Masso jt, 2024). Sellises olukorras ei ole teatud jurisdiktsioonid järelevalve seisukohast läbipaistvad, vaid toimivad praktiliselt „mustade kastidena“, süvendades kriminogeenseid asümmeetriaid piiriüleses digitaalses keskkonnas.

Sellisel vaadatuna toimib e-residentsus konkreetse institutsionaalse näitena sellest, kuidas Castelli kirjeldatud voogude ruum ja Passase käsitletud regulatiivsed asümmeetriad praktikas põimuvad. Digitaalne identiteet loob legaalse kanali piiriüleseks ettevõtluseks, kuid samal ajal asetub see keskkonda, kus jurisdiktsioonilised lõhed ja erinevused järelevalves võivad muutuda ära kasutatavaks. Seega ei ole tegemist üksnes digitaalse kodakondsuse laiendamisega, vaid ka uue regulatiivse ruumiga, kus tehnoloogilised ja normatiivsed asümmeetriad võivad omandada kriminogeense potentsiaali. Sellisel moodustub keskkond, kus riigi strateegiline innovatsioon, globaalne võrgustikuühiskond ja regulatiivsed asümmeetriad põimuvad, luues nii uusi majanduslikke võimalusi kui ka struktuurseid riske.

Eelneva teoreetilise käsitluse põhjal saab kriminogeenseid asümmeetriaid käesolevas töös mõtestada nelja omavahel seotud vormina:

- Informatsiooniline asümmeetria viitab olukorrale, kus vajalik teave isikute, tegevuste, seoste või rahavoogude kohta on ebaühtlaselt jaotunud, puudulik või raskesti kättesaadav. Passase käsitluses seostub see „mustade kastide“ ja tegelike kasusaajate varjatusega.
- Regulatiivne asümmeetria tuleneb õigusnormide, kontrollistandardite ja järelevalvepraktikate erinevusest eri jurisdiktsioonides. See haakub Passase käsitluses jurisdiktsiooni šoppamise ja regulatiivsete lünkade ärakasutamisega.
- Jurisdiktsiooniline asümmeetria avaldub siis, kui tegevus, selle tagajärjed ja kontrollivõimalused paiknevad eri riiklikes jurisdiktsioonides. Castelli käsitluses väljendub see voogude ruumi ja paikade ruumi lahknevusena.
- Institutsionaalne asümmeetria viitab vastutuse, pädevuse ja kontrollivõimekuse hajumisele mitme institutsiooni või tasandi vahel. See seostub Passase kirjeldatud vastutuse hajumise, ülesannete delegeerimise ja legaalse-illegaalse sfääri liidesega.

Need neli asümmeetriat moodustavad edasise empiirilise analüüsi peamise tõlgendusraami ning võimaldavad hinnata, milliste struktuursete ebakõlade kaudu e-residentsusega seotud finantskuritegevuse riskid kujunevad ja milliste mehhanismide kaudu neid maandatakse.

2.2. Finantskuritegevuse riskid e-residentsuse kontekstis

Nicholas Ryderi (2011) käsitluses defineeritakse finantskuritegevust kui laia katusmõistet, mis hõlmab ebaseadusliku majandustegevuse vorme, nagu rahapesu, korruptsioon, pettused ja maksudest kõrvalehoidumine. Tegemist on kuritegudega, mille eesmärk on ebaseadusliku majandusliku kasu saamine finantssüsteemi, ettevõtlusstruktuuride või majandustehingute väärkasutamise kaudu, kasutades seejuures sageli keerukaid rahvusvahelisi skeeme. Ryder rõhutab, et tänapäevast finantskuritegevust tuleb analüüsida just 21. sajandi globaliseerunud majanduse ning poliitikakujundamise kontekstis, kuna sellel on otsene ja sügav mõju riikide majanduslikule ning institutsionaalsele stabiilsusele. Selline raamistik võimaldab liigutada fookuse üksikjuhtumitelt laiematele süsteemsetele ja regulatiivsetele riskidele. (Ryder, 2011)

2.2.1. Rahapesu olemus ja kolmeastmeline mudel

Rahapesu on läbi aja olnud organiseeritud kuritegevuse keskne toimetehhanism, mis võimaldab kuritegelikel võrgustikel muuta ebaseaduslikult saadud tulu näiliselt legitiimseks varaks, tagades sellega tegevuse jätkusuutlikkuse ja võimaldades laiendada oma mõju ning finantseerida edasisi kuritegelikke operatsioone. See protsess ühendab ebaseadusliku tegevuse seadusliku majandusega, tugevdades kuritegelikke struktuure ja võimaldades neil siseneda legaalsesse ettevõtluskeskkonda. (Europol, 2025)

Traditsiooniliselt liigitatakse rahapesu kolme põhietappi: paigutamine (*placement*), mille käigus viiakse kuritegelik tulu esmakordselt seaduslikku finantssüsteemi; kihistamine (*layering*), mis koosneb mitmetasandilistest tehingutest, ülekannetest ja konverteerimistest eesmärgiga varjata raha algset päritolu; ning integreerimine (*integration*), mille käigus suunatakse pestud vahendid tagasi ametlikku majandusse, näiteks investeringutena kinnisvarasse, luksuskaupadesse või seaduslikesse ettevõtetesse. (Europol, 2025; *Financial Action Task Force* (FATF), 2025)

Europoli riskihinnangute kohaselt süvendavad rahapesuga seotud haavatavusi tehnoloogilised ja piiriülesed lahendused, sealhulgas virtuaalvääringud, tehisintellekti kasutamine ja detsentraliseeritud finantsplatvormid, mis muudavad ebaseaduslike rahavoogude tuvastamise keerukamaks (Europol, 2023; Europol, 2025). E-residentsuse kontekstis on see oluline, kuna distantsilt tegutsemise võimalus võib teatud tingimustel raskendada seoste tuvastamist legitiimse äritegevuse ja varjatud kuritegelike võrgustike vahel.

2.2.2. E-residentsuse programmiga kaasnevad süsteemsed riskid

E-residentsuse programm ei kujuta endast finantskuritegevuse riski iseenesest, kuid selle piiriülene ja digitaalne ülesehitus võib luua keskkonna, kus seaduslikke majandusstruktuure on võimalik kasutada tegevuse tegeliku sisu, kontrolli või kasusaajate varjamiseks. E-residendi digi-ID võimaldab isikul distantsilt kasutada Eesti e-teenuseid ja asutada Eesti ettevõtte, kuid riigi järelevalve- ja kontrollimehhanismid sõltuvad jätkuvalt territoriaalsetest registritest, rahvusvahelisest andmevahetusest ning eri institutsioonide pädevusest. Selline lahknevus muudab e-residentsuse finantskuritegevuse riskide analüüsimisel oluliseks juhtumiks, kus digitaalne ligipääs, juriidiline vorm ja riiklik kontroll ei pruugi täielikult kattuda. (RAB, 2022a; Rahandusministeerium, 2025)

Moneyvali 2022. aasta hindamisaruandes käsitletakse e-residentsuse programmi süsteemse haavatavusena eeskätt seetõttu, et Eesti ettevõtete tegelike omanike ja kontrollijate tuvastamine võib piiriüleses keskkonnas olla piiratud. Moneyvali hinnangul võib see vähendada äriregistri ja finantssüsteemi läbipaistvust ning mõjutada ka laiemat piirkondlikku riskiprofiili, kuna Eesti väljastatud digitaalne identiteet ja juriidiline vorm võivad luua rahvusvahelises majanduskeskkonnas usalduse, mis ei pruugi alati vastata taustakontrolli tegelikule ulatusele (Moneyval, 2022). Käesolevas töös käsitletakse seda mitte tõendina iga e-residendi või e-residendi ettevõtte riskantsusest, vaid viitena süsteemsele riskikeskkonnale, mille empiirilist avaldumist tuleb eraldi analüüsida.

E-residentsusega seotud haavatavused ilmnevad eelkõige olukordades, kus formaalne seos Eestiga on olemas, kuid tegevuse sisuline kontroll ja järelevalveks vajalik teave paiknevad mujal. RAB on osutanud, et e-residentsuse kaudu loodud juriidilist isikut võidakse kasutada ebasoovitavaks ettevõtluseks olukorras, kus ettevõtte registreerimise koht ja juhtimise tegelik asukoht ei lange kokku ning järelevalvemenetluse läbiviimine on seetõttu raskendatud (RAB, 2022a). Selline risk haakub Passase kriminogeensete asümmeetriate käsitlusega, mille kohaselt võivad legaalsed institutsionaalsed vormid ja piiriülesed regulatiivsed erinevused kujundada tingimusi, kus ebaseaduslik tegevus saab toimida seadusliku majanduskeskkonna sees.

Oluline osa riskikeskkonnast on seotud taustateabe kättesaadavuse ja kontrollitavusega. E-residendi staatuse andmine toimub haldusmenetluses, mille raames ei ole riigil alati võimalik kasutada kõiki rahvusvahelisi õiguskaitsealase koostöö mehhanisme. Riigikontroll on osutanud, et PPA võimalused kontrollida välisriikide karistusandmeid ja ärikeelde on olnud piiratud, mis võib vähendada taustakontrolli sisulist ulatust (Riigikontroll, 2020). Sarnane probleem on eriti terav kolmandate riikide puhul, kus koostöökanalid ja andmete

usaldusväärsus võivad olla ebaühtlased (Rahandusministeerium, 2025). Seetõttu ei seisne risk üksnes selles, kas isik esitab vormiliselt korrektse taotluse, vaid selles, kas riigil on piisav ja usaldusväärne teave taotleja tegeliku tausta, seoste ja kavandatava tegevuse hindamiseks.

E-residentsuse riskikeskkonda mõjutavad ka erasektori vahendajad, kelle kaudu muutub Eesti ettevõtluskeskkond e-residentidele praktiliselt kasutatavaks. Äriühinguteenuse pakkujad, kontaktisikuteenuse osutajad, raamatupidajad ja muud teenusepakkujad võivad täita olulist väravahoidja rolli, kuna nende tegevusest sõltub, millisel määral tuvastatakse kliendi tegelik tegevus, kasusaajad ja võimalikud riskisignaalid. Kui hoolsusmeetmeid rakendatakse formaalselt või riskisignaalid ei jõua järelevalveasutusteni, võib vahendajate roll muutuda kriminogeenseks mitte seetõttu, et nad ise tingimata kuritegevuses osalevad, vaid seetõttu, et nende teenused võivad võimaldada juriidilise fassaadi loomist ja tegeliku kontrolli hajutamist (RAB, 2024a; Rahandusministeerium, 2025).

Lisaks õiguslikele ja institutsionaalsetele piirangutele tuleb arvestada tehnoloogiliste haavatavustega. Digitaalse identiteedi ja kaugtuvastuse kasutamine eeldab, et isiku, tema esitatud andmete ja hilisema tegevuse vaheline seos on usaldusväärselt kontrollitav. FATF on rõhutanud, et digitaalse identiteedi süsteemides tuleb arvestada identiteedivarguse, võltsitud andmete ja anonüümsuse kuritarvitamise riskidega, mis võivad hõlbustada vara päritolu varjamist rahapesuskeemides (FATF, 2020). Rahandusministeeriumi riskihinnangus on samuti osutatud, et tehisintellekti ja sünavõltsingute areng võib suurendada riski, et isikut tõendavaid dokumente või biomeetrilisi tuvastusprotsesse manipuleeritakse finants- või virtuaalvääringu teenustele ligipääsu saamiseks (Rahandusministeerium, 2025, lk 140).

Kokkuvõttes käsitletakse e-residentsust käesolevas töös süsteemse riskikeskkonnana, kus finantskuritegevuse riskid võivad tekkida digitaalse ligipääsu, Eesti juriidilise vormi, piiriülese majandustegevuse, vahendajate ja piiratud kontrollivõimekuse koosmõjus. See ei tähenda, et e-residentsus ise oleks finantskuritegevuse põhjus, vaid et selle kaudu loodud seaduslikud võimalused võivad teatud tingimustel muutuda kasutatavaks piiriülestes skeemides. Töö empiirilises analüüsis hinnatakse, kas ja millistes vormides need teoreetiliselt eeldatavad haavatavused praktikas avalduvad.

2.3. Riskipõhise regulatsiooni teoreetilised alused

E-residentsuse programmi riskide maandamine eeldab strateegilist lähenemist, mis suudab ühendada tehnoloogilise innovatsiooni, majandusliku avatuse ning järelevalve- ja julgeolekukaalutlused. Black ja Baldwin (2010) rõhutavad, et tõhus riskipõhine regulatsioon peab olema mitte ainult proportsionaalne, vaid „tõeliselt kohanev“ (*really responsive*). See tähendab, et regulatsioon peab kohanema reguleeritava valdkonna dünaamikaga, arvestama reguleeritavate osapoolte käitumisega ning reageerima keskkonnamuutustele, sealhulgas tehnoloogilisele arengule. Riskipõhine lähenemine ei saa piirduda staatilise eelkontrolliga, vaid peab hõlmama pidevat monitooringut, tagasiside mehhanisme ning institutsionaalset õppimist. (Black ja Baldwin, 2010)

Lisaks rõhutavad Black ja Baldwin, et riskipõhine regulatsioon eeldab regulaatorilt nn poliitilist luba tegutseda, kuna ressursside prioritiseerimine tähendab paratamatult teadlikku riskimist valdkondades, mis on klassifitseeritud madala ohuastmega. See võib asetada järelevalveasutused avaliku vastutuse ja kriitika alla, kui riskid realiseeruvad valdkondades, mida peeti esialgu madala riskiga. (Black ja Baldwin, 2010)

E-residentsuse puhul omandab selline riskipõhise regulatsiooni poliitiline ja institutsionaalne keerukus erilise tähenduse, kuna territoriaalsed järelevalvemudelid toimivad paikade ruumi loogikas, samas kui e-residentsuse kaudu loodud majandustegevus asetub piiriülesesse voogude ruumi (Castells, 2010). See võimaldab osapooltel ära kasutada jurisdiktsioonilisi erinevusi ja soodustab nn jurisdiktsioonilist šoppamist, mille puhul tegevus ja vastutus hajutatakse mitme riigi vahel. Sellistes tingimustes ei piisa järelevalvelt üksnes rikkumistele reageerimisest, vaid vajalik on ennetav ja paindlik kohanemisvõime.

E-residentsuse kontekstis tähendab see, et pelgalt taustakontroll digi-ID väljastamise hetkel ei ole piisav, vaid vajalik on Blacki ja Baldwini mõistes tõeliselt kohanev järelevalve, mis suudab tuvastada muutusi riskiprofiilides, arvestada reguleeritavate käitumisstrateegiatega ning reageerida uutele finants- ja küberkuritegevuse vormidele.

Seda süsteemset vaadet toetab rahvusvaheline standard International Organization for Standardization (ISO) 31000 (2018), mis käsitleb riskijuhtimist kui organisatsiooni juhtimise lahutamatu osa, mille eesmärk on aidata luua ja kaitsta väärtust. Standardi järgi ei ole riskijuhtimine üksik kontrollimeede, vaid pidev ja süsteemne protsess, mis hõlmab riskide tuvastamist, hindamist, käsitlemist ning nende järjepidevat jälgimist ja ülevaatamist. Risk tähendab ISO 31000 käsitluses ebakindluse mõju eesmärkidele, mistõttu peab riskijuhtimine

olema kohandatud konkreetsele tegevuskeskkonnale ning arvestama nii sisemiste kui väliste muutustega. Oluline on, et see protsess oleks integreeritud otsustusprotsessidesse ning põhineks parimal kättesaadaval teabel, võttes arvesse ka inimkäitumise ja organisatsioonikultuuri mõju. (ISO 31000, 2018)

E-residentsuse kontekstis tähendab see, et riskijuhtimine peab olema integreeritud kogu programmi elutsükklisse ning võimaldama süsteemset seiret, andmevahetust ja koostööd nii riigisiselt kui ka EL-i tasandil. Samas peab riskipõhine strateegia suutma ühendada kaks erinevat lähenemist: reeglite täitmise kontrolli ja tegeliku ohu märkamise. Praktikas võib tekkida olukord, kus e-resident või temaga seotud ettevõtte vastab formaalselt nõuetele, kuid tegevuse tegelik riskiprofiil viitab kõrgendatud ohule. Samuti võib järelevalve tuvastada reaalse riski, kuid tal puudub seaduslik alus sekkumiseks, sest ühtegi konkreetset reeglit pole veel rikutud. Tõhus riskijuhtimine peabki ISO 31000 käsitluse järgi leidma tasakaalu, et järelevalve ei piirduks formaalse nõuetele vastavuse kontrolliga, vaid keskenduks programmi tegelikule riskitasemele ja turvalisusele. (ISO 31000, 2018)

Selleks, et järelevalve püsiks ajakohasena, peab see vältima ka mudeli lühinägelikkust ehk olukorda, kus ametnikud jäävad liigselt kinni varem kokkulepitud ohumärkidesse. Kuna e-residentsuse keskkond ja tehnoloogia muutuvad kiiresti, ei pruugi vanad kontrollimeetodid uusi ohte enam tuvastada. ISO 31000 standard toetab seda mõtet, märkides, et riskijuhtimine peab olema dünaamiline (ISO 31000, 2018).

E-residentsuse areng on algusest peale toimunud innovatsiooni ja julgeoleku vahelises pingeväljas. Nagu Kotka, Vargas Alvarez del Castillo ja Korjus (2016) rõhutavad, kujundab programmi edasiminekut pidev tasakaaluotsing majandusliku avatuse ja turvalisuse vahel. See tähendab, et riskijuhtimine ei tohi muutuda innovatsiooni pärssivaks, kuid samal ajal ei saa institutsionaalset usaldust eksportida ilma piisava kontrollivõimekuseta (Kotka, Vargas Alvarez del Castillo & Korjus, 2016). See eeldab riskijuhtimist, mis on integreeritud programmi juhtimisse ning mida ajakohastatakse vastavalt muutuvatele tehnoloogilistele ja piiriülestele riskidele.

Sellisel mõistetuna ei ole riskide maandamine e-residentsuse puhul üksikute meetmete kogum, vaid kohanemisvõimeline institutsionaalne protsess, mis peab olema proportsionaalne ja suutma reageerida digitaalses ning piiriüleses keskkonnas tekkivatele kriminogeensetele asümmeetriatele. Riskipõhine regulatsioon muutub seega mehhanismiks, mille kaudu riik püüab tasakaalustada usalduse ekspordi ja kontrolli säilitamise vahel tekkinud struktuurset pinget.

2.4. Analüütiline mudel: kriminogeensete asümmeetriate rakendamine e-residentsuse kontekstis

Käesoleva töö analüütiline mudel tugineb eelnevalt käsitletud Passase (2003) kriminogeensete asümmeetriate teooriale ja Castellsi (2010) võrgustikuühiskonna käsitlusele. Passase teooria võimaldab selgitada, kuidas regulatiivsed, institutsionaalsed, informatsioonilised ja jurisdiktsioonilised ebakõlad võivad luua finantskuritegevust soodustavaid tingimusi. Castellsi käsitlus aitab omakorda mõtestada, miks need ebakõlad avalduvad eriti teravalt piiriüleses digitaalses keskkonnas, kus majandustegevus, kapital ja informatsioon liiguvad voogude ruumis, samal ajal kui järelevalve, vastutus ja õiguslik sekkumisvõimekus jäävad valdavalt paikade ruumi loogikasse.

E-residentsuse kontekstis tähendab see, et finantskuritegevuse riskid ei tulene üksnes üksikutest rikkumistest või tehnilistest puudustest, vaid võivad kujuneda süsteemsetest haavatavustest. Digi-ID, Eesti ettevõtte, äriühinguteenuse pakkujad, finantsteenuste vahendajad ja piiriülesed makselahendused toimivad eraldiseisvalt õiguspärase mehhanismidena, kuid nende koosmõjus võib tekkida keskkond, kus juriidiline legitiimsus, digitaalne ligipääs ja territoriaalselt piiratud järelevalve loovad võimalusi kuritegeliku tegevuse varjamiseks või hajutamiseks. Sellisel juhul ei ole tegemist süsteemivälise rikkumisega, vaid olukorraga, kus legaalsed institutsioonid ja teenused võivad tahtmatult toimida kuritegelike skeemide infrastruktuurina.

Analüütilises mudelis rakendatakse eelnevalt määratletud nelja asümmeetriat e-residentsuse kontekstis. Informatsiooniline asümmeetria avaldub olukorras, kus Eesti ametiasutustel või kohustatud isikutel puudub piisav, usaldusväärne või õigeaegne teave taotleja tausta, tegeliku tegevuse, kasusaajate või rahavoogude kohta. See võib tekkida näiteks juhul, kui vajalik info paikneb välisriigi registrites, sõltub rahvusvahelisest andmevahetusest või jääb erasektori vahendajate poolt tuvastamata ja edastamata. Regulatiivne asümmeetria väljendub olukorras, kus õigusnormide, hoolsusmeetmete või järelevalvestandardite erinevused võimaldavad osapooltel kasutada Eesti digitaalset ja ettevõtluskeskkonda soodsama või nõrgema kontrollikeskkonnana. Jurisdiktsiooniline asümmeetria tekib siis, kui ettevõtte registreerimise koht, tegelik juhtimine, majandustegevus, rahavood, kannatanud ja kahju paiknevad eri riikides. Institutsionaalne asümmeetria viitab pädevuste, vastutuse ja infovahetuse hajumisele erinevate riigiasutuste, EL-i tasandi institutsioonide ning erasektori teenusepakkujate vahel.

Need asümmeetriad ei toimi e-residentsuse süsteemis eraldi, vaid põimuvad omavahel. Näiteks võib Eestis registreeritud ettevõtte anda piiriülesele tegevusele formaalse õiguspärasuse, samal ajal kui ettevõtte tegelik juhtimine, pangakonto, kliendid ja rahavood paiknevad teistes

jurisdiktsioonides. Sellises olukorras ühenduvad jurisdiktsiooniline ja informatsiooniline asümmeetria: Eesti riigil on küll formaalne seos juriidilise isikuga, kuid sisuline kontroll tegevuse, tegelike kasusaajate ja rahavoogude üle sõltub teiste riikide andmetest ja koostöövalmidusest. Kui sellele lisandub erasektori vahendajate keskne roll ettevõtte loomisel ja haldamisel, muutub risk ka institutsionaalseks, sest kontrollivõimekus ei sõltu üksnes riigiasutustest, vaid ka kohustatud isikute hoolsus- ja teatamiskohustuse sisulisest täitmisest.

Selline mudel võimaldab käsitleda e-residentsust mitte üksnes digitaalse identiteedi või ettevõtlusprogrammina, vaid piiriülese regulatiivse ruumina, kus riiklikult väljastatud usaldusmärk võib omandada kuritegelikes skeemides väärtuse just oma formaalse legitiimsuse tõttu. Eesti digi-ID, juriidiline vorm või tegevusluba võivad sellistes skeemides toimida usaldusmehhanismina, mis aitab varjata tegevuse tegelikku sisu, tegelikke kasusaajaid või rahavoogude päritolu. See haakub Passase käsitlusega legaalse ja illegaalse sfääri liidesest ning süsteemsest sünergiast: kuritegelik tegevus ei pruugi toimida väljaspool seaduslikku majanduskeskkonda, vaid võib kasutada selle enda institutsioone, teenuseid ja usaldusmehhanisme.

Samal ajal tuleb arvestada, et e-residentsuse süsteem ei kujuta endast ainult riskiallikat, vaid on seotud ka Eesti strateegilise eesmärgiga laiendada oma digitaalset ulatust ja eksportida institutsionaalset usaldust. Hardy (2023) käsitlus aitab siin mõista, miks väikeriik võib avatud ja asukohasõltumatut digitaalset majandusruumi arendada ka olukorras, kus sellega kaasneb järelevalvevõimekuse ja avatuse vaheline pinge. Seega ei käsitleta käesolevas töös e-residentsusega seotud riske pelgalt programmi puudujääkidena, vaid laiemate struktuursete pingetena, kus majanduslikud, strateegilised ja regulatiivsed eesmärgid ei pruugi täielikult kattuda.

Eeltoodust lähtudes suunavad empiirilist analüüsi järgmised teoreetilised ootused:

- 1) E-residentsusega seotud finantskuritegevuse riskid avalduvad korduvate riskimustritena ning põhinevad Eesti digitaalse identiteedi, juriidilise vormi või ettevõtluskeskkonna usaldusväärse kasutamisel piiriülestes skeemides.
- 2) Riskimustrid peegeldavad informatsioonilisi, regulatiivseid, jurisdiktsioonilisi ja/või institutsionaalseid asümmeetriaid.

- 3) Riskid realiseeruvad legaalse ja illegaalse sfääri liideses, kus formaalselt õiguspäraseid ettevõtteid, tegevuslubasid, makselahendusi või vahendajaid kasutatakse tegevuse varjamiseks või hajutamiseks.
- 4) Regulatiivsete ja järelevalvemehhanismide toimivust piirab piiriülese digitaalse keskkonna ja territoriaalselt korraldatud järelevalve vaheline lahknevus.

Nende ootuste alusel seostatakse empiirilises analüüsis dokumentides ja intervjuudes tuvastatud riskimustrid kriminogeensete asümmeetriatega ning hinnatakse, mil määral vastavad regulatiivsed ja järelevalvemehhanismid riskide tegelikule olemusele. Analüüsi keskmes ei ole seega üksnes küsimus, milliseid riske e-residentsus tekitab, vaid ka see, miks need riskid võivad kujuneda just piiriüleses digitaalses keskkonnas ning millised struktuursed piirangud nende maandumist mõjutavad.

3. Metoodika ja andmeallikad

Magistritöö kolmas peatükk annab ülevaate uurimuse metodoloogilisest ülesehitusest, andmeallikatest ja analüütilisest raamistikust. Peatükis põhjendatakse valitud kvalitatiivset uurimisstrateegiat ning kasutatud meetodeid, mille abil analüüsitakse e-residentsusega seotud finantskuritegevuse riskide realiseerumist, nende seost kriminogeensete asümmeetriatega ning regulatiivsete ja järelevalvemehhanismide toimivust. Samuti selgitatakse, kuidas teoreetilises raamistikus sõnastatud ootused suunavad dokumentide ja intervjuuandmete analüüsi.

3.1. Kvalitatiivne uurimisstrateegia ja meetodite põhjendus

Käesolev magistritöö põhineb kvalitatiivsel uurimisstrateegial, mille eesmärk on analüüsida e-residentsusega seotud finantskuritegevuse riskide realiseerumist, seostada tuvastatud riskimustrid kriminogeensete asümmeetriatega ning hinnata, mil määral vastavad Eesti ja EL-i regulatiivsed ning järelevalvemehhanismid nende riskide tegelikule olemusele. Uurimisprobleemi iseloomust tulenevalt ei ole eesmärgiks kvantitatiivne üldistamine, vaid riskide avaldumise mehhanismide, nende piiriülese iseloomu ning regulatiivsete ja institutsionaalsete mehhanismide süvitsi mõistmine. Selline lähenemine võimaldab käsitleda uuritavat uurimisobjekti selle kompleksuses ning on suunatud sotsiaalsete protsesside ja tähenduste tõlgendamisele (Creswell, 2014).

Käesolevas uurimuses käsitletakse e-residentsust mitmetasandilise nähtusena, kus põimuvad tehnoloogilised, õiguslikud ja institutsionaalsed aspektid ning mille toimimist ei saa eraldada selle laiemast kontekstist. Selliste protsesside analüüsimine eeldab süvitsi minevat ja kontekstipõhist käsitlust (Yin, 2018), kuna e-residentsusega seotud riskid avalduvad valdavalt piiriüleses keskkonnas ning on seotud kriminogeensete asümmeetriatega. Seetõttu ei ole neid võimalik adekvaatselt analüüsida üksnes statistiliste näitajate kaudu, vaid vajalik on nende kontekstuaalne ja sisuline tõlgendamine.

Analüüsis rakendatakse induktiivset loogikat, liikudes üksikutest empiirilistest tähelepanekutest üldisemate teemade ja korduvate riskimustrite suunas (Braun & Clarke, 2006). Selline lähenemine sobib uurimuse eesmärgiga, kuna võimaldab tuvastada e-residentsuse süsteemile omaseid korduvaid mehhanisme ilma neid eelnevalt rangelt ette määratlemata. Uurimistulemuste usaldusväärsuse tagamiseks kasutatakse andmete triangulatsiooni, kombineerides dokumendianalüüsi ja ekspertintervjuusid (Yin, 2018; Creswell, 2014), mis

võimaldab võrrelda ametlikes dokumentides esitatud riskimustreid institutsioonide praktikatasandi hinnangutega.

Teoreetiline raamistik suunab empiirilist analüüsi eelkõige nelja asümmeetria kaudu: informatsiooniline, regulatiivne, jurisdiktsiooniline ja institutsionaalne asümmeetria. Nende kaudu tõlgendatakse dokumentides ja intervjuudes ilmnevaid riskimustreid ning hinnatakse, kuidas need seostuvad piiriülese digitaalse keskkonna ja territoriaalselt korraldatud järelevalve vahelise pingega.

Uurimuse teoreetiline raamistik toetub transnatsionaalse kuritegevuse käsitlustele, Passase (2003) kriminogeensete asümmeetriate teooriale ning Castellsi (2010) võrgustikuühiskonna käsitlusele. Passase teooriat kasutatakse riskimustrite aluseks olevate regulatiivsete, institutsionaalsete ja jurisdiktsiooniliste ebakõlade selgitamiseks, samas kui Castellsi käsitlus aitab mõtestada piiriülese digitaalse majandustegevuse ja territoriaalse järelevalve vahelist pinget. Regulatiivsete ja järelevalvemehhanismide toimivuse hindamisel lähtutakse riskipõhise regulatsiooni põhimõtetest (ISO 31000, 2018; FATF, 2025), keskendudes nende võimekusele riske ennetada, tuvastada ja neile reageerida.

Seega põhineb analüüs kolmel omavahel seotud sammul: esiteks kaardistatakse empiiriliselt tuvastatud riskimustrid, teiseks seostatakse need kriminogeensete asümmeetriatega ning kolmandaks hinnatakse, milliste regulatiivsete ja järelevalvemehhanismide kaudu neid riske ennetatakse, tuvastatakse ja neile reageeritakse ning mil määral vastavad need mehhanismid riskide tegelikule olemusele.

3.2. Uurimismeetodid

Käesolevas magistritöös kasutatakse kvalitatiivset uurimismeetodite kombinatsiooni, mis hõlmab dokumendianalüüsi ning poolstruktureeritud ekspertintervjuusid. Selline lähenemine võimaldab analüüsida e-residentsuse programmiga seotud finantskuritegevuse riskide avaldumist ning siduda teoreetiline raamistik empiiriliste tähelepanekutega.

3.2.1. Dokumendianalüüs

Dokumendianalüüsi kasutatakse uurimuse keskse meetodina, mille eesmärk on kaardistada e-residentsuse programmiga seotud finantskuritegevuse riskide realiseerumine ning tuvastada nende aluseks olevad mustrid ja mehhanismid. Dokumendianalüüs võimaldab süstemaatiliselt analüüsida olemasolevaid tekstilisi allikaid ning tuvastada neis esinevaid mustreid ja tähendusi, pakkudes seejuures institutsionaalset konteksti uuritava nähtuse mõistmiseks (Bowen, 2009).

Dokumendianalüüs hõlmab rahvusvahelisi ja riiklikke analüütilisi ning hindavaid allikaid, sealhulgas Rahandusministeeriumi riikliku rahapesu riskihinnangut (2025), Kaitsepolitsei 2024-2025 ning 2025-2026 aastaraamatuid, RAB uuringut „Virtuaalvääringu teenuse pakkujatega seonduvad riskid Eestis“ (2022), RAB tüpoloogiateadet (2024c), Moneyval 2022. aasta hindamist „Rahapesu ja terrorismi rahastamise vastased meetmed Eestis“ (2022) ning Riigikontrolli auditit (2020). Selliste dokumentide kasutamine võimaldab analüüsida e-residentsusega seotud finantskuritegevuse riske ametlike allikate põhjal, mis kajastavad nii riskide tuvastamist, nende realiseerumise juhtumeid kui ka järelevalveasutuste praktilisi hinnanguid süsteemi toimimise ja haavatavuste kohta.

Dokumendianalüüsi käigus keskendutakse eelkõige järgmistele aspektidele:

- e-residentsusega seotud finantskuritegevuse riskid ja nende avaldumisvormid
- konkreetsete juhtumite ja tüpoloogiate põhjal tuvastatud korduvad riskimustrid ning nende toimemehhanismid
- Eestis loodud juriidiliste isikute, digitaalse identiteedi ja vahendajate roll piiriülestes finantskuritegevuse skeemides
- viited kriminogeensetele asümmeetriatele, sh jurisdiktsioonilistele, informatsioonilistele, institutsionaalsetele ja regulatiivsetele lahkevustele
- regulatiivsete ja järelevalvemehhanismide praktiline toimimine riskide ennetamisel, tuvastamisel ja neile reageerimisel ning nende toimimist mõjutavad regulatiivsed ja institutsionaalsed kitsaskohad.

Analüüsi raames kasutatakse toetavalt ka statistilisi näitajaid (nt e-residentidega seotud välispäringute andmed ning kriminaalmenetluste ja kohtuasjadega seotud kvantitatiivne teave), mis võimaldavad illustreerida riskide ulatust ning toetada kvalitatiivsete leidude tõlgendamist. Neid andmeid ei kasutata kvantitatiivse analüüsi läbiviimiseks, vaid taustainfona, mis aitab paremini mõtestada tuvastatud riskimustreid.

Dokumendianalüüsi tulemusi tõlgendatakse töö teoreetilise raamistiku valguses, keskendudes eeskätt sellele, milliseid korduvaid riskimustreid ja toimemehhanisme ametlikud allikad e-residentsuse kontekstis esile toovad. Passase kriminogeensete asümmeetriate teooriat kasutatakse selleks, et selgitada riskimustrite aluseks olevaid informatsioonilisi, regulatiivseid, institutsionaalseid ja jurisdiktsioonilisi ebakõlasid. Castelli võrgustikuühiskonna käsitlus aitab mõtestada piiriülese digitaalse majandustegevuse ja territoriaalse järelevalve vahelist pinget.

3.2.2. Poolstruktureeritud ekspertintervjuud

Dokumendianalüüsi täiendavad poolstruktureeritud ekspertintervjuud, mille eesmärk on saada parem arusaam sellest, kuidas e-residentsusega seotud riskid praktikas avalduvad, millised mehhanismid neid maandavad või kus esineb lünki. Samuti keskendutakse sellele, millistes punktides tekivad kriminogeensed asümmeetriad ning kuidas toimivad olemasolevad regulatiivsed ja järelevalvemehhanismid. Intervjuude abil kaardistatakse ka ekspertide hinnangud süsteemi arenguvajaduste kohta, sealhulgas praktilised kogemused ja hinnangud regulatsiooni toimivusele, mis ei pruugi kajastuda ametlikes dokumentides.

Poolstruktureeritud intervjuud sobivad käesoleva uurimistöö jaoks, kuna võimaldavad eesmärgipärase vestluse kaudu süvitsi mõista e-residentsusega seotud riske. Samuti võimaldavad need koguda detailset ja sisukat teavet, mida saab analüüsida andmetest lähtuvate teemade ja kategooriate kaudu (Yin, 2018). See lähenemine ühendab endas temaatilise võrreldavuse ja paindlikkuse, tuginedes varem koostatud temaatilisele intervjuukavale, mis tagab sarnaste põhiteemade käsitlemise kõigi osalejate puhul, kuid säilitab samal ajal vabaduse esitada täpsustavaid lisaküsimusi ja mõista uuritavat nähtust vahetult ekspertide vaatenurgast (Kalmus, Masso & Linno, 2015).

Intervjuukava ehitati üles uurimisküsimustest ja teoreetilisest raamistikust lähtuvate teemablokkide kaupa. Esmalt käsitleti e-residentsusega seotud riskide praktilist avaldumist ja peamisi riskimustreid. Teiseks keskenduti sellele, millistes punktides ilmnevad kriminogeensed asümmeetriad, sealhulgas informatsiooni, jurisdiktsiooni, institutsionaalse vastutuse või regulatiivse kontrolli lahknevus. Kolmandaks käsitleti olemasolevaid regulatiivseid ja järelevalvemehhanisme, eelkõige riskide ennetamist, tuvastamist ja neile reageerimist. Neljandaks käsitleti koostöö- ja andmevahetuse mehhanisme ning süsteemi arenguvajadusi.

Intervjueeritavateks olid e-residentsuse ökosüsteemiga seotud Eesti riigiasutuste eksperdid. Kokku viidi läbi kolm ekspertintervjuud: üks PPA, üks RAB-i ja üks MTA eksperdiga. Asutuste valik põhines nende kesksel rollile e-residentsusega seotud riskide tuvastamisel, hindamisel ja maandamisel. PPA vastutab e-residendi digi-ID väljastamise ning eel- ja järelkontrolli eest, RAB tegeleb finantskuritegevuse riskide analüüsi ja kahtlaste tehingute tuvastamisega ning MTA-l on vahetu kokkupuude e-residentidega seotud maksukäitumise ja majandustegevuse järelevalvega.

Selline valim võimaldab käsitleda e-residentsusega seotud riskide avaldumist ning nende üle teostatavat järelevalvet erinevate asutuste vaatenurgast. Kuigi intervjueeritavate arv on piiratud, on kvalitatiivse uurimuse eesmärk keskenduda nähtuse põhjalikule analüüsile ja selle toimimise

eripärade mõistmisele, mitte tulemuste statistilisele üldistamisele (Creswell, 2014). Dokumendianalüüsi ulatuslik kasutamine toetab seejuures empiirilist katvust, võimaldades intervjuude abil süvendada ja paremini lahti mõtestada dokumentidest tulenevaid leide.

Intervjuude valimi kujundamisel võeti ühendust ka FI ja RIA esindajatega. FI selgitas, et nende roll seisneb finantssektori järelevalves ja rahapesu tõkestamise süsteemide toimimise kontrollis, kuid neil puudub otsene kokkupuude e-residentsusega seotud riskimustrite ja konkreetsete juhtumite analüüsiga. RIA tõi esile, et e-residentide digi-ID ei erine tehniliselt teistest elektroonilise identiteedi vahenditest ning RIA roll piirdub digitaalse identiteedi taristu turvalisuse ja toimimise tagamisega. Nende seisukohtade põhjal otsustati keskenduda intervjuudes asutustele, kellel on otsene ja operatiivne kokkupuude e-residentsusega seotud finantskuritegevuse riskide avaldumise ja järelevalvega.

Kuigi kõik intervjuud kavandati läbi viia poolstruktureeritud formaadis, ilmnis MTA puhul erisus intervjuu läbiviimise viisis. Asutuse sisekorra kohaselt tuli eksperdil enne vastamist kooskõlastada nii intervjuu küsimused kui ka vastused asutuse sisekontrolliga. Sellest tulenevalt otsustati intervjuu läbi viia kirjalikus vormis e-posti teel küsimus-vastus formaadis. Selline lähenemine ei võimaldanud esitada täpsustavaid lisaküsimusi ega kohapealset arutelu, kuid tagas vastuste ametliku kooskõlastatuse, sisulise täpsuse ning adekvaatse ja põhjaliku informatsiooni, kuigi vähendas intervjuu paindlikkust võrreldes suulise formaadiga.

Käesolevas töös kasutatakse kvalitatiivsete andmete analüüsimiseks temaatilist analüüsi (Braun & Clarke, 2006), mille eesmärk on tuvastada ja tõlgendada andmetes esinevaid korduvaid tähendusmustreid. Suulised intervjuud transkribeeriti ehk litereeriti, st helisalvestised muudeti kirjalikuks tekstiks (Laherand, 2008).

Andmestik koosneb nii suuliste intervjuude transkriptsioonidest kui ka kirjalikus küsimus-vastus vormis saadud vastustest. Saadud andmestikku analüüsiti, keskendudes sellele, kuidas erinevad asutused kirjeldavad e-residentsusega seotud riskide avaldumist, nende põhjuseid ning regulatiivsete ja järelevalvemehhanismide toimimist. Analüüsi käigus võrreldi erinevate asutuste seisukohti omavahel ning seostati saadud tulemusi dokumendianalüüsi leidudega, et hinnata, kuivõrd kattuvad praktikas kirjeldatud riskid ja mehhanismid ametlikes raportites tuvastatud mustritega.

Selline kombineeritud analüüs võimaldab käsitleda e-residentsusega seotud finantskuritegevuse riske mitmetasandiliselt, sidudes riskide realiseerumise, regulatiivsete ja

institutsionaalsete mehhanismide toimimise ning nende piirangud ühtseks analüütiliseks tervikuks.

3.3. Analüütiline raamistik ja metoodilised piirangud

Analüütiline raamistik

Käesoleva uurimuse analüütiline raamistik põhineb e-residentsusega seotud finantskuritegevuse riskide realiseerumise ning nende maandamiseks rakendatud regulatiivsete ja institutsionaalsete mehhanismide toimivuse hindamisel. Uurimuse keskmes on küsimus, millisel määral vastavad olemasolevad regulatiivsed ja järelevalvemehhanismid praktikas avalduvatele riskimustritele ning millised struktuursed tegurid mõjutavad nende toimivust.

Empiiriline analüüs tugineb dokumendianalüüsi ja ekspertintervjuude kombineerimisele, mille kaudu seostatakse dokumentides tuvastatud riskimustrid asutuste praktikatasandi hinnangutega. Selline lähenemine võimaldab võrrelda, kuivõrd kattuvad ametlikes allikates esitatud riskikäsitlused praktikute kogemustega ning millised erinevused viitavad võimalikele regulatiivsetele ja institutsionaalsetele kitsaskohtadele.

Analüüsi loogika on mitmetasandiline. Esiteks kaardistatakse empiiriliselt tuvastatud riskide realiseerumise vormid ja mustrid ning grupeeritakse need nende realiseerumise mehhanismide alusel. Teiseks analüüsitakse, milliseid regulatiivseid ja institutsionaalseid mehhanisme nende riskide ennetamiseks, tuvastamiseks ja neile reageerimiseks rakendatakse. Kolmandaks tõlgendatakse saadud tulemusi teoreetilise raamistiku valguses, et selgitada, millised struktuursed ebakõlad mõjutavad nii riskide kujunemist kui ka nende maandamise võimalikkust.

Regulatiivsete mehhanismide toimivust ei hinnata käesolevas töös pelgalt küsimuse kaudu, kas need toimivad või mitte, vaid kolme analüütilise dimensiooni kaudu, lähtudes riskipõhise regulatsiooni loogikast. Selle kohaselt käsitletakse regulatsiooni protsessina, mis hõlmab riskide ennetamist, tuvastamist ja neile reageerimist. Selline lähenemine tugineb riskijuhtimise põhimõtetele (ISO 31000, 2018), mille kohaselt tuleb esmalt tuvastada ja hinnata riskid ning seejärel rakendada nende maandamiseks sobivaid kontrollimehhanisme. Sarnane loogika on aluseks ka rahapesu tõkestamise rahvusvahelises raamistikus, kus rõhutatakse riskide tuvastamist ja hindamist, proportsionaalsete maandamismeetmete rakendamist ning süsteemi võimekust tuvastada rikkumisi ja neile reageerida (FATF, 2025).

Sellest lähtuvalt hinnatakse käesolevas töös regulatiivsete mehhanismide toimivust kolme analüütilise dimensiooni kaudu:

- Ennetamine - mil määral on olemasolevad mehhanismid suunatud riskide tekkimise vältimisele (nt eelkontroll, hoolsusmeetmed)
- Tuvastamine - mil määral võimaldavad järelevalve- ja seiresüsteemid riske õigeaegselt avastada (nt rahapesukahtluse teated, välipäringud, riskiprofiilid)
- Reageerimine - milliseid meetmeid rakendatakse pärast riskide realiseerumist (nt tegevuslubade tühistamine, digi-ID kehtetuks tunnistamine, kriminaalmenetlus).

Analüüsi käigus seostatakse empiiriliselt tuvastatud riskimustrid, institutsioonide praktikad ja teoreetilises raamistikus käsitletud kriminogeensed asümmeetriad, et hinnata, mil määral vastavad regulatiivsed ja institutsionaalsed mehhanismid riskide tegelikule olemusele ning kas nende toimivust mõjutavad struktuursed piirangud piiriüleses digitaalses keskkonnas.

Metoodilised piirangud

Uurimisel on mitmeid piiranguid, mida tuleb tulemuste tõlgendamisel arvesse võtta. Analüüs põhineb avalikult kättesaadavatel sekundaarsetel allikatel ning institutsioonide poolt edastatud teabel, mille detailsus ja ulatus on paratamatult piiratud. Nii dokumendianalüüsis kui ka intervjuudes esitatud teave kajastab peamiselt avalikku või avalikustamiseks sobivat informatsiooni, mistõttu ei hõlma see kõiki e-residentsusega seotud riskijuhtumeid ega näita nende tegelikku ulatust. Seda kinnitas ka intervjuude käigus ilmnenu asjaolu, et osa käsitletavast teabest on asutusesiseseks kasutamiseks ning ei ole avalikustatav.

Samuti on piiratud ja osaliselt killustunud uurimuses kasutatav statistiline teave. E-residentidega seotud kuritegevuse, päringute ja järelevalvemenetluste kohta puudub ühtne ja terviklik andmestik, kuna vastavad andmed on jaotunud erinevate asutuste vahel ning ei ole täiel määral avalikult kättesaadavad. Seetõttu kasutatakse kvantitatiivseid näitajaid üksnes illustratiivsel eesmärgil ning need ei võimalda teha järeldusi riskide tegeliku leviku kohta.

Lisaks iseloomustab käsitletavat nähtust latentne kuritegevus, mistõttu ei pruugi kõik toimepandud õigusrikkumised jõuda õiguskaitseasutuste vaatevälja ega kajastuda ametlikes menetlustes või statistikates. Sellest tulenevalt võib uurimuses käsitletud realiseerunud juhtumite ja riskimustrite põhjal kujunev pilt olla paratamatult osaline.

Uurimus keskendub peamiselt Eesti riigiasutuste perspektiivile, mistõttu EL-i tasandi regulatiivsete ja järelevalvemehhanismide praktiline toimimine kajastub eelkõige kaudselt, dokumentide ja riiklike praktikate kaudu. Kuigi EL-i tasandi regulatsioonid loovad e-residentsuse toimimiseks üldise õigusraamistiku, ei ole nende rakendumist ja mõju konkreetsetele riskijuhtumitele võimalik käesolevas töös vahetult hinnata.

Nende piirangute leevendamiseks kasutatakse erinevate andmeallikate triangulatsiooni, mis võimaldab kompenseerida avalike andmete piiranguid, sidudes dokumendianalüüsi tulemused juhtumipõhiste näidete ja ekspertide praktikakogemusega.

Käesoleva töö koostamisel kasutati tehisintellektil põhinevaid abivahendeid, sealhulgas ChatGPT-d teksti keeleliseks toimetamiseks ja NotebookLM-i allikate läbitöötamise toetamiseks. Töö sisulised seisukohad, analüüs ja järeldused on autori enda omad.

4. Empiiriline analüüs

Käesolevas peatükis analüüsitakse, millisel määral ja millistes vormides on e-residentsuse programmiga seotud finantskuritegevuse riskid praktikas realiseerunud. Empiiriline analüüs põhineb kvalitatiivsel lähenemisel, mis ühendab dokumendianalüüsi ning poolstruktureeritud ekspertintervjuud.

Riskide realiseerumise all mõistetakse käesolevas töös olukordi, kus e-residentsuse kaudu loodud ettevõtteid või digitaalset identiteeti on kasutatud rahapesu, maksupettuste, sanktsioonirikkumiste või muu finantskuritegevusega seotud tegevustes. Analüüsi eesmärk on selgitada, millistes mehhanismides ja struktuurides sellised riskid avalduvad, milline on nende piiriülene iseloom ning kuidas toimivad nende maandamiseks loodud kontrolli- ja järelevalvemehhanismid.

Dokumendianalüüsi käigus käsitletakse eelkõige institutsionaalsetes allikates kajastatud riskijuhtumeid, tüpoloogiaid ja riskihinnanguid, tuginedes Rahandusministeeriumi riiklikule rahapesu riskihinnangule (2025), Kaitsepolitsei 2024-2025 ning 2025-2026 aastaraamatutele, RAB uuringule „Virtuaalvääringu teenuse pakkujatega seonduvad riskid Eestis“ (2022), RAB tüpoloogiateatele (2024c), Moneyval 2022. aasta hindamisele „Rahapesu ja terrorismi rahastamise vastased meetmed Eestis“ (2022) ning Riigikontrolli auditile (2020).

Nimetatud allikates käsitletakse e-residentsust eeskätt piiriülese riskikeskkonnana, kus Eesti digitaalset identiteeti ja juriidilist vormi võidakse kasutada olukorras, kus tegelik tegevus, kontroll, rahavood või kahju paiknevad väljaspool Eesti vahetut jurisdiktsiooni. Moneyvali 2022. aasta hindamine rõhutab seejuures eelkõige tegelike kasusaajate tuvastamise ja ettevõtete läbipaistvusega seotud haavatavusi, samas kui Rahandusministeeriumi 2025. aasta riskihinnang toob peamise rahapesuriskina esile Eestis loodud ettevõtete ärakasutamise teistes riikides. Need hinnangud moodustavad dokumendianalüüsi lähtekoha, mida täpsustatakse järgnevalt konkreetsete riskimustrite ja juhtumite kaudu.

Dokumendianalüüsi täiendavad poolstruktureeritud ekspertintervjuud, mille eesmärk on avada, kuidas kirjeldatud riskid avalduvad praktikas, kuidas neid riigiasutuste tasandil hinnatakse ning milliseid lünki nähakse olemasolevates regulatiivsetes ja järelevalvemehhanismides. Selline lähenemine võimaldab siduda teoreetilises raamistikus käsitletud kriminogeensed asümmeetriad empiiriliste tähelepanekute ja praktikute hinnangutega.

Kuna e-residentsusega seotud kõiki riskijuhtumeid ei ole süsteemselt käsitletud ning avalikult kättesaadav teave nende kohta on piiratud, käsitletakse käesolevas peatükis tuvastatud

juhtumeid indikatiivsete näidetena laiematest struktuursetest haavatavustest. Üksikjuhtumid võimaldavad hinnata, millistes mehhanismides ja kontekstides riskid avalduvad ning kas teoreetilises osas käsitletud kriminogeensed asümmeetriad leiavad praktikas kinnitust.

Rahandusministeeriumi Eesti riikliku rahapesu riskihinnangu (2025) kohaselt on e-residentsuse programmi rahapesu jääkriski tase keskmine. Jääkriski all mõistetakse riskitaset, mis püsib ka pärast rahapesu ennetamiseks ja tõkestamiseks rakendatud kontrolli-, järelevalve- ja hoolsusmeetmeid ning peegeldab hinnangut sellele, kui tõenäoline on rahapesu aset leidmine vaatamata olemasolevatele meetmetele. Peamine e-residentsusega kaasnev rahapesurisk on Eestis loodud ettevõtte ärakasutamine teistes riikides (Rahandusministeerium, 2025, lk 154), mis viitab riskide valdavalt transnatsionaalsele iseloomule ning haakub teорияosas käsitletud kriminogeensete asümmeetriatega.

Seega käsitletakse peatükis esmalt dokumendianalüüsi tulemusi (alapeatükk 4.1), mis keskendub realiseerunud riskijuhtumitele, riskimustritele ja nende toimetehhanismidele ning seejärel ekspertintervjuude tulemusi (alapeatükk 4.2), mis võimaldavad hinnata nende riskide praktilist käsitlemist, institutsionaalset toimimist ning regulatiivseid kitsaskohti.

4.1. E-residentsusega seotud finantskuritegevuse riskide realiseerumine

4.1.1. Realiseerunud riskimustrid ja juhtumianalüüs

Käibemaksupettused

MTA hinnangul on e-residentidega seotud riskimustrites keskse tähtsusega käibemaksukohustuslase registreerimisnumbri (KMKR) kuritarvitamine. Rahapesu kontekstis käsitatakse selliseid skeeme tüpoloogiana, kus maksupettus toimib rahapesu eelkuriteona. (Rahandusministeerium, 2025). Praktikas tähendab see, et Eesti ettevõtteid kasutatakse piiriülestes käibemaksupettuse skeemides formaalsete tehingupartnerite või vahendajatena, mille eelduseks on kehtiva KMKR numbri olemasolu.

Rahapesu Andmebüroo 2022. aasta tüpoloogiateate kohaselt lisab KMKR numbri olemasolu Eesti juriidilisele isikule näilise usaldusvääruse, mida võidakse ära kasutada nii käibemaksupettustes kui ka rahapesuskeemides. KMKR ei ole üksnes maksutehniline tunnus, vaid toimib EL-i siseturul usaldusmehhanismina, mis võimaldab ettevõtetel osaleda piiriülestes tehingutes ja rakendada nullmääraga maksustamist (RAB, 2022b). Just see formaalne õiguspärasus võimaldab ettevõtetel osaleda rahvusvahelistes tarneahelates ka siis, kui tegelik majandustegevus Eestis puudub või on minimaalne.

Passase käsitlemise järgi on selline olukord iseloomulik legaalse ja illegaalse sfääri liidesele, kus õiguspärane regulatiivne tunnus, antud juhul KMKR number, võimaldab kuritegelikus skeemis tekitada usaldusväärsuse ja formaalse vastavuse mulje. Seetõttu ei seisne risk üksnes KMKR tehnilises kuritarvitamises, vaid selles, et EL-i siseturu toimimiseks loodud usaldusmehhanismi saab kasutada piiriülese pettuse varjamiseks.

Nii RAB 2022 tüpoloogiateade kui ka Eesti riiklik rahapesu riskihinnang 2020–2024 osutavad muustrile, kus Eesti juriidilisi isikuid kasutatakse välisriikides toimepandavates maksupettustes vahelülidena. Sageli on selliste ettevõtete juhatuse liikmeteks või seotud isikuteks mitteresidendid, sh e-residendid ning ettevõtte tegelik juhtimine toimub väljaspool Eestit. Sellisel juhul ei seisne risk digitaalse identiteedi tehnilises väärkasutuses, vaid selles, et e-residentsuse kaudu loodud Eesti ettevõtte toimib rahvusvahelises maksupettuse ahelas vahendina (Rahandusministeerium, 2025; RAB, 2022b).

Järgnevalt käsitletakse kahte Eesti riiklikus rahapesu riskihinnangus esitatud juhtumit, mis illustreerivad KMKR kuritarvitamisega seotud piiriülese käibemaksupettuse skeeme.

JUHTUM 1

Uurimise kohaselt asutasid kahtlusalused 15 EL-i liikmesriigis ettevõtteid, mis tegutsesid seaduslike elektroonikakaupade tarnijatena. Veebipoodide kaudu müüdi EL-is asuvatele klientidele üle 1,48 miljardi euro väärtuses elektroonikaseadmeid. Kuigi lõpptarbijad maksid oma ostudelt käibemaksu, ei tasunud kaupu müüvad äriühingud oma maksukohustusi. Ettevõtteid maha jättes välditi tasumata maksusummade ülekandmist erinevatele riiklikele maksuhalduritele. Teised pettuseahela lülid taotlesid seejärel riiklikelt maksuhaldurilt käibemaksutagastust, millega tekitati hinnanguliselt 297 miljoni euro suurune käibemaksukahju. Kuritegelikust tegevusest saadud tulu liigutati *offshore* kontodele. Rahade liigutamiseks kasutati muu hulgas 11 tegelikku majandustegevust mitteomavat Eesti OÜ-d, millega oli seotud 13 e-residenti. (Rahandusministeerium, 2025, lk 159)

Selle juhtumi põhjal võib järeldada, et risk ei realiseerunud mitte Eesti siseselt, vaid piiriüleses skeemis, kus Eesti ettevõtteid kasutati rahavoogude vahendamiseks ja tehinguahela ülesehituse toetamiseks. Kuigi põhiline müügitegevus ja maksukahju tekkimine toimusid teistes EL-i liikmesriikides, täitsid 11 tegeliku majandustegevuseta Eesti ettevõtted skeemis tehnilist ja juriidilist rolli, võimaldades raha liigutamist ning andes tehingutele formaalse legitiimsuse. Nende ettevõtetega seotud 13 e-residendi osalus viitab sellele, et e-residentsuse kaudu loodud või juhitud ettevõtteid kasutati skeemis distantsilt hallatavate struktuuridena, millel puudus sisuline seos Eesti majanduskeskkonnaga.

Järgnevalt käsitletav juhtum näitab, et sarnane loogika võib avalduda ka teistsuguses kontekstis, viidates korduva riskimuustrile.

JUHTUM 2

Alates 2017. aastast juhtis ühe EL-i riigi vahendustevõtte erinevaid käibemaksupettuse skeeme. 2020. aastal sisenesid samad käibemaksupettuse skeemi korraldajad kaitsemaskide turule. Kuritegeliku ühenduse juhitud tarneahelas kasutati eri riikides, sealhulgas Hongkongis ja asjaomases EL-i riigis, varifirmasid, variisikuid ja fiktiivseid identiteete. Uurimise kohaselt ei tasunud tarneahela alguses olev ettevõtte ega Hongkongis asuv ettevõtte käibemaksu summadel, mille nad olid saanud näomaskide müügist EL-i riigi ministriumile. Teadaolevalt osales skeemis kaks Eesti ettevõtet, millest ühe juhatuse liikmeks oli välisriigi kodanikust e-resident. Eesti ettevõttel puudus tegelik tegevus. Hinnanguliselt peteti skeemiga välja kuni 195 miljonit eurot. (Rahandusministeerium, 2025, lk 159)

Teine juhtum näitab, et Eesti ettevõtete kasutamine piiriülestes käibemaksupettustes ei olnud üksikjuhtum. Ka selles skeemis täitsid Eesti ettevõtted formaalset ja vahendavat rolli, kuigi Eestis neil puudus tegelik majandustegevus. Eesti juriidiline vorm võimaldas skeemi ülesehitust ning andis tehingutele näilise õiguspärasuse, samal ajal kui maksukahju tekkis teises liikmesriigis. Asjaolu, et ühe Eesti ettevõtte juhatuse liikmeks oli e-resident ning ettevõtte juhtimine toimus sisuliselt väljastpoolt Eestit, viitab taas sellele, et risk seisneb eeskätt distantsilt hallatavate juriidiliste isikute kasutamises rahvusvahelistes skeemides.

Nimetatud juhtumid näitavad, et e-residentsusega seotud käibemaksupettuse risk ei tulene niivõrd süsteemi tehnilisest puudujäägist, vaid Eesti õigusruumi, KMKR-i ja juriidilise vormi usaldusväärsuse ärakasutamisest piiriülestes skeemides. Passase käsitluses väljendub siin legaalse ja illegaalse sfääri liides: formaalselt õiguspärased ettevõtlusstruktuurid võimaldavad anda petuskeemidele usaldusväärse vormi ning hajutada tegevuse mitme jurisdiktsiooni vahel. Castelli käsitluses avaldub sama dünaamika voogude ruumi ja paikade ruumi lahknevusena, kus tehingud ja kahju liiguvad piiriüleses võrgustikus, kuid kontrollimehhanismid jäävad seotuks riiklike jurisdiktsioonidega.

Juhtumid näitavad ühtlasi, et kuigi Eesti ettevõtteid kasutatakse skeemides olulise lülina, tekib otsene maksukahju teistes liikmesriikides. Seetõttu toimib Eesti juriidiline vorm sellistes skeemides pigem vahendava platvormina, samas kui peamine majanduslik kahju realiseerub väljaspool Eesti jurisdiktsiooni.

Rahapesu

Eesti riikliku rahapesu riskihinnangu (2025) kohaselt ei seisne e-residentsusega seotud rahapesurisk enamasti Eesti siseses eelkuriteos, vaid olukorras, kus Eestis registreeritud ettevõtteid kasutatakse välismaal toime pandud kuritegudest saadud tulu liigutamiseks ja kihistamiseks. Tüüpiline muster hõlmab Eesti ettevõtte nimel pangakontode avamist - sageli

välisriikide makseasutustes - kuhu laekuvad vahendid pettustest, maksurikete või muudest eelkuritegudest. Seejärel liiguvad rahalised vahendid edasi eri jurisdiktsioonide vahel, muutes nende päritolu tuvastamise keerukamaks (Rahandusministeerium, 2025).

Castelli käsitles on selline rahapesumuster tüüpiline voogude ruumi loogikale: rahalised vahendid, maksekontod ja tehingud liiguvad piiriüleses digitaalses võrgustikus, samal ajal kui nende kontrollimine sõltub riigipõhistest menetlustest ja andmevahetusest.

Selline muster haakub laiemate riskiteguritega, millele on viidanud RAB varasemad analüüsid. Väheste või olematu majandustegevusega juriidilised isikud kujutavad endast kõrgendatud riski rahapesuks ja muudeks finantskuritegudeks. 2024. aasta järelanalüüsis märgitakse, et registrist kustutatud ettevõtete hulgas oli välismaalastega seotud ettevõtteid proportsionaalselt enam kui üksnes Eesti isikutega seotud ettevõtteid, mis viitab nõrkadele aktiivsuse näitajatele ja potentsiaalsele kuritarvitamise riskile (RAB, 2024b).

Eelkirjeldatud riskimustrite kontekstis on oluline roll ka äriühinguteenuse pakkujatel, kellel lasub kohustus rakendada hoolsusmeetmeid ning teatada kahtlastest tehingutest. RAB-i 2024. aasta uuring täpsustab nende kesket rolli e-residentide ja Eesti ärikeskkonna vahelise liidesena: ligikaudu 69% e-residentidega seotud ettevõtetest kasutas äriühinguteenuse pakkuja kontaktisikuna, samas kui elamisloaga välismaalaste puhul oli see osakaal ligikaudu 9%. Lisaks pakuvad samad teenuseosutajad sageli paralleelselt ettevõtte loomise, raamatupidamise ja nõustamise teenuseid, mistõttu on nad seotud ettevõtte mitme toimimistasandiga. (RAB, 2024a) Riikliku rahapesu riskihinnangu kohaselt on nende teatamisaktiivsus praktikas väga madal, mistõttu oluline osa esmastest riskisignaalidest ei jõua järelevalveasutusteni (Rahandusministeerium, 2025). See on e-residentsuse kontekstis eriti problemaatiline, sest vahendajad täidavad korraga nii ligipääsu võimaldaja kui ka esmase kontrollija rolli.

Vahendajate roll on otseselt seotud ka juriidiliste isikute läbipaistvuse ja tegelike kasusaajate tuvastamisega. Kuigi Eesti lõi 2023. aastal tegelike kasusaajate andmekogu (TEKSA), jääb välisriigi omanikega ettevõtete puhul andmete õigsus ja ajakohasus sõltuvaks kolmandate riikide teabe kvaliteedist ning kohustatud isikute hoolsusmeetmete täitmisest (Rahandusministeerium, 2025, lk 46). See haakub Moneyvali hinnanguga, et Eesti ei pruugi piisava kindlusega tuvastada paljude ettevõtete tegelikke omanikke, mis vähendab äriregistri läbipaistvust ja suurendab riski, et Eesti juriidilist vormi kasutatakse piiriülestes skeemides tegeliku kontrolli varjamiseks (Moneyval, 2022).

Passase teooria vaates ei ole sellised vahendajad pelgalt kõrvalised teenuseosutajad, vaid potentsiaalsed legaalse ja illegaalse sfääri ühendajad. Kui äriühinguteenuse pakkujad aitavad ettevõtteid luua ja hallata, kuid ei täida sisuliselt hoolsus- ja teatamiskohustusi, võib nende roll muutuda kriminogeenseks: nad ei pruugi ise olla kuritegeliku skeemi korraldajad, kuid nende teenused võimaldavad skeemidel omandada õiguslikult korrektse vormi.

Rahapesu riskimustri keskne kriminogeenne asümmeetria avaldub jurisdiktsioonilises killustatuses: ettevõtte registreerimise riik, pangakonto asukoht, tehingu toimumiskoht ja tegelik kasusaaja võivad paikneda eri riikides. Selline struktuur peegeldab Passase käsitles kirjeldatud kriminogeenset asümmeetriat, kus majandustegevus ja regulatiivne kontroll paiknevad eri jurisdiktsioonides. See raskendab oluliselt ka järelevalveasutuste koostööd, pikendab infovahetuse ahelat ning hajutab vastutuse sidumise võimalusi. E-residentsus ei ole siin iseenesest eelkuriteo allikas, vaid võimaldab toimida digitaalse infrastruktuurina, mille kaudu saab piiriülest skeemi administratiivselt hallata.

Empiirilised andmed kinnitavad kirjeldatud riskimustrit. Eesti riikliku rahapesu riskihinnangu (2025) andmetel on e-residentsusega seotud ettevõtted rahapesukahtlusega teadetes märkimisväärselt nähtavad: aastatel 2020–2024 oli 5,4% kõigist RAB-le esitatud teadetest seotud e-residendi või tema ettevõttega ning tervikuna on järelevalveasutuste teadetest läbi käinud 5,8% kõigist e-residentidega seotud Eesti ettevõtetest. (Rahandusministeerium, 2025)

Teadete sisulist kaalukust ilmestab asjaolu, et 11,7% e-residentide või nende ettevõtete kohta esitatud teadetest edastati teistele ametiasutustele. Tegemist on mõnevõrra kõrgema edastamise protsendiga kui teiste RAB-i teadete puhul, mis viitab, et e-residentide ja nende ettevõtete kohta tehtud teadetes esinevad viited kahtlasele tegevusele on keskmisest tugevamad. Programmi rahvusvahelist mõõdet peegeldab ka välispäringute osakaal: 53% e-residentide kohta tehtud teadetest pärineb välisriikidest ning tervelt 23,4% kõikidest välisriikide ametiasutustelt Eestile laekunud sisulistest rahapesukahtlusega päringutest on otseselt seotud e-residentide või nende poolt asutatud ettevõtetega. (Rahandusministeerium, 2025, lk 157) See osutab, et risk realiseerub valdavalt piiriüleses kontekstis.

PPA statistika kohaselt tunnistati aastatel 2020–2024 võimaliku rahapesu või rahapesukahtluse tõttu kehtetuks 78 e-residendi digi-ID. Kuigi PPA andmestik ei ole täielik - välispäringute puhul oli üksnes 44% juhtudest märgitud osapoole isiku- või registrikood -, näitavad olemasolevad andmed, et rahapesumärgendiga välispäringud laekusid 113 ettevõtte kohta, millest 31% olid seotud e-residentidega. Lisaks tehti päringuid kokku üheksa e-residendi kohta. Välispäringutes esinevaid ettevõtteid iseloomustab mitmekihiline isikuline seotus, kus sama struktuuriga on

seotud nii Eesti kodanikud, e-residendid kui ka muud mitteresidendid, mis viitab piiriülesele ja komplekssele omandistruktuurile. (Rahandusministeerium, 2025, lk 159)

Seega avaldub e-residentsusega seotud rahapesurisk eeskätt piiriüleses kontekstis, mida kinnitavad nii teadete kõrgem edastamismäär kui ka välisriikide märkimisväärne osakaal päringutes. Empiirilised andmed viitavad, et risk ei väljendu üksikjuhtumites, vaid korduvates mustrites, kus Eestis registreeritud ettevõtteid kasutatakse transnatsionaalsetes skeemides rahaliste vahendite liigutamiseks ja kihistamiseks. Seda võib tõlgendada Castelli ja Passase käsitluste koostoimes: rahapesukahtlused muutuvad Eestile nähtavaks sageli alles välisriikide päringute kaudu, sest kuritegelikud rahavood ja kannatanud paiknevad piiriüleses voogude ruumis, samal ajal kui Eesti ametiasutuste esmane teadmine sõltub territoriaalsest ja institutsionaalselt vahendatud infovahetusest.

Virtuaalvääringu teenusepakkujatega seotud realiseerunud riskimustrid

E-residentsuse programmi ja Eesti virtuaalvääringute sektori seotus illustreerib ilmekalt, kuidas transnatsionaalsed finantskuritegevuse riskid praktikas realiseerusid. 2025. aasta riikliku rahapesu riskihinnangu ja varasemate analüüside kohaselt on virtuaalvääringute sektor olnud üks peamisi kanaleid, kus e-residendi staatust on kuritarvitatud juriidilise fassaadi loomiseks, et pakkuda teenuseid ilma sisulise seoseta Eesti majandusruumiga (Rahandusministeerium, 2025; Moneyval, 2022).

Eesti oli üks esimesi jurisdiktsioone, mis rakendas 2017. aastal virtuaalvääringute teenuste (VASP) regulatsiooni, kuid esialgne tegevuslubade väljastamine oli pigem tehniline protsess, mis ei sisaldanud piisavat sisulist kontrolli turule sisenemisel. Praktikas võimaldas see paljudel ettevõtetel saada Eesti tegevusluba ilma, et neil oleks olnud Eestis reaalne tegevus või piisav vastavuskontrolli süsteem. RAB 2022. aasta uuringu andmetel oli 2021. aastal juulis ligi viis kuuendikku (umbes 83%) kehtiva Eesti tegevusloaga VASP-idest registreeritud neljale Tallinnas asuvalle aadressile, mis viitab sektori märkimisväärsele koondumisele ning formaalse tegevuskoha kasutamisele ilma tegeliku majandustegevuseta Eestis. (RAB, 2022a)

Sellise formaalse loamenetluse tulemusena kasvas väljastatud tegevuslubade arv kiiresti, ulatudes 2019. aasta lõpuks kokku 2447 loani, millest märkimisväärne osa kuulus e-residentidele. Riskide realiseerumine kulmineerus perioodil 2020–2022, mil RAB tühistas ligikaudu 70% väljastatud VASP-i litsentsidest, sh ainuüksi 2020. aastal 1808 litsentsi. Kehtetuks tunnistamiste aluseks olid muu hulgas nõrk või formaalne seos Eestiga,

hoolsusmeetmete ebapiisav rakendamine ning tegevuslubade kasutamine skeemides, mis olid seotud rahapesu- ja pettuseriskidega. RAB 2022. aasta analüüs kinnitas, et 44% aktiivsetest VASP-idest oli seotud endiste või selleaegsete e-residentidega, kes kasutasid Eesti jurisdiktsiooni usaldusväärse saavutamiseks, et varjata tegevust välisriikides. (RAB, 2022a; Moneyval, 2022)

Vastavalt RAB 2022. aasta analüüsile „Virtuaalvääringu teenuse pakkujatega seonduvad riskid Eestis“ ning Moneyval 2022. aasta hindamisele „Rahapesu ja terrorismi rahastamise vastased meetmed Eestis“ realiseerusid järgmised riskid:

- Äriühinguteenuse pakkujad asutasid massiliselt ettevõtteid (ligi 75% Eesti tegevusloaga virtuaalvääringu teenuse pakkujatest oli seotud isikute hulgas märgitud äriühinguteenuse pakkuja), hankisid neile VASP-litsentsid ning müüsid need seejärel e-residentidele, tekitades olukorra, kus järelevalveasutustel puudus reaalne ülevaade ettevõtte tegelikest juhtidest ja ärimudelitest.
- Eesti tegevusloaga VASP pakkujaid kasutati valdavalt rahapesu kihistamise etapis, kus välisriikides toime pandud kuritegudest – eeskätt pettustest, lunavararünnakutest ja narkokuritegevusest – saadud vara liikus läbi Eesti VASP-ide. RAB-i uuringu kohaselt oli Eesti residentidest klientide osakaal marginaalne (0,6-2%), samal ajal kui 83% teenusepakkujate kaudu liikunud vahenditest suunati Eestist edasi välisriikidesse, mis näitab Eesti rolli eeskätt piiriülese transiidisõlmena, mitte lõpliku sihtriigina. Ka välisriikide päringud ja õigusabitaotlused puudutasid peamiselt kuritegeliku päritoluga vara liikumist Eesti tegevusloaga VASP-teenusepakkujate kaudu.
- Realiseerus risk, kus Eesti litsentsi varjus tegutsev VASP pakkus korrespondentsuhte kaudu teenust tuhandetele tundmatutele klientidele *offshore* piirkondades, mille tulemusel puudus Eesti tegevusloaga teenusepakkujal tegelik ülevaade lõppklientide isikusamasusest, tegelikest kasusaajatest ja tehingute majanduslikust sisust, vähendades oluliselt läbipaistvust ning suurendades rahapesu ja sanktsioonirikkumiste riski.

VASP-ide juhtum tõi esile regulatiivse ebakõla, kus varasem loapõhine ja formaalse vastavuse kontrollile tuginev raamistik ei olnud piisav piiriülesest tegutsetavate ning tehnoloogiliselt vahendatud ärimudelite riskide maandamiseks. Selline olukord peegeldab Passase käsitluses kirjeldatud kriminogeenset asümmeetriat, kus globaalne majandustegevus ja finantsvood arenevad kiiremini kui riikide regulatiivne ja järelevalveline võimekus. Seda dünaamikat saab tõlgendada ka Castelli kirjeldatud voogude ruumi kaudu, kus kapital ja teenused liiguvad üle

riigipiiride digitaalses võrgustikus, samas kui riiklik järelevalve tugineb paikade ruumile omasele territoriaalsele loogikale. Eesti tegevusloa usaldusväärsus ja sektori kiire kasv ületasid riigi esialgse järelevalve tegeliku suutlikkuse, võimaldades turule siseneda ettevõtetel, kelle tegevus ei vastanud tegelikule riskitasemele.

E-residentsus ei olnud antud juhtumi juures risk iseenesest, vaid mehhanism, mis võimaldas Eesti jurisdiktsiooni usaldusväärst rahvusvaheliselt eksportida. Hardy varjupaigateooria valguses võib seda käsitleda väikeriigi strateegilise digitaalse avatusega kaasneva riskina: institutsionaalse usalduse eksport loob majanduslikke ja poliitilisi võimalusi, kuid võib samal ajal muuta selle usalduse kuritarvitatavaks olukorras, kus järelevalvevõimekus ei arene samas tempos (Hardy, 2023). See kogemus viitab sellele, et kui tehnoloogiline areng edestab järelevalvevõimekust, realiseeruvad piiriülesed riskid kiiresti, mistõttu peab regulatsioon olema ennetav, sisuline ja pidevalt kohanduv, et vältida olukorda, kus riik tegeleb üksnes juba tekkinud rikkumiste ja mainekahju tagajärgedega.

Riigi reaktsioon 2020. ja 2022. aasta RahaPTS-i muudatustega tähistas üleminekut formaalselt loapõhiselt lähenemiselt sisulisele riskipõhisele regulatsioonile. 2020. aasta RahaPTS muudatustega kehtestati muu hulgas kohustuslik tegelik tegevuskoht Eestis, rangemad nõuded juhatuse liikmete ja kontaktisikute pädevusele ning täpsustati hoolsusmeetmete rakendamise kohustusi. 2022. aastal karmistati nõudeid veelgi, tõstes omakapitali miinimumnõudeid ning tugevdades organisatsioonilisi ja järelevalvelisi kontrollimehhanisme. (Rahandusministeerium, 2025)

Sanktsioonikuriteod

Pärast Venemaa täiemahulise agressioonisõja algust Ukrainas 2022. aastal on suurenenud risk, et Venemaa ja Valgevene isikutega seotud Eesti ettevõtteid kasutatakse rahvusvahelistest sanktsioonidest hoidumiseks (Rahandusministeerium, 2025). RAB tüpoloogiateates 7TT202401 (2024) kirjeldatud skeemides on ühelt poolt indikaatoriteks majandusnäitajate ja tegevuse anomaaliad ning teiselt poolt seos Venemaa ja Valgevene kodanikega, sh läbi e-residentsuse (RAB, 2024c). 2024. aastal tuvastas MTA kokku 14 juhtumit rikkumisi Venemaa-vastaste ekspordipiirangute suhtes. Rikkumistega olid enim seotud Venemaa, Valgevene ja Iisraeli kodakondsusega seotud Eesti e-residendid või nende ettevõtted (Rahandusministeerium, 2025, lk 160)

Kaitsepolitseiameti aastaraamatust (2026) nähtub, et e-residentsuse kaudu loodud ettevõtteid on kasutatud strateegilise kauba hankimiseks Venemaa sõjatööstuse tellimusel. Siinkohal piirdub Eesti ärikeha funktsioon lääne tarnijate eksitamisega, samal ajal kui tegelik juhtimine ja tellimuste vormistamine toimub füüsiliselt Venemaal (KAPO, 2026, lk 54).

Kirjeldatud rikkumised ja riskid viitavad sellele, et e-residentsuse kaudu loodud ettevõtteid võivad toimida vahendavate üksustena sanktsioonirežiimist kõrvalehoidmisel. Risk ei seisne üksiktehingus, vaid struktuuris, kus Eesti ettevõtte osaleb tehinguahelas, samas kui tegelik majanduslik huvi või kontroll võib paikneda sanktsioonipiirangutega seotud jurisdiktsioonis. Selline skeem haakub Passase kirjeldatud kriminogeense asümmeetria loogikaga, kus majandustegevus ja kontroll paiknevad eri jurisdiktsioonides ning legaalse ettevõtlusstruktuuri kaudu hajutatakse vastutus ja tegelik kasusaaja üle mitme riigi. Castelli käsitluses väljendub sama dünaamika piiriüleste voogude ja territoriaalse kontrolli lahknevusena.

Mittetulundussektor

Eesti riikliku rahapesu riskihinnangu (2025) kohaselt on e-residentsuse programmiga seotud riskid realiseerunud ka mittetulundussektoris. Kuigi mittetulundusühingute (MTÜ) üldine rahapesu jääriski tase on hinnatud madalaks, osutab riskihinnang üksikjuhtumitele, kus e-residendid on kasutanud juriidilisi isikuid anonüümsete rahavoogude vahendamiseks. Erinevalt ettevõtetest, mille puhul eeldatakse selget majandustegevust, võimaldab MTÜ vorm koguda annetusi, mille puhul on doonorite ja vara päritolu tuvastamine sageli keerukam (Rahandusministeerium, 2025).

Järgnevalt käsitletav juhtum illustreerib näidet, kus annetuste päritolu ja kasutuse jälgitavus osutus ebapiisavaks ning organisatsiooniga olid seotud ka e-residendid.

JUHTUM 3

Juhtum kirjeldab Eesti mittetulundusühingule laekunud annetusi, mille puhul ei olnud võimalik tuvastada annetajaid ega vara täpset edasist kasutust. Konkreetse MTÜ-ga oli seotud mitu e-residenti. (Rahandusministeerium, 2025, lk 111).

Antud juhtum näitab, et risk ei pruugi avalduda klassikalise eelkuriteo ja sellele järgneva rahapesu skeemina, vaid võib seisneda rahaliste vahendite läbipaistmatuse ja kontrollitavuse puudumises. Kui annetajate identiteeti ei ole võimalik tuvastada ning vahendite kasutus jääb ebaselgeks, tekib olukord, kus MTÜ võib toimida vahendina teadmata päritoluga raha liigutamiseks või hoidmiseks. Asjaolu, et MTÜ-ga olid seotud e-residendid, viitab sellele, et e-

residentsuse kaudu loodud või juhitud juriidilised isikud võivad osaleda ka sellistes struktuurides, kus risk ei seisne otseses finantskuriteos, vaid järelevalve raskendatuses ja tehingute läbipaistvuse puudumises.

Seega avaldub e-residentsusega seotud risk ka usalduspõhises mittetulundussektoris, kus organisatsiooniline vorm ja rahvusvaheline seotus võivad muuta tegelike rahavoogude tuvastamise keerukamaks. Selline olukord haakub Passase käsitluses kirjeldatud legaalse ja illegaalse sfääri liidesega, kus seaduslik organisatsiooniline vorm võib pakkuda katet rahavoogudele, mille päritolu, eesmärk või tegelik kasusaaja ei ole tuvastatav. MTÜ vormi usalduspõhine ja annetustel põhinev iseloom võib seetõttu teatud tingimustel võimendada informatsioonilist asümmeetriat rahastajate, organisatsiooni ja järelevalveasutuse vahel.

Seos terrorismiga

Kaitsepolitseiameti aastaraamatu (2025) kohaselt on alates e-residentsuse programmi algusest 2014. aastal kokku tuvastatud 31 islamistliku terrorismi ja äärmusluse seostega välismaalast, kes on või on olnud e-residendid või on taotlenud e-residentsust. Lisaks sellele on e-residentide ja e-residentsuse taotlejate hulgas täheldatud isikuid, kes on seotud muude äärmuslike ja julgeolekuohu valdkondadega. (KAPO, 2025, lk 55) Antud juhul ei seisne risk üksnes võimalikus terrorismi rahastamises, vaid ka isiku tausta varjamises, kus e-residentsust on kasutatud vahendina ettevõtte loomiseks Eestis (KAPO, 2025).

Järgnevalt käsitletav juhtum illustreerib mustrit, kus isiku varasem seotus terrorismiga jäi nimevahetuse tõttu taustakontrollis tuvastamata ning e-residentsuse kaudu loodi Eestis ettevõtte.

JUHTUM 4

KAPO kirjeldab juhtumit, kus Euroopa päritolu isik reisis Süürias ja liitus terroristliku organisatsiooniga. Mitme aasta möödudes naasis ta Euroopasse ning muutis elukohariigis seaduslikult oma nime. Pärast nime muutmist taotles isik Eesti e-residentsust äritegevuse alustamiseks. Nimevahetuse tõttu ei tuvastatud tema varasemat seotust terrorismiga. Peale e-residendiks saamist asutas isik Eestis ettevõtte, mis ei alustanud majandustegevust. Isik käis korduvalt Eestis, külastas muu hulgas siinset lasketiiru ja harjutas eri relvade kasutamist. Kui KAPO tuvastas seose nimevahetuse ja terrorismitausta vahel, tehti kohe ettepanek isikule sissesõidukeelu kehtestamiseks ja e-residentsus tunnistati kehtetuks (KAPO, 2025, lk 51)

Antud juhtum näitab olukorda, kus e-residentsusega kaasnevad riskid ei realiseeru mitte otsese finantskuritegevuse, vaid identiteedipõhise kontrollilünga ja juriidilise vormi väärkasutamise kaudu. E-residentsuse programm loob võimaluse asutada Eestis ettevõtte ning siseneda EL-i

majandusruumi, mistõttu on taustakontrolli tõhusus kriitilise tähtsusega. Kui isik muudab seaduslikult oma nime, võib see ajutiselt katkestada varasema julgeolekualase info sidumise uue identiteediga. Juhtum näitab, et e-residentsuse kaudu loodud ettevõtte peamine roll ei pruugi seisneda majandustegevuses, vaid juriidilise ja majandusliku kohalolu loomises EL-is. Selline skeem ei eelda kohest finantskuritegu, kuid võib pakkuda katet edasiseks tegevuseks või tugevdada isiku legitiimsuse kuvandit.

Juhtum osutab, et piiriüleses keskkonnas sõltub taustakontroll suurel määral riikidevahelisest andmevahetusest ning identiteedi tuvastamisest, mistõttu võivad seaduslikud identiteedimuudatused ajutiselt tekitada kontrollilünki. E-residentsuse staatus ja sellega loodud juriidiline isik toimivad ka siin usaldusmehhanismina, mis annab isikule formaalse õiguspärasuse rahvusvahelises keskkonnas ka olukorras, kus tema varasem taust oleks pidanud takistama sellise staatuse saamist. Passase teooria vaates avaldub siin informatsiooniline asümmeetria: Eesti ametiasutuse otsus tugineb andmetele, mis sõltuvad teise riigi registritest, nimevahetuse jälgitavusest ja rahvusvahelise infovahetuse kvaliteedist.

Seega ei seisne risk üksnes üksikisiku tegevuses, vaid ka süsteemses olukorras, kus piiriülene identiteedihaldus, rahvusvaheline andmevahetus ja riiklikud kontrollimehhanismid ei pruugi olla täielikult kooskõlas. Selline olukord võib võimaldada julgeolekuriskiga isikutel kasutada legaalseid majandusstruktuure oma tegevuse varjamiseks või legitiimsuse suurendamiseks.

Tabelis 1 on kokkuvõtlikult esitatud dokumendianalüüsi põhjal tuvastatud peamised e-residentsusega seotud riskimustrid, nende empiiriline avaldumine ning teoreetiline tõlgendus kriminogeensete asümmeetriate ja piiriülese digitaalse keskkonna kontekstis.

Tabel 1. E-residentsusega seotud riskimustrid ja teoreetiline tõlgendus

Riskimuster	Empiiriline avaldumine	Teoreetiline tõlgendus
Käibemaksupettused	Eesti ettevõtte ja KMKR-i kasutamine piiriülestes tehinguahelates, kus maksukahju tekib valdavalt väljaspool Eestit	Legaalse ja illegaalse sfääri liides, jurisdiktsiooniline asümmeetria, piiriüleste voogude ja territoriaalse kontrolli lahknevus
Rahapesu	Eesti ettevõtete kasutamine välismaal toime pandud kuritegudest saadud raha liigutamiseks ja kihistamiseks	Jurisdiktsiooniline ja informatsiooniline asümmeetria, rahavoogude liikumine piiriüleses voogude ruumis
VASP sektor	Eesti tegevusloa, juriidilise fassaadi ja formaalse tegevuskoha kasutamine teenuste pakkumiseks ilma sisulise seoseta Eestiga	Regulatiivne ja informatsiooniline asümmeetria, voogude ruumi ja paikade ruumi lahknevus, institutsionaalse usalduse ekspordiga kaasnev risk

Sanktsioonirikkumised	Eesti ettevõtete kasutamine vahendava lülina sanktsioonidest kõrvalehoidmisel ja strateegilise kauba hankimisel	Jurisdiktsiooniline ja informatsiooniline asümmeetria, vastutuse ja tegeliku kasusaaja hajumine, piiriüleste tarneahelate ja territoriaalse kontrolli lahknevus
Mittetulundussektor	MTÜ vormi kasutamine anonüümsete või raskesti kontrollitavate rahavoogude vahendamiseks	Legaalse ja illegaalse sfääri liides, informatsiooniline asümmeetria rahastajate, organisatsiooni ja järelevalveasutuse vahel
Identiteedi- ja julgeolekuriskid	Taustakontrolli lüngad, nimevahetus, karistusandmete ja välisriigi riskiteabe piiratud kättesaadavus	Informatsiooniline ja jurisdiktsiooniline asümmeetria, digitaalse ligipääsu ja territoriaalselt paikneva taustateabe lahknevus

4.1.2. E-residentidega seotud välispäringute statistika

Eelneva põhjal joonistub välja e-residentsusega seotud riskide piiriülene iseloom. Täiendava mõõdme annab sellele PPA infosüsteemi sisestatud e-residentidega seotud välispäringute statistika aastatel 2020–2024, mis võimaldab hinnata riskide realiseerumise intensiivsust ajas (tabel 2).

Aastatel 2020–2024 puudutasid PPA-le laekunud välispäringud valdavalt kelmusi, rahapesu ja kuritegeliku tulude liikumist. Sisuliselt keskendusid pöördumised olukordadele, kus e-residendiga seotud ettevõtet kahtlustati kasutatavat ebaseaduslikes skeemides, sealhulgas ettevõtte pangakonto vahendite kihistamiseks või edasikandmiseks. 2023. aastal laekus enim välispäringuid Venemaa, Ukraina, Poola ja Läti kodakondsusega e-residentide kohta. Võrreldes 2022. aastaga langes Läti kodanikega seotud päringute arv kolm korda, samal ajal kui Venemaa kodakondsusega e-residentide kohta esitatud päringute maht kasvas umbes viiendiku võrra. (Rahandusministeerium, 2025, lk 160)

Tabel 2. E-residentide osas PPA-le laekunud välispäringud aastatel 2020–2024

Aasta	Füüsiliste isikute päringute arv	Juriidiliste isikute päringute arv	Kokku päringuid
2020	68	63	131
2021	51	82	133
2022	67	92	159
2023	51	68	119
2024	50	38	88
Kokku	287	343	630

Allikas: Rahandusministeerium, 2025 (Eesti riikliku rahapesu riskihinnang)

Tabelis 2 esitatud andmed osutavad, et aastatel 2020–2022 kasvas e-residentidega seotud välispäringute koguarv järjepidevalt (131 → 133 → 159), saavutades tipu 2022. aastal, millele järgnes langus 2023. ja 2024. aastal (119 ja 88). Langus ei pruugi siiski tähendada riskide tegelikku vähenemist, vaid võis osaliselt tuleneda menetluslikest ja tehnilistest muudatustest infosüsteemi kasutuskorralduses, sh võimalusest sisestada päringuid alates 16.06.2023 tagantjäre (Rahandusministeerium, 2025, lk 160). Seetõttu tuleb muutust tõlgendada ettevaatlikult ning mitte käsitleda seda otsese indikaatorina riskide kahanemisest.

Tabelist 2 nähtub, et perioodil 2021–2023 ületas juriidiliste isikute kohta tehtud päringute arv füüsiliste isikute päringuid. See viitab sellele, et riskikese paikneb eeskätt ettevõtete ärakasutamises võimalikes piiriülestes skeemides. Välispäringute koguarv saavutas haripunkti 2022. aastal (159 päringut), mis ajaliselt langeb kokku Venemaa täiemahulise agressioonisõja algusega Ukrainas 2022. aasta veebruaris. Kuigi otsest põhjuslikku seost ei saa esitatud andmete põhjal tuvastada, võis muutunud geopoliitiline olukord suurendada rahvusvaheliste õiguskaitseasutuste tähelepanu sanktsioonidega seotud riskidele.

2024. aastal langes päringute arv madalaimale tasemele (88 päringut). See võib olla seotud varem mainitud tehnilistest muudatustest PPA infosüsteemis, kuid võib ka otseselt olla seotud PPA poolt tõhustatud eelkontrolliga, mille negatiivsete otsuste osakaal taotlustele on tõusnud 2%-lt (2018) kuni 10,9%-le (2024), mis on aidanud ebasobiva taustaga isikuid programmist eemal hoida (Rahandusministeerium, 2025, lk 162). Esitatud andmete põhjal ei ole võimalik eristada, millises ulatuses mõjutasid päringute arvu tehnilised muudatused ning millises ulatuses eelkontrolli tugevnemine.

Tervikuna näitab analüüs, et välispäringute fookus on seotud ettevõtete kaudu toimivas piiriüleses finantsliikumises, mis kinnitab varasemalt tuvastatud transnatsionaalse riskimustri süsteemset iseloomu. Castelli käsitluses kinnitab see paikade ruumi ja voogude ruumi lahknevust: riskid tekivad ja liiguvad piiriülestes finants- ja ettevõtlusvõrgustikes, kuid Eesti ametiasutustele muutuvad need sageli nähtavaks alles siis, kui mõne teise riigi õiguskaitse- või järelevalveasutus esitab päringu. Seetõttu ei peegelda välispäringud üksnes konkreetseid kahtlusi, vaid ka seda, et e-residentsusega seotud kontroll sõltub suurel määral rahvusvahelise infovahetuse toimimisest.

4.1.3. E-residendid kriminaalmenetlustes ja kohtuasjades

E-residentide ja nendega seotud ettevõtete statistika kriminaalmenetlustes viitab sellele, et Eesti roll sellistes skeemides võib olla valdavalt piiriülese transiidikanali ja administratiivse fassaadi pakkumine. Aastatel 2020–2024 PPA-s menetletud 66-st rahapesu kriminaalasjast olid vaid viis seotud e-residentidega, millest omakorda üks lõpetati ja teine kvalifitseeriti ümber strateegilise kauba käitlemise nõuete rikkumiseks (Rahandusministeerium, 2025, lk 160). Siseriiklike menetluste vähesus peegeldab e-residentide ettevõtetega seonduvat peamist tegutsemisviisi, kus kuritegelik tegevus ja selle tulu liigutamine toimub väljaspool Eesti vahetut jurisdiktsiooni.

Seda toetab ka Riigiprokuratuuri hinnang, mille kohaselt on e-residentide ja nende ettevõtete kohta tehtavad päringud üks peamisi õigusabitaotlusi, mida Eesti Riigiprokuratuur teistest riikidest saab ning valdavalt on need välispäringud seotud just välisriikides toime pandud kelmustega (Rahandusministeerium, 2025, lk 161). Siseriiklike menetluste vähesuse ja välisriikidest laekuvate arvukate õigusabitaotluste ebakõla viitab sellele, et e-residendi juriidilist keha kasutatakse peamiselt väljaspool Eesti jurisdiktsiooni toime pandud eelkuritegude (nt kelmused, maksupettused ja küberkuritegevus) varjamiseks, mistõttu on siseriiklik kohtupraktika e-residentide osas peaaegu olematu – viie aasta jooksul on jõustunud vaid üks selline kohtuotsus.

Vähene siseriiklike menetluste arv tuleneb asjaolust, et e-residentide ettevõtetel puudub Eestis sageli reaalne majandustegevus ja kohalik pangakonto, mistõttu kuriteo vahetu toimepanemise paik ja tõendid asuvad välisriikides. Kuna Eesti karistusseadustik on territooriumikeskne ja piiriülene tõendite kogumine on ebatõhus, suunatakse menetlused eelistatult nendesse riikidesse, kus asuvad kannatanud või kus isik tegelikult tegutseb (Rahandusministeerium, 2025, lk 161). See toetab varem esile toodud riski: e-residentsus pakub kurjategijatele usaldusväärset juriidilist fassaadi, mis võimaldab hoida distantse tegeliku kuriteo toimumispaiga ja juriidilise lüli vahel.

See muster kinnitab Passase kirjeldatud vastutuse ja kontrolli hajumist: Eesti ettevõtte võib olla skeemis oluline juriidiline lüli, kuid kuriteo toimepanemise koht, kannatanud, tõendid ja rahavood paiknevad teistes jurisdiktsioonides. Castelli mõttes tähendab see, et kuritegelik tegevus organiseerub voogude ruumis, samas kui kriminaalmenetlus ja tõendite kogumine jäävad paikade ruumi institutsionaalsete piirangute alla.

Kokkuvõttes avaldub e-residentsusega seotud risk Eesti jaoks pigem rahvusvahelise koostöö ja õigusabitaotluste tasandil, kinnitades, et riigi roll on sellistes skeemides enamasti administratiivne või registripõhine, mitte vahetu kuriteo toimepanemise koht.

4.1.4. E-residendi staatuse omandamisega seotud realiseerunud riskid: eel- ja järelkontrolli haavatavused

E-residentsuse programmi usaldusväärsus toetub riigi suutlikkusele veenduda digitaalse identiteedi saajate tausta õiguskuulekuses, kuid praktikas on tuvastatud süsteemseid lünki, kus infosüsteemide puudulikkus ja piiratud andmevahetus on võimaldanud staatuse omandamist ebasobitavatel isikutel. Järgnevad juhtumid illustreerivad, kuidas takistused rahvusvahelises teabevahetuses ja siseriiklikes järelkontrolli protsessides on loonud võimalusi programmi väärkasutamiseks isikute poolt, kelle varasem karistusregister või äritegevuse piirangud oleksid pidanud olema takistuseks.

Välisriigi karistusregistrite kättesaamatus haldusmenetluses on üks kriitilisemaid kohti, mida ilmestab Riigikontrolli poolt läbi viidud võrdlus Soome registritega. Audit tuvastas, et e-residendi staatuse oli saanud 48 Soome kodanikku, kellel oli taotlemise hetkel koduriigis kehtiv kriminaalkaristus, sealhulgas süüdimõistmised kelmuste, mõrvakatse, vägistamise ja lapsporno omamise eest. Seejuures oli neljandikule neist määratud reaalne vangistus ning viiendikule karistus majanduskuritegude eest (Riigikontroll, 2020, lk 11). Probleemi põhjus seisneb asjaolus, et PPA-l puudub e-residentsuse kui haldusmenetluse raames õiguslik alus teha päringuid Euroopa karistusregistri infosüsteemi (ECRIS), mis on avatud vaid kriminaalmenetluste tarbeks (Riigikontroll, 2020).

Teoreetiliselt väljendab see Passase kirjeldatud informatsioonilist ja jurisdiktsioonilist asümmeetriat: e-residentsuse staatus annab isikule ligipääsu Eesti digitaalsele ja ettevõtluslikule taristule, kuid otsuse tegemiseks vajalik info paikneb teises jurisdiktsioonis ning ei ole haldusmenetluses kättesaadav. Seetõttu tekib olukord, kus formaalselt õiguspärane menetlus võib põhineda sisuliselt puudulikul riskiteabel.

Sarnane probleem avaldub ka välisriikides kehtestatud ärikeeldude tuvastamisel, mis on eriti problemaatiline, kuna suur osa e-residente liitub programmiga just ettevõtluse eesmärgil. Soome näitel selgus, et e-residendi staatuse oli programmi algusest kuni märtsini 2019 saanud vähemalt üheksa ärikeeluga isikut, kellest kaks tegutsesid Eesti ettevõtete juhatuse liikmetena. Nende riskide maandamiseks tõhustati kontrolli Soome suunal alates 2019. aasta aprillist ning PPA teeb nüüdseks eelkontrolli käigus päringuid Soome ärikeeldude kohta (Riigikontroll, 2020, lk 13-14). Sellest hoolimata püsib andmevahetuse vaakum ülejäänud maailma osas, kuna teiste riikidega, sealhulgas EL-i riikidega, puudub ärikeeldude valdkonnas siiani igasugune toimiv infovahetus (EIS, 2025; Rahandusministeerium, 2025). See võimaldab isikutel, kellel on

keelatud ettevõtlusega tegeleda oma asukohariigis, jätkata majandustegevust Eesti juriidilise keha varjus.

Lüngad ei piirdu vaid eelkontrolliga, vaid kandusid edasi ka järelkontrolli protsessi. 2020. aastal tuvastas Riigikontrolli audit juhtumeid, kus PPA oli jätnud digi-ID kehtetuks tunnistamata e-residentidel, kes on Eestis olles toime pannud kuritegusid, nagu kehaline väärkohtlemine, ähvardamine või narkootilise aine suures koguses ebaseaduslik käitlemine (Riigikontroll, 2020, lk 17). Samuti tuvastati olukord, kus e-residendile väljastati korduv dokument hoolimata asjaolust, et tal oli esimese digi-ID kehtivuse ajal saadud kehtiv kriminaalkaristus (Riigikontroll, 2020, lk 37). Siiski on olukord võrreldes 2020. aasta Riigikontrolli auditiga oluliselt muutunud ning PPA rakendab alates 2022. aasta juunist järelkontrolli automaatlahendust, mis võimaldab kontrollida e-residendiga seotud riskiinfot regulaarselt ja automaatselt (Rahandusministeerium, 2025).

Eel- ja järelkontrolli haavatavusi süvendavad ka tehnoloogilised arengud, mis võivad raskendada isiku tegeliku identiteedi ja tegevuse kontrollimist elektroonilistes keskkondades. Rahandusministeeriumi riskihinnangu kohaselt suurendab tehisintellekti ja süvavõltsingute kasutuselevõtt riski, et kuritegelikud võrgustikud manipuleerivad isikut tõendavate dokumentide, biomeetriliste tuvastusprotsesside või kaugtuvastuse lahendustega, et avada e-residentide nimel pangakontosid või virtuaalvääringu rahakotte (Rahandusministeerium, 2025, lk 140). FATF on samuti rõhutanud, et digitaalse identiteedi kasutamisel tuleb arvestada identiteedivarguse, võltsitud andmete ja anonüümsuse kuritarvitamise riskidega, mis võivad soodustada vara päritolu varjamist rahvusvahelistes rahapesuskeemides (FATF, 2020)

Viimastel aastatel on e-residentsuse programmis lisandunud julgeolekualased riskid ja oht ideoloogilisele radikaliseerumisele, mida kinnitab KAPO 2024. aasta statistika. Nimelt tegi KAPO 2024. aastal ettepaneku tühistada e-residentsus neljal isikul, kes olid radikaliseerunud terroristliku propaganda mõjul seoses Hamasi ja Iisraeli konfliktiga (KAPO, 2025, lk 48). Samuti tõkestati Araabia Ühendemiraatides elaval terrorismi toetajal IT-ettevõtte loomine Eestis, mida planeeriti kasutada terrorismi rahastamise kattevarjuna, illustreerides süsteemseid püüdlusi kasutada Eesti digitaalset ärikeskkonda kuritegeliku tegevuse fassaadina (KAPO, 2025, lk 55). Need juhtumid rõhutavad programmi süsteemset haavatavust, mis avaldub eriti teravalt kolmandatest riikidest – näiteks Pakistani, Hiina, India ja Türgi – pärit taotlejate puhul, kes moodustavad olulise osa programmi kasutajaskonnast (EIS, 2025, lk 26). Kuna nendes jurisdiktsioonides puuduvad Eestil sageli toimivad justiits-, julgeoleku- või õiguskaitsealased koostöösuhted, on isikute kriminaalse tausta, tegelike kuritegelike sidemete ja neist lähtuva

julgeolekuohu usaldusväärne kontrollimine praktiliselt võimatu (Rahandusministeerium, 2025).

E-residendi staatuse omandamisega seotud eelkontrolli konkreetne haavatavus realiseerus juhtumis, kus 2022. aasta jaanuari seisuga olid e-residendi staatuse saanud ja Eestis IT-ettevõtte asutanud kaks Põhja-Korea kodanikku. Need isikud pärinesid jurisdiktsioonist, mis on kantud FATF-i musta nimekirja (Moneyval, 2022, lk 26). FATF määratleb kategooria „Kõrge riskiga jurisdiktsioonid, mille suhtes FATF kutsub üles rakendama vastu meetmeid“ kui jurisdiktsioonid, mille rahapesu ja terrorismi rahastamise tõkestamise süsteemides on tuvastatud tõsised strateegilised puudujäägid ning mille suhtes kutsutakse liikmesriike üles rakendama kõrgendatud hoolsusmeetmeid ja vajaduse korral vastumeetmeid (FATF, 2022). Kuigi kõnealune ettevõtte eemaldati registrist enne tegevuse alustamist (Moneyval, 2022), illustreerib juhtum programmi eelkontrolli haavatavust: isegi teadaoleva päritoluriigi puhul võib inimlik eksimus või ebatäpsus võimaldada kõrge riskiprofiliga isikutel pääseda ligi Eesti juriidilisele infrastruktuurile. See osutab vajadusele sisulisema ja riskipõhisema eelkontrolli järele, et vältida riikliku digitaalse identiteedi usaldamist isikutele, kelle puhul esinevad ilmsed rahvusvahelised ohumärgid.

Analüütiliselt osutab juhtum sellele, et kõrge riskiga jurisdiktsioonide puhul ei piisa formaalsest taotluse kontrollist, vaid riskihindamine peab suutma siduda isiku päritolu, rahvusvahelise riskiprofiili ja kavandatava tegevuse sisulise hindamise. Passase mõttes avaldub siin regulatiivne asümmeetria: Eesti digitaalse ettevõtluskeskkonna avatus võimaldab ligipääsu ka olukorras, kus rahvusvaheline riskiteave peaks juba eelnevalt viitama kõrgendatud ohule.

Empiiriline analüüs näitab, et e-residentsusega seotud riskid ei avaldu üksikute erandlike juhtumitena, vaid korduvate mustritena eri valdkondades – maksupettustes, rahapesus, sanktsioonirikkumistes, virtuaalväeringute sektoris ning julgeolekujuhtumites. Nende juhtumite ühisjooneks on see, et Eestis registreeritud ettevõtted toimivad sageli piiriülestes skeemides vahendavate lülidena, samal ajal kui kuritegelik tegevus ja otsene kahju realiseeruvad valdavalt väljaspool Eesti jurisdiktsiooni.

Seda dünaamikat saab tõlgendada Passase kriminogeensete asümmeetriate ja Castelli ruumilise loogika koostoimes. Passase mõistes avaldub siin legaalse ja illegaalse sfääri liides, kus õiguspärased institutsionaalsed vormid, nagu Eesti ettevõtte, digi-ID, tegevusluba või MTÜ, võivad võimaldada kuritegeliku tegevuse varjamist või hajutamist. Castelli mõistes liiguvad tehingud, rahavood ja tegelik juhtimine voogude ruumis, samal ajal kui kontroll, vastutus ja

sekkumisvõimekus jäävad valdavalt paikade ruumi ehk riiklike jurisdiktsioonide ja andmevahetusmehhanismide raamidesse.

Dokumendipõhine analüüs võimaldab tuvastada riskide struktuuri ja ulatust, kuid ei anna täielikku ülevaadet sellest, kuidas neid riske praktikas tajutakse, hinnatakse ja maandatakse. Seetõttu käsitletakse järgmises alapeatükis ekspertintervjuude tulemusi, et hinnata, millisel viisil avalduvad kirjeldatud riskimustrid riigiasutuste igapäevases töös ning milliseid süsteemseid kitsaskohti praktikute hinnangul esineb.

4.2. Ekspertintervjuude tulemused

Ekspertintervjuude analüüs näitab, et e-residentsusega seotud finantskuritegevuse riskid ei avaldu üksikute eraldiseisvate juhtumitena, vaid korduvate mustrite ja mehhanismidena, mille keskseks tunnuseks on nende piiriülene iseloom ning seotus legaalse majandusstruktuuridega. Intervjuude põhjal kirjeldavad nii PPA, RAB kui ka MTA e-residentsust keskkonnana, kus riskide realiseerumine ei tulene niivõrd e-residendi staatusest iseenesest, vaid võimalusest kasutada Eesti digitaalset identiteeti ja ettevõtluskeskkonda osana rahvusvahelistest skeemidest. Sellest tulenevalt ilmnevad riskid eelkõige süsteemsete mehhanismidena, mis on seotud nii regulatiivsete ja informatsiooniliste piirangute kui ka piiriülese järelevalve killustatusega.

Intervjuutulemuste esitamisel eristatakse asutuste seisukohti üldistatud viidetega „PPA ekspert“, „RAB-i ekspert“ ja „MTA ekspert“. Kuna intervjuueeritavad käsitlesid osaliselt samu riskimustreid eri institutsionaalsest vaatenurgast, tuuakse järgnevalt välja nii kattuvad hinnangud kui ka asutusepõhised rõhuasetused. Selline esitus võimaldab näidata, millised riskid ilmnevad kõigi asutuste hinnangul süsteemselt ning millised probleemid tõusevad esile konkreetse järelevalve- või menetlusfunktsiooni kaudu.

4.2.1. Riskide avaldumine praktikas

Intervjuudes tõusis kõige selgemalt esile maksupettuste ja KMKR-i kuritarvitamise risk, kuid eri asutused kirjeldasid seda oma pädevusest lähtuvalt. MTA ekspert käsitles seda eeskätt maksujärelevalve probleemina: e-residendi asutatud Eesti ettevõttele taotletakse KMKR ning käibedeklaratsioonidel kajastatakse fiktiivseid soetusarveid ja 0% määraga müügiarveid, mis võib viia alusetute käibemaksutagastusteni ja välisriigis maksude vältimiseni. PPA ekspert kirjeldas sama mustrit taotluste ja järelevalve vaates, rõhutades, et Eesti ettevõtte ja KMKR-i

kasutamine võimaldab isikul esitada end eri riikide maksuhalduritele erinevalt. RAB-i vaates haakub maksupettuste risk rahapesu laiemate tüpoloogiatega, sest maksupettus võib toimida eelkuriteona ning Eesti juriidilist isikut kasutatakse hiljem piiriülese skeemi osana.

Rahapesu puhul on kõige otsesem institutsionaalne vaade RAB-il, kelle hinnangul jõuab suurem osa e-residentidega seotud infost RAB-i välisriikide rahapesu andmebüroode päringute kaudu. RAB ekspert rõhutas, et sageli on seos Eestiga üksnes siin asutatud juriidiline isik, millel puudub Eestis majanduslik tegevus või pangakonto, samal ajal kui kuritegu ja rahaliste vahendite liikumine toimuvad välisriigis. PPA ekspert kirjeldas sarnast mustrit kriminaalmenetluse vaates: rahapesu ja kelmuste puhul on Eesti ettevõtte sageli juriidiline lüli, kuid kannatanud, tõendid ja menetlus asuvad teises riigis. MTA vaade seostub selle riskiga peamiselt maksukuritegude kaudu, kuivõrd KMKR-i kuritarvitamine ja maksupettus võivad kujuneda rahapesu eelkuriteoks.

RAB viitab, et sarnaseid struktuure ja tüpoloogiaid kasutatakse ka sanktsioonidest kõrvalehoidumiseks, mis osutab selle riskimustri praktilisele esinemisele ning kasvavale olulisusele julgeolekupoliitilises kontekstis.

Sellega seondub keskne probleem, millele viitavad kõik kolm asutust, kus e-residenti asutatud ettevõtetel puudub sisuline majandustegevus Eestis ning selle juhtimine, kliendid ja rahavood paiknevad eri jurisdiktsioonides. Selline juriidilise vormi ja tegeliku majandustegevuse lahknemine võimaldab kasutada Eesti ettevõtteid piiriülestes skeemides, kus tehingud ei ole sisuliselt Eestiga seotud. Nii RAB-i kui PPA eksperdid viitavad, et suur osa e-residentide ettevõtetest on nn tühjad kehad, millel puudub Eestis pangakonto ja mis ei maksa siin makse. RAB-i eksperdi hinnangul on siin üheks oluliseks põhjuseks asjaolu, et Eesti pangad ei ole sageli valmis e-residentidele kontosid avama, pidades neid kõrgendatud riskiga klientideks. Selle tulemusena kasutatakse alternatiivseid makseasutusi, mille järelevalve on killustatum ning riskipõhise kontrolli rakendamine ebaühtlasem. See raskendab oluliselt kontrolli tehingute sisu ning tegelike kasusaajate üle.

Olulist rolli riskide realiseerumisel mängivad nii PPA kui RAB-i eksperdi arvates vahendajad ja äriühinguteenuse pakkujad, kes toimivad süsteemi nn väravahoidjatena, kuid kelle tegevuses ilmnevad olulised süsteemsed puudujäägid. PPA ekspert nägi probleemi eeskätt taotluste menetlemise kontekstis: osa teenusepakkujaid pakub e-residendile tervikpaketti, mis hõlmab e-residentsuse taotlemist, Eesti ettevõtte loomist ja vajadusel KMKR-i taotlemist, samuti on PPA tuvastatud sarnaste vastustega taotluste koondumist. RAB-i ekspert rõhutas seevastu äriühinguteenuse pakkujate rolli rahapesu tõkestamise süsteemi väravahoidjatena: kui

hoolsusmeetmeid ei rakendata sisuliselt ja kahtlastest asjaoludest ei teatata, ei jõua riskisignaali RAB-ini. Seega avaldub vahendajate risk kahes etapis: PPA vaates juba süsteemi sisenemisel ning RAB-i vaates hilisemas hoolsus- ja teatamiskohustuse täitmisel.

Lisaks ettevõtete ja tehingutega seotud riskidele toovad eksperdid esile ka identiteediga seotud ohud, mis avalduvad e-residentsuse taotlemise etapis. Käesolevas töös käsitletakse identiteediriski informatsioonilise asümmeetria praktilise avaldumisvormina, kuna probleem seisneb taotleja tegeliku isikusamasuse, kavatsuste või kasutaja kontrollitavuses.

PPA hinnangul on praktikas tuvastatud juhtumeid, kus taotlus esitatakse teise isiku dokumendi alusel või dokumendi kättesaamiseks saadetakse saatkonda volitamata isik. Digitaalse taotlusprotsessi käigus esitatavate dokumentide ja fotode puhul esineb võltsimisriske, mida PPA püüab maandada täiendavate kontrollimeetmetega, nagu lisafotode või videokinnituste küsimine. Samal ajal jääb füüsiline tuvastamine saatkonnas oluliseks kontrollibarjääriks. Riskikohtadena tõusevad esile ka vahendajad, kelle toel taotlemine võib suunata taotleja vastuseid ja tegevust menetlusprotsessis ning tehisintellekti kasutamine taotluste koostamisel, mis PPA hinnangul raskendab taotleja tegelike kavatsuste hindamist.

Riskide avaldumise dünaamikat kirjeldades märgivad eksperdid, et osa varasemalt esile tõusnud riskidest ei ole praktikas realiseerunud või on nende olulisus ajas vähenenud. PPA hinnangul oli varasemalt aktuaalne migratsioonirisk, kus e-residentsust püüti kasutada viisa või riiki sisenemise alusena, kuid see ei realiseerunud, kuna olemasolevad kontrollimehhanismid võimaldasid sellised juhtumid ennetavalt tuvastada ja tõkestada. Samal ajal kinnitavad nii PPA kui RAB, et varem kõrgendatud riskiga virtuaalväeringute teenusepakkujate (VASP) valdkond ei ole enam samal määral probleemne. See on seotud eelkõige järelevalve ja õigusraamistiku tugevdamisega, mille tulemusel suur osa tegevuslubadest tühistati ning turule on jäänud oluliselt vähem teenusepakkujaid, mille tagajärjel on vastava riskivaldkonna olulisus märkimisväärselt vähenenud.

Seejuures viitab RAB-i ekspert ka uuele potentsiaalsele riskisuunale hasartmängusektoris, kus õigusraamistiku muutused võivad suurendada e-residentide huvi kaughasartmängu tegevuslubade taotlemise vastu.

Kirjeldatud riskimuustrid viitavad olukorrale, kus majandustegevus, selle juriidiline vorm ja tegelik toimumiskoht paiknevad eri jurisdiktsioonides, luues võimalusi piiriüleseks väärkasutuseks. Intervjuude põhjal kasutatakse Eesti ettevõtet, KMKR-i, digi-ID-d ja vahendajate teenuseid legaalsete struktuuridena, mis annavad piiriülesele tegevusele formaalse

õiguspärasuse. Seejuures ei toimu riskide realiseerumine süsteemist väljaspool, vaid olemasoleva õigusliku ja institutsionaalse raamistiku sees, mis haakub kriminogeensete asümmeetriate teooria lähtekohaga.

4.2.2. Koostöö ja andmevahetuse mehhanismid

Ekspertintervjuudest ilmneb, et e-residentsuse süsteemi iseloomustab suhteliselt tugev siseriiklik koostöö, kuid samal ajal piiratud ja ebaühtlane rahvusvaheline andmevahetus. PPA ekspert tõi esile igapäevase koostöö MTA ja KAPO-ga ning kirjeldas RAB-iga suhtlust pigem kaasusepõhisena. MTA ekspert hindas riigisisest koostööd väga heaks ning rõhutas, et probleemsetes olukordades reageeritakse kiiresti ühiselt. RAB-i ekspert pidas juhtumipõhist koostööd toimivaks, kuid tõi esile vajaduse käsitleda e-residentsusega seotud riske laiemalt riskipõhise juhtimise ja riigi riskiisu vaates.

Rahvusvahelisel tasandil on pilt ebaühtlasem. PPA ja RAB rõhutasid, et oluline osa riskiteabest sõltub välisriikide päringutest, infovahetuse kiirusest ja konkreetse riigi koostöövalmidusest. PPA hinnangul on eriti piiratud ligipääs karistusandmetele, kuna mitmed riigid ei jaga vastavat teavet haldusmenetluse raames. Samuti sõltub info kättesaadavus taotleja päritoluriigist: kolmandatest riikidest pärinev teave võib olla raskesti kättesaadav, ebausaldusväärne või täielikult puududa. MTA ekspert nägi EL-i tasandi andmevahetust toetava vahendina terviklikuma riskipildi kujundamisel, kuid tõi esile vajaduse Euroopa-üleselt sidusama ettevõtte- ja isikuinfo järele.

Samas ei ole rahvusvaheline koostöö kõigis valdkondades ühtmoodi piiratud. RAB-i eksperdi hinnangul toimib rahapesu andmebüroode vaheline infovahetus suhteliselt kiiresti ja operatiivselt ning suur osa e-residentidega seotud riskisignaalidest jõuab Eestisse just välisriikide päringute kaudu. See viitab olukorrale, kus koostöö tõhusus sõltub kasutatavast kanalist ja valdkonnast: rahapesu andmebüroode võrgustikus võib info liikuda kiiresti, samas kui taustakontrolli, karistusandmete või maksualase info kättesaadavus on oluliselt piiratum.

Intervjuudes tõusis eraldi probleemina esile ka erasektori väravahoidjate roll. RAB-i ekspert rõhutas, et äriühinguteenuse pakkujatel lasub kohustus koguda ja hinnata teavet klientide tegevuse kohta ning edastada kahtluse korral teade, kuid praktikas on nende teatamisaktiivsus madal. See tähendab, et oluline osa esmatasandi riskiteabest ei pruugi jõuda järelevalveasutusteni. Seetõttu ei sõltu riskide tuvastamine üksnes riigiasutuste omavahelisest

koostööst või rahvusvahelisest andmevahetusest, vaid ka sellest, kas erasektori teenusepakkujad täidavad sisuliselt neile pandud hoolsus- ja teatamiskohustust.

Kokkuvõttes ilmneb, et e-residentsuse süsteemis on siseriiklik koostöö asutuste hinnangul toimiv, kuid rahvusvaheline andmevahetus jääb valdkonniti ebaühtlaseks. Riskide tuvastamine sõltub sellest, kas vajalik info liigub õigel ajal üle riigipiiride, kas see jõuab Eesti ametiasutusteni ning kas esmatasandi teenusepakkujad tuvastavad ja edastavad riskisignaale. Passase käsitluses peegeldab see informatsioonilist ja jurisdiktsioonilist asümmeetriat: piiriülene majandustegevus ja finantsvood liiguvad üle riigipiiride, samal ajal kui kontrollimehhanismid, andmebaasid ja menetlusõigused jäävad seotuks konkreetsete riikide ja institutsioonidega. Castelli vaates väljendub sama probleem voogude ruumi ja paikade ruumi lahknevuses: e-residentsusega seotud tegevus toimub piiriüleses digitaalses võrgustikus, kuid järelevalve sõltub territoriaalselt paiknevatest andmetest, asutustest ja koostöökanalitest.

4.2.3. Riskide maandamise strateegiad ja tulevikuvaade

Ekspertintervjuude põhjal on e-residentsusega seotud riskide maandamisel fookus nihkunud ennetavatele meetmetele, tehnoloogilistele lahendustele ning riskipõhisele järelevalvele. PPA eksperdi hinnangul väljendub see nii rangemates nõuetes kõrgendatud riskiga riikide taotlejate suhtes kui ka järelevalve praktikas, kus e-residentsuse staatuse tühistamine põhineb sageli riskihinnangul, mitte juba realiseerunud rikkumistel. PPA vaates on oluline arendada andmepõhiseid ja automatiseeritud riskihindamise lahendusi, sealhulgas tehisintellektil põhinevaid tööriistu, mis aitaksid taustakontrolli tõhustada ning suunata menetlusressurssi keerukamatele juhtumitele.

Oluliseks arengusuunaks peab PPA ka tehnoloogilisi lahendusi, eelkõige biomeetrilisel tuvastusel põhinevat mobiilirakendust HÕIVE, mis võimaldaks isikut tuvastada reaalajas ning vähendada sõltuvust füüsilisest dokumendist ja saatkonnakülastusest. Selline lahendus võib suurendada identiteedikontrolli usaldusväärsust, kuid eeldab samal ajal, et kaugtuvastuse ja biomeetria kasutamisega seotud riskid oleksid tehniliselt piisavalt maandatud. PPA hinnangul on oluline ka järelkontrolli arendamine, et isiku tegelik tegevus ja e-residentsuse kasutus vastaksid taotluses esitatud eesmärkidele.

MTA vaates seisneb riskide maandamine eelkõige riskipõhistes kontrollimenetlustes ja KMKR-i kasutamise sisulises hindamises. Tulevikuvaates rõhutas MTA ekspert vajadust Euroopa-ülese

andmetaristu järele, mis võimaldaks tõhusamalt kontrollida ettevõtetega seotud isikuid, sh ärikeelde, karistusi, juhatuse liikmeid ja osanikke.

RAB-i eksperdi intervjuust ilmneb, et riskide maandamisel on keskne vajadus selgemalt määratleda riigi riskiisu ning tasakaalustada programmi majanduslikud eesmärgid järelevalvevõimekusega. RAB-i vaates tuleb paremini mõtestada, millistele sihtrühmadele e-residentsust pakutakse, millist majanduslikku kasu programm tegelikult loob ning millist riski on riik valmis selle nimel aktsepteerima. Samuti toob RAB esile äriühinguteenuse pakkujate rolli tugevdamise, kuna nende madal teatamisaktiivsus piirab süsteemi võimekust tuvastada riskiskeeme varajases etapis. Lisaks näeb RAB-i ekspert vajadust lihtsustada e-residentsuse kehtetuks tunnistamise protsessi ning siduda see automaatselt seotud teenuste sulgemisega.

Kokkuvõttes näitavad ekspertintervjuud, et riskide maandamine liigub üha enam ennetava ja riskipõhise kontrolli suunas. PPA vaates tähendab see tugevamat eel- ja järelkontrolli, automatiseeritud riskihindamist ning tehnoloogilisi tuvastuslahendusi; MTA vaates riskipõhiseid kontrollimenetlusi ja paremat piiriülest andmetaristut; RAB-i vaates aga riigi riskiisu selgemat määratlemist, äriühinguteenuse pakkujate kontrollirolli tugevdamist ning tõhusamat reageerimist juba antud ligipääsudele. Teoreetiliselt viitavad need meetmed katsele vähendada e-residentsuse süsteemis avalduvaid informatsioonilisi, regulatiivseid ja jurisdiktsioonilisi asümmeetriaid. Samas ei ole neid asümmeetriaid võimalik täielikult kõrvaldada, sest riskide tuvastamine sõltub jätkuvalt rahvusvahelisest andmevahetusest, erasektori väravahoidjate tegevusest ja sellest, kas riigi järelevalvevõimekus suudab kaasas käia piiriülese digitaalse ettevõtluse tempoga.

4.2.4. Kriminogeensed asümmeetriad ja süsteemsed lõhed

Ekspertintervjuud viitavad, et e-residentsusega seotud riskid tulenevad süsteemsetest teguritest, mitte üksikutest kontrollipuudustest ning on seotud programmi piiriülese toimimisloogikaga. Kuigi PPA, RAB ja MTA käsitlevad riske erinevate institutsionaalsete ülesannete kaudu, kattuvad nende hinnangud selles, et riskide tuvastamine ja maandamine sõltub sageli infost, mis paikneb väljaspool ühe asutuse või ühe jurisdiktsiooni vahetut kontrolli.

Olulise asümmeetriana tõuseb esile informatsiooniline piiratus. PPA hinnangul tugineb taustakontroll suuresti avatud allikatele ja taotleja enda esitatud teabele, mille usaldusväärsus ei ole alati kontrollitav ning mida on võimalik teadlikult kujundada menetluse nõuetele vastavaks. Seda süvendab tehnoloogiline areng, sh tehisintellekti kasutamine taotluste ja

vastuste koostamisel, mis raskendab taotleja tegeliku profiili hindamist. Samal ajal on rahvusvaheliste andmete kättesaadavus piiratud - näiteks puudub haldusmenetluses ligipääs ECRIS-ele, mistõttu võivad varasemad rikkumised jääda tuvastamata. PPA vaates avaldub informatsiooniline asümmeetria seega eeskätt taotleja tausta ja kavandatava tegevuse kontrollimisel.

MTA viitab samale probleemile maksujärelevalve vaates, tuues esile vajaduse saada terviklikumat infot Euroopa tasandil, sh Euroopa äriregistri kaudu ärikeeldude, karistuste, juhatuse liikmete ja osanike kohta. Seega avaldub informatsiooniline piiratus MTA vaates eeskätt selles, kas maksuhalduril on piisav piiriülene info ettevõtte ja sellega seotud isikute tegeliku riskiprofiili hindamiseks.

RAB-i ekspert nägi informatsioonilist piirangut eeskätt finantsinfo liikumises: kui Eesti pangad e-residentide ettevõtteid ei teeninda ja äriühinguteenuse pakkujad ei rakenda sisuliselt hoolsusmeetmeid, ei teki ka RAB-ile piisavalt siseriiklikke riskisignaale. Samuti tõi RAB täiendavalt esile, et töös olev tegelike kasusaajate registri (TEKSA) juurdepääsu piiramine avalikkusele vähendab kättesaadava teabe hulka, mis süvendaks informatsioonilist asümmeetriat veelgi. Kokku näitavad need hinnangud, et informatsiooniline asümmeetria ei avaldu ühes andmelüngas, vaid eri asutuste tööprotsessides erineval kujul.

Informatsioonilist piirangut ei kujunda aga üksnes andmete kättesaadavus, vaid ka nende töötlemise praktilised võimalused. PPA eksperdi hinnangul laekub ühes nädalas keskmiselt 400 e-residentsuse taotlust, mis tuleb sama ajaperioodi jooksul menetleda, mistõttu vaatab üks menetleja päevas läbi keskmiselt 12–15 taotlust. Selline töökoormus ei tähenda iseenesest, et taustakontroll oleks ebapiisav, kuid see viitab praktilisele piirangule: suure taotluste mahu juures on süvitsi minev individuaalne hindamine paratamatult võimalik üksnes valitud juhtumites ning kontroll tugineb eeskätt kättesaadavale ja kiiresti kontrollitavale teabele.

Regulatiivne asümmeetria avaldub e-residentsuse ökosüsteemis eelkõige vahendajate ja riikliku järelevalve vahelises lõhes. Passase käsitluse kohaselt tekivad kriminogeensed asümmeetriad sageli seal, kus legaalsed ja illegaalsed struktuurid põimuvad. Intervjuudest ilmneb, et äriühinguteenuse pakkujad peaksid toimima süsteemi väravahoidjatena, kuid nende rolli nähakse PPA ja RAB-i vaates erinevalt: PPA jaoks avaldub vahendusrisk taotluste ettevalmistamises ja taotlejate juhendamises, RAB-i jaoks aga hoolsusmeetmete ja teatamiskohustuse nõrgas täitmisel. Selline olukord loob regulatiivse ebakõla, kus erasektori vahendajad võimaldavad ligipääsu Eesti ettevõtluskeskkonnale, kuid nende kontrollifunktsioon ei pruugi praktikas vastata neile pandud rollile. Seeläbi võib Eesti legitiimne

ettevõtluskeskkond muutuda vahendiks piiriülestes skeemides, sh maksupettustes ja sanktsioonidest kõrvalehoidumisel.

Jurisdiktsiooniline asümmeetria avaldub e-residentsuse kontekstis olukorras, kus majandustegevus on oma olemuselt piiriülene, kuid järelevalve ja õiguskaitse jäävad riigipõhiseks. Intervjuudest ilmneb, et e-residentide ettevõtted võivad toimida nn „tühjade kehadena“, millel puudub sisuline seos Eesti majanduskeskkonnaga ning mille rahavood liiguvad väljaspool Eesti finantssüsteemi. RAB-i ekspert rõhutas, et välispäringutes võib Eesti seos seisneda üksnes Eestis asutatud juriidilises isikus, samal ajal kui kuritegu ja rahaliste vahendite liikumine toimuvad välisriigis. PPA ekspert kirjeldas sama probleemi kriminaalmenetluse vaates: kui kannatanud, tõendid ja kuriteo toimepanemise koht paiknevad välisriigis, menetleb juhtumit üldjuhul teine riik ning Eesti roll piirdub peamiselt info andmise ja e-residendi staatusega seotud meetmetega. Selline olukord peegeldab Passase kirjeldatud asümmeetriat, kus globaalselt toimivad majandussuhted ei ole kooskõlas territoriaalselt piiratud kontrollimehhanismidega.

Lisaks ilmneb institutsionaalne asümmeetria, kus riskide hindamine ja maandamine on jaotatud mitme asutuse vahel. Kuigi PPA, MTA ja RAB-i vaheline koostöö on igapäevane ja toimiv, kujuneb terviklik riskipilt erinevate infokildude ühendamisel ning sõltub suuresti andmevahetuse kiirusest ja kvaliteedist. Seetõttu ei toimi süsteem ühe keskse kontrollimehhanismina, vaid hajutatud institutsionaalse võrgustikuna, kus riskide nähtavus sõltub sellest, kas eri kontrollipunktides tekkiv info jõuab õigel ajal teiste asutusteni.

Süsteemne lõhe avaldub ka majanduslike eesmärkide ja turvakaalutluste vahelises pinges. RAB-i ekspert viitas riigi riskiisu küsimusele, rõhutades vajadust mõtestada, millistele sihtrühmadele e-residentsust pakutakse, millist majanduslikku kasu programm tegelikult loob ning millist riski on riik valmis selle nimel aktsepteerima. Hardy varjupaigateooria valguses saab seda käsitleda väikeriigi strateegilise avatuse dilemma: institutsionaalse usalduse eksport loob majanduslikke ja poliitilisi võimalusi, kuid võib samal ajal muuta selle usalduse kuritarvitatavaks. Passase käsitluses võib selline pinge muutuda kriminogeenseks olukorras, kus majanduslikud stiimulid ja programmi laiendamise loogika arenevad kiiremini kui regulatiivne ja järelevalveline võimekus. Castelli vaates väljendub sama probleem selles, et riik laiendab oma mõju globaalses digitaalses voogude ruumis, samal ajal kui kontroll jääb territoriaalselt piiratud.

Kokkuvõttes näitavad ekspertintervjuud, et e-residentsusega seotud riskid ei avaldu üksnes eraldiseisvate juhtumitena, vaid korduvate riskimustritena, mille keskmes on piiriülese

majandustegevuse, digitaalse ligipääsu ja territoriaalse järelvalve lahknevus. PPA, RAB-i ja MTA vaated kinnitavad, et riskide maandamine sõltub nii riigiasutuste koostööst, erasektori väravahoidjate tegevusest kui ka rahvusvahelise andmevahetuse toimimisest. Järgmises peatükis seostatakse dokumendianalüüsi ja intervjuude tulemused ühtseks analüütiliseks tervikuks, et hinnata, mil määral vastavad olemasolevad regulatiivsed ja järelvalvemehhanismid e-residentsusega seotud riskide tegelikule olemusele.

5. Analüüs ja tulemused

Käesoleva peatüki eesmärk on liikuda empiirilises analüüsis kirjeldatud riskijuhtumitelt ja mustritelt teoreetilisema ja süsteemsema tõlgenduse suunas, hinnates, millisel määral on olemasolevad regulatiivsed ja järelevalvemehhanismid suutnud neid riske ennetada, tuvastada ja neile reageerida. Analüüs tugineb peatükis neli esitatud empiirilistele leidudele, mille põhjal on võimalik eristada korduvaid mehhanisme, mille kaudu finantskuritegevuse riskid praktikas realiseeruvad.

Selleks on käesolevas peatükis riskid grupeeritud nende realiseerumise mehhanismide alusel, mitte üksikute juhtumite või valdkondade kaupa. Selline lähenemine võimaldab hinnata regulatsioonide toimivust mitte üksnes konkreetsete rikkumiste tasandil, vaid laiemalt selles osas, millistes süsteemi etappides ja struktuurides kontrollimehhanismid toimivad, ebaõnnestuvad või osutuvad ebapiisavaks. Analüüsi lähtub kolmetasandilisest loogikast, mille kohaselt vaadeldakse eraldi riskide ennetamise, tuvastamise ja neile reageerimise mehhanisme, võimaldades hinnata nii regulatiivse raamistiku ülesehitust kui ka selle praktilist rakendamist.

Empiirilise analüüsi põhjal eristuvad kolm peamist riskide realiseerumise mehhanismi, mis on tuletatud Passase kriminogeensete asümmeetriate teooriast:

1. Juriidiline vorm kui „legaalne fassaad“ piiriülestes skeemides, mis peegeldab Passase kirjeldatud legaalse ja illegaalse sfääri liidest. See mehhanism võimaldab integreerida ebaseadusliku tegevuse formaalselt õiguspärasesse majanduskeskkonda, kasutades Eesti usaldusväärset kilbina.
2. Identiteedi ja jurisdiktsiooni kaudu loodud varjatus, mis vastab vastutuse strukturesele hajumisele. Digitaalne identiteet ja piiriülene ettevõtluskeskkond võimaldavad eraldada registris nähtava isiku tegevuse tegelikust kontrollijast või kasusaajast, raskendades nii osapoolte kui ka tegevuse tegeliku asukoha tuvastamist.
3. Professionaalsed vahendajad kui asümmeetriate kujundajad, kes täidavad Passase käsitluses professionaalsete hõlbustajate rolli. Nende tegevus loob ja võimendab kriminogeenseid asümmeetriaid, kujundades keskkonna, kus regulatiivsed lõhed saavad realiseeruda.

Käesolevas peatükis analüüsitakse, mil määral on Eesti ja EL-i regulatiivne raamistik suutnud neid süsteemseid mehhanisme ohjata ning millistes aspektides jääb järelevalvevõimekus alla globaalsete finantsvoogude ja digitaalse ettevõtluskeskkonna arengule.

5.1. Riskide realiseerumine ja regulatiivne vastus

5.1.1. Juriidiline vorm kui „legaalne fassaad“ piiriülestes skeemides

Empiiriline analüüs näitab, et üks keskseid mehhanisme, mille kaudu e-residentsuse kontekstis finantskuritegevuse riskid realiseeruvad, on ettevõtete kasutamine „legaalsete fassaadidena“. Nendes juhtumites ei seisne probleem mitte e-residendi staatuses, vaid selles, kuidas Eestis registreeritud ettevõtte võimaldab anda välisriigis toimuvale tegevusele usaldusväärse juriidilise vormi. See ilmnes nii maksupettuste skeemides, rahapesuga seotud juhtumites, virtuaalvääringu teenuse pakkujate puhul kui ka julgeolekuvaldkonnas, kus KAPO andmetel kasutati Eesti ettevõtteid Venemaa sõjatööstuse tellimuste täitmiseks ja lääne tarnijate eksitamiseks. Neid juhtumeid ühendab asjaolu, et ettevõtted luuakse Eestis, kuid nende tegelik majandustegevus ja rahavood paiknevad väljaspool Eesti jurisdiktsiooni, samal ajal säilitavad nad EL-i õiguskeskkonnaga seotud usaldusmärgid, nagu KMKR number või ligipääs finantsteenustele, mis loovad näilise õiguspärasuse.

Selline mehhanism oli selgelt nähtav nii varifirmade kasutamises piiriülestes maksupettustes kui ka VASP juhtumites, kus ettevõtte juriidiline vorm võimaldas pakkuda teenuseid välisriikides ilma tegeliku seoseta Eesti majandusruumiga. Olulist rolli mängisid seejuures äriühinguteenuse pakkujad, kes loid ja haldasid neid struktuure, võimaldades ettevõtete kiiret ja standardiseeritud loomist. Sellisel juhul ei toimi ettevõtte sisulise majandustegevuse kandjana, vaid vahendina, mille kaudu saavutatakse ligipääs usaldusväärsele õiguskeskkonnale, finantsteenustele või tegevuslubadele.

Regulatiivse vastuse vaates ilmneb, et ennetustasandil on selliste riskide piiramine empiiriliste juhtumite põhjal piiratud tõhususega. Eelkontroll, mida viib läbi PPA e-residendi staatuse andmisel, keskendub isiku tausta ja võimalike riskinäitajate hindamisele. MTA roll ennetuses avaldub eeskätt ettevõtete ja maksukäitumise riskipõhises hindamises, mis tugineb esitatud andmetele ning tuvastatavatele mustritele. Praktikas tähendab see, et kontroll on suunatud eelkõige olemasoleva info ja varasema käitumise hindamisele, kuid võimaldab piiratud ulatuses tuvastada majandustegevuse tegelikku sisu ja selle seotust Eestiga.

Samal ajal lasub ennetuslik roll ka äriühinguteenuse pakkujatel, kes on kohustatud rakendama hoolsusmeetmeid ning koguma teavet klientide ja nende äritegevuse kohta. Empiirilised näited viitavad siiski sellele, et nende roll jääb sageli formaalseks, piirdudes nõutud andmete kogumisega ilma sisulise riskihindamiseta. See vähendab süsteemi ennetavat võimekust, kuna ettevõtte loomise ja haldamise käigus ei hinnata tegelikult, kas kavandatav tegevus vastab esitatud andmetele ja omab sisulist seost Eestiga.

Sisuliselt tuleneb eelkontrolli piiratus sellest, et see on paratamatult seotud infoga, mida isik ise enda kohta avaldab ning millist teavet on võimalik olemasolevatest andmeallikatest kontrollida. Seega saab hinnata ja analüüsida eelkõige isiku varasemat käitumist, mitte seda, millist äritegevust ta reaalselt kavandab või kus see tegelikult toimuma hakkab. Kuigi PPA on täiendanud rahvusvahelisi andmevahetuskanaleid ning liidestanud rohkem andmebaase, ei ole eelkontrollis kasutatavad andmeallikad siiski täielikud ning siiani ei ole kättesaadav teave isiku suhtes kehtestatud ärikeeldude või välisriikides tehtud süüdimõistvate otsuste kohta. Samuti tugineb osa kontrollist avalikult kättesaadavale teabele, mille sisu ja usaldusväärsus võivad olla piiratud, kuna isik saab oma digitaalset jalajälge teadlikult kujundada, eemaldada varasemaid seoseid või luua usaldusväärsust toetava kuvandi näiteks LinkedInis.

Siin mängib olulist rolli ka eelkontrolli praktiline korraldus. Intervjuude põhjal selgus, et üks PPA menetleja vaatab päevas läbi ligikaudu 12–15 e-residentsuse taotlust, mis piirab oluliselt võimalust iga juhtumi sisuliseks analüüsiks ning suunab kontrolli paratamatult pigem kättesaadavale ja kiiresti kontrollitavale teabele.

Sellest tulenevalt on eelkontrolliga keeruline tuvastada olukordi, kus formaalselt korrektse taustaga isik kasutab ettevõtet hiljem üksnes juriidilise vormina piiriülestes skeemides. Eelkontroll võimaldab hinnata eelkõige taotleja tausta, esitatud andmete usaldusväärsust ja teadaolevaid riskinäitajaid, kuid mitte täielikult seda, millist rolli hakkab tema loodav ettevõtte hiljem tegelikus majandustegevuses täitma. Passase käsitluses peegeldab see informatsioonilist asümmeetriat: riik teeb otsuse selle teabe põhjal, mis on menetluse ajal kättesaadav ja kontrollitav, samal ajal kui ettevõtte tegelik kasutus võib avalduda alles hiljem ning teistes jurisdiktsioonides.

Tuvastamise etapis muutub juriidilise vormi kui „legaalse fassaadi“ mehhanism Eesti järelevalve jaoks eriti problemaatiliseks. Kui ettevõtte on juba süsteemi sisenenud ja omandanud formaalsed usaldusmärgid, nagu Eesti juriidiline vorm, KMKR number või ligipääs finantsteenustele, võib selle tegelik roll piiriüleses skeemis jääda Eesti registri- ja järelevalveinfos varjatuks.

Tuvastamise mehhanism toimib seetõttu valdavalt reaktiivselt ning sõltub suurel määral välisriikidest laekuvast teabest. Seda kinnitab asjaolu, et 53% e-residentide kohta RAB-ile tehtud rahapesukahtlusega teadetest pärineb välisriikidest ning 23,4% kõigist välisriikide ametiasutustelt Eestile laekunud sisulistest rahapesukahtlusega päringutest on seotud e-residentide või nende ettevõtetega. Ka RAB-i eksperdi hinnangul jõuab oluline osa riskiteabest

Eesti asutusteni alles välipäringute kaudu, mis tähendab, et rikkumine muutub Eesti jaoks nähtavaks sageli alles pärast selle tuvastamist mõnes teises jurisdiktsioonis.

See peegeldab informatsioonilist asümmeetriat, mille puhul Eesti järelevalveasutuste riskipilt sõltub suuresti sellest, milline teave jõuab nendeni teiste riikide asutuste, kohustatud isikute või rahvusvaheliste koostöökanalite kaudu. Seetõttu võib risk muutuda nähtavaks alles siis, kui kahtlane tegevus on tuvastatud mõnes teises jurisdiktsioonis. Passase käsitles ei seisne probleem siin üksnes teabe puudulikkuses, vaid selles, et legaalne juriidiline vorm võimaldab hoida ettevõtte välise kuvandi ja tegeliku majandusliku sisu lahus. Nii võib ettevõtte registriandmete järgi näida korrektne, kuigi selle tegelik roll piiriüleses skeemis avaldub Eesti jaoks alles hilinenult ja vahendatud info kaudu.

Kuigi PPA, MTA, RAB-i ja KAPO vaheline koostöö on ekspertide hinnangul operatiivne, sõltub terviklik riskipilt erinevate andmekildude ühendamisest, mis ei ole alati süsteemselt integreeritud. PPA saab teistelt asutustelt sisendit maksukäitumise, rahapesuriskide ja julgeolekuohtude kohta, kuid see ei tähenda, et riigil oleks ühene ja vahetu ülevaade e-residendi tegelikust piiriülesest tegevusest. Näiteks võib teave tehingute kohta paikneda ühes jurisdiktsioonis, tegelik kasusaaja teises ja juriidiline keha Eestis. Sama killustatus avaldub ka kohustatud isikute tasandil. Äriühinguteenuse pakkujad, kellel on kohustus tuvastada kahtlasi tegevusmustreid ja teavitada RAB-i, on praktikas madala teatamisaktiivsusega, mistõttu oluline osa riskiteabest järelevalveasutusteni ei jõua.

Seega näitab tuvastamise etapi analüüs, et kui juriidiline vorm on juba „fassaadina“ kasutusse võetud, muutub selle sisuline läbivalgustamine Eesti tasandil väga keeruliseks. Riiklik järelevalve toimib territoriaalses ja registripõhises paikade ruumis, samas kui rahavood, tegelikud kasusaajad ja kuritegelik tegevus liiguvad piiriüleses voogude ruumis. Tulemuseks on olukord, kus juriidiline vorm ei ole üksnes neutraalne ettevõtlusvahend, vaid võib toimida varjava kihina, mis raskendab tegevuse tegeliku majandusliku sisu, mitte üksnes selle toimumise asukoha tuvastamist.

Reageerimise etapis avaldub juriidilise vormi kui „legaalse fassaadi“ piirang eeskätt selles, et Eesti saab sageli sekkuda vaid oma pädevuse ulatuses. Kui risk on juba tuvastatud, seisneb Eesti tasandi reaktsioon eelkõige halduslikes meetmetes, nagu e-residendi digi-ID kehtetuks tunnistamine, tegevuslubade tühistamine või maksualaste kontrollimeetmete rakendamine. Need meetmed võimaldavad piirata Eesti digitaalse ja ettevõtluskeskkonna edasist kasutamist, kuid ei anna Eestile alati võimalust mõjutada kogu piiriülese skeemi edasist menetlemist.

Siseriiklike kriminaalmenetluste vähesus ei tähenda seetõttu tingimata riskide puudumist, vaid peegeldab nende piiriülest iseloomu. Empiirilised andmed näitavad, et e-residentidega seotud juhtumites paiknevad kuriteo toimepanemise koht, kannatanud, tõendid ja rahavood enamasti väljaspool Eestit. Sellisel juhul toimub põhiline menetlus tavaliselt selles riigis, kus kahju tekkis. Eesti rolliks jääb sellistes olukordades rahvusvahelisele õigusabile vastamine, teabe edastamine, e-residendi staatusega seotud haldusmeetmete rakendamine ning vajaduse korral ettevõtte või tegevusloa kaudu antud legitiimsuse lõpetamine.

See näitab, et reageerimine on e-residentsuse kontekstis sageli tagajärgede piiramine, mitte kogu skeemi vahetu lõpetamine Eesti tasandil. Passase käsitluses peegeldab see jurisdiktsioonilist ja institutsionaalset asümmeetriat: juriidiline keha asub Eestis, kuid selle kaudu toime pandud või võimaldatud tegevuse tegelik kontroll, kahju ja menetluslik raskuskese võivad paikneda teistes jurisdiktsioonides. Seetõttu saab Eesti küll eemaldada süsteemist riskantse digitaalse identiteedi või juriidilise vormi, kuid sõltub kuritegeliku tegevuse sisuliseks menetlemiseks rahvusvahelisest koostööst ja välisriikide menetlusvõimekusest.

Reageerimise tõhusus sõltub seega sellest, kui kiiresti jõuab riskiteave Eesti asutusteni ning kui hästi on võimalik siduda halduslikud meetmed rahvusvahelise õiguskaitsekoostööga. Kui info liigub hilinevalt või killustatult, võib Eesti reaktsioon piirduda juba toimunud väärkasutuse lõpetamisega, samal ajal kui kahju hüvitamine, vara jälitamine või süüteo tõendamine jääb teise riigi menetluse kanda. See kinnitab, et juriidilise fassaadi kasutamise puhul ei ole probleem üksnes õigusliku vormi kuritarvitamises, vaid ka selles, et reageerimisvõimekus on jagatud mitme riigi ja institutsiooni vahel.

5.1.2. Identiteedi ja jurisdiktsiooni kaudu loodud varjatus

Selle mehhanismi keskmes ei ole enam niivõrd Eesti ettevõtte vormiline usaldusväärsus, vaid digitaalse identiteedi, tegeliku kontrolli ja tegevuse asukoha lahknemine. E-residentsus loob riiklikult kinnitatud digitaalse identiteedi, kuid see ei tähenda, et järelevalveasutustel oleks vahetu ülevaade sellest, kes ettevõtte tegevust tegelikult juhib, kus tegevus toimub või millistes jurisdiktsioonides avaldub selle majanduslik mõju.

Identiteedi ja jurisdiktsiooni kaudu loodud varjatus väljendub seega olukorras, kus formaalselt tuvastatud isik ja registrites nähtav seos ei anna piisavat teavet tegevuse tegeliku kontrolli, kasusaajate ega riskiprofiili kohta. Selline lahknemine loob Passase käsitluses vastutuse

struktuurse hajumise: õiguslik seos Eestiga on olemas, kuid tegevuse sisuline raskus paikneb sageli väljaspool Eesti vahetut kontrolliruumi.

Ennetustasandil on keskseks mehhanismiks PPA poolt teostatav e-residendi staatuse taotlemise eelkontroll, mille eesmärk on filtreerida välja isikud, kes võivad kujutada ohtu avalikule korrale või riigi julgeolekule. Empiiriline analüüs näitab, et viimastel aastatel on eelkontroll muutunud rangemaks (negatiivsete otsuste osakaal on kasvanud 2%-lt 10,9%-le), süsteemi on täiendatud andmepõhise automatiseeritud järelkontrolliga ning toetatud saatkondades toimuva isikusamasuse kontrolliga. Kuigi täienenud meetmed vähendavad ilmsete riskijuhtumite süsteemi sisenemist, keskendub eelkontroll peamiselt isiku formaalsele identiteedile ja registriandmetele ega võimalda hinnata isiku tegelikke seoseid.

Siin avaldub Passase kirjeldatud informatsiooniline ja jurisdiktsiooniline asümmeetria. Kuna e-residendi staatuse andmine toimub haldusmenetluse korras, puudub PPA-l õiguslik alus teha päringuid ECRIS-e süsteemi, mistõttu ei ole EL-i tasandi andmevahetus ennetusfaasis täiel määral rakendatav. Selle tulemusena võivad teistes liikmesriikides kriminaalkorras karistatud isikud jääda eelkontrollis nähtamatuks. Sama loogika ilmneb kolmandate riikide puhul, kus koostöömehhanismide puudumisel tugineb taustakontroll piiratud ja ebaühtlase kvaliteediga teabele. Ka identiteedi seaduslik muutmine võib katkestada seose varasema riskiteabega, võimaldades varjatust õiguspäraste mehhanismide kaudu. Nii kujuneb olukord, kus formaalne identiteet on olemas, kuid selle taga olev tegelik taust jääb osaliselt läbipaistmatuks - just sellised legaalse ja illegaalse kasutuse vahele tekkivad ebakõlad loovad Passase käsitluses kriminogeenseid võimalusi.

Seda piirangut võimendab Castellsi kirjeldatud pinge paikade ruumi ja voogude ruumi vahel. Eelkontroll tugineb territoriaalse riigi loogikale ja registripõhisele teabele, samas kui identiteet, ettevõtlus ja riskiseosed liiguvad piiriüleselt võrgustikulises ruumis. Seetõttu on riigi kontroll tugevam lokaalselt registreeritava teabe üle, kuid piiratum hajutatud ja piiriüleste seoste osas, mistõttu võib formaalselt korrektne identiteet jääda sisulise riskihinnangu seisukohalt puudulikuks.

Eelkontrolli toimivust mõjutab ka selle praktiline korraldus. Nagu eelnevalt käsitletud, suunab suur taotluste maht kontrolli eeskätt standardiseeritud ja kiiresti kontrollitavale teabele. Identiteedi ja jurisdiktsiooni kaudu loodud varjatuse puhul tähendab see, et keerukamad seosed, mis ei avaldu registriandmetes, võivad jääda tuvastamata.

Tehnoloogiline areng süvendab seda piirangut. Tehisintellekti ja süvavõltsingute levik suurendab riski, et esitatud andmed, dokumendid või digitaalne kuvand näivad usutavad, kuid ei pruugi anda piisavat kindlust isiku tegeliku tausta ja kavatsuste kohta. Seega ei tulene ennetuse piiratus üksnes info puudumisest, vaid ka sellest, et kättesaadava info usaldusväärsust on üha keerulisem hinnata.

Sellest tulenevalt näitab analüüs, et identiteedi ja jurisdiktsiooni kaudu loodud varjatuse ennetamisel ei seisne keskne probleem üksnes informatsiooni puudumises, vaid piiratud võimekuses siduda olemasolev info konkreetse isiku, tema seoste ja tegeliku tegevusega. Selle tulemusena hajub vastutus mitme jurisdiktsiooni vahel ning Passase käsitluses väljendub see vastutuse struktuurses hajumises, kus isegi tuvastatud tegevuse puhul ei ole üheselt selge, kes seda tegelikult kontrollib või juhib.

Tuvastamise etapp toob kõige selgemalt esile e-residentsuse süsteemi struktuursed piirangud, mis tulenevad digitaalse identiteedi, territoriaalse järelevalve ja piiriülese majandustegevuse lahknevusest. Empiiriline analüüs näitab, et kuigi formaalne isikusamasus on e-residentsuse raames kõrgel tasemel kontrollitud, jääb tegeliku tegevuse, asukoha ja riskiprofiili muutuste tuvastamine märkimisväärselt piiratuks.

Tuvastamise mehhanismi reaktiivset ja välipäringutest sõltuvat iseloomu on käsitletud eelmises alapeatükis, kuid identiteedi ja jurisdiktsiooni kaudu loodud varjatuse kontekstis avaldub see eeskätt raskusena siduda tuvastatud tegevus konkreetse isikuga. Välisriikidest laekuv info võib küll viidata kahtlasele tegevusele, kuid ei pruugi võimaldada selgelt tuvastada, kes on selle tegelik korraldaja, kasusaaja või otsustaja, mistõttu jääb vastutuse omistamine ka olemasoleva info põhjal piiratud.

Tuvastamise etapis on toimunud nihe ühekordselt eelkontrollilt pidevale seirele: alates 2022. aastast rakendatav PPA automaatne järelkontroll jälgib e-residentidega seotud riskisignaale Eesti ja EL-i andmekogudes. See vastab riskipõhise regulatsiooni loogikale, kus hinnang ei piirdu taotluse hetkega. Samas jääb mehhanism sõltuvaks andmete kättesaadavusest: kui tehingud toimuvad välisriigi makseteenuse pakkuja juures või väljaspool EL-i, ei pruugi riskisignaal Eesti süsteemidesse jõuda. Seega suurendab dünaamiline seire küll tuvastamise ajakohasust, kuid ei kõrvalda informatsioonilist asümmeetriat.

Tuvastamist piirab digitaalse identiteedi ja tegeliku tegevusruumi lahknevus. Castelli voogude ruumi kontekstis tegutsevad järelevalveasutused territoriaalses paikade ruumis, kuid kontrollitav tegevus on hajutatud võrgustikus. Praktikas tähendab see, et isegi formaalselt

korrektnel identiteet (nt ettevõte Eestis, KMKR olemasolu) ei võimalda hinnata, kus tehingud tegelikult toimuvad või kes neid juhib, mistõttu jääb sisuline riskihinnang piiratud.

Seega ei seisne tuvastamise probleem üksnes selles, kas isik on formaalselt tuvastatud, vaid selles, kas tema tegelik roll piiriülese tegevusahelas on nähtav. Passase käsitlel toimub siin vastutuse struktuurne hajumine: tegevus võib olla seotud Eesti digi-ID ja ettevõttega, kuid selle tegelik korraldaja, lõplik kasusaaja või otsustaja ei ole vahetult tuvastatav.

Reageerimise etapis avaldub identiteedi ja jurisdiktsiooni kaudu loodud varjatuse piirang selles, et Eesti saab sekkuda eelkõige siis, kui risk on juba tuvastatud ning seos konkreetse isiku või ettevõttega on piisavalt selge. Sellisel juhul seisneb Eesti tasandi reaktsioon peamiselt ligipääsu lõpetamises või piiramises, näiteks e-residendi digi-ID kehtetuks tunnistamises, ettevõttega seotud kontrollimeetmete rakendamises või julgeolekuriski korral sissesõidukeelu kehtestamises. Need meetmed võimaldavad katkestada isiku edasise ligipääsu Eesti digitaalsele ja ettevõtluskeskkonnale, kuid ei pruugi iseenesest lahendada piiriülese tegevuse sisulist menetlemist.

Empiirilised juhtumid näitavad, et reageerimine võib olla kiire ja otsustav juhul, kui riskiteave on Eesti asutustele kättesaadav ning isik on selgelt tuvastatav. Näiteks julgeolekuriskide puhul on KAPO ettepaneku alusel võimalik e-residendi staatus kehtetuks tunnistada ning vajaduse korral kehtestada isikule sissesõidukeeld. VASP-sektori puhul näitab riigi reaktsioon aga, et riskide maandamine eeldas õigusraamistiku tugevdamist. Kui teenusepakkujatele kehtestati rangemad nõuded, sai riik selgemalt hinnata, kas ettevõtte on tegelik seos Eestiga ja kas ta vastab rahapesu tõkestamise nõuetele. Sellised meetmed näitavad, et Eesti reageerimisvõimekus on tugevam siis, kui risk on seotud konkreetse staatuse, loa või Eesti õiguskeskkonna kaudu antud ligipääsuga ning kui õigusraamistik annab selle ligipääsu lõpetamiseks selge aluse.

Samas on reageerimine piiratum juhul, kui tuvastatud risk ei ole selgelt seostatav konkreetse isiku tegeliku rolli või kontrolliga. Sellisel juhul ei piisa üksnes formaalse identiteedi olemasolust, vaid vajalik on välisriikidest saadav lisateave, mis võimaldaks hinnata isiku tegelikku seotust kahtlase tegevusega. Passase käsitlel peegeldab see taaskord vastutuse struktuurset hajumist.

Seega on reageerimine identiteedi ja jurisdiktsiooni kaudu loodud varjatuse puhul eeskätt riskantse ligipääsu lõpetamine, mitte alati kogu piiriülese tegevusahela läbivalgustamine. Reageerimise tõhusus sõltub sellest, kas digitaalne identiteet on võimalik siduda konkreetse

isiku, tema tegeliku tegevuse ja vastutusega. Kui see seos jääb ebaselgeks või sõltub välisriigis paiknevast teabest, piirab see Eesti võimalust reageerida sisuliselt, mitte ainult halduslikult.

5.1.3. Professionaalsed vahendajad kui asümmeetriate kujundajad

Kolmanda mehhanismina ilmneb e-residentsuse süsteemis professionaalsete vahendajate keskne roll. Kui juriidilise vormi kaudu loodud „legaalne fassaad“ puudutab eelkõige Eesti ettevõtte kasutamist piiriülestes skeemides ning identiteedi ja jurisdiktsiooni kaudu loodud varjatus isiku tegeliku rolli ja asukoha hägustumist, siis vahendajate puhul seisneb risk selles, et just nemad muudavad need võimalused praktikas kasutatavaks. Äriühinguteenuse pakkujad, kontaktisikuteenuse osutajad, raamatupidajad ja nõustajad täidavad e-residentsuse ökosüsteemis vahendavat rolli, aidates e-residentidel luua ettevõtteid, täita vorminõudeid, taotleda käibemaksukohustuslasena registreerimist või tegevuslubasid ning hallata ettevõtte igapäevast toimimist.

Empiiriline analüüs näitab, et vahendajate roll ei ole e-residentsuse kontekstis kõrvaline, vaid süsteemi toimimise seisukohalt keskne. E-residentidele pakutakse sageli terviklahendusi, mis hõlmavad e-residentsuse taotlemist, ettevõtte asutamist, kontaktisikuteenust, raamatupidamist ja vajaduse korral ka KMKR-i või tegevusloa taotlemist. VASP-sektori puhul ilmnes eriti selgelt, kuidas äriühinguteenuse pakkujad aitasid massiliselt luua ettevõtteid, hankida neile tegevuslubasid ning müüa neid edasi välisriikidest pärit klientidele. Seega ei kujunda vahendajad üksnes tehnilist ligipääsu Eesti ettevõtluskeskkonnale, vaid võivad mõjutada ka seda, kui sisuliseks või formaalseks jääb riskikontroll süsteemi sisenemisel.

Ennetustasandil on vahendajatele antud oluline väravahoidja roll. Rahapesu tõkestamise raamistik eeldab, et äriühinguteenuse pakkujad rakendavad hoolsusmeetmeid, tunnevad oma kliente, hindavad nende äritegevuse eesmärki ja tuvastavad vajaduse korral kahtlased asjaolud. Sellise mudeli loogika seisneb selles, et riik ei saa kõiki e-residentide ja nende ettevõtetega seotud riske vahetult kontrollida, mistõttu osa ennetavast kontrollist on delegeeritud erasektori kohustatud isikutele. Vahendajad peaksid seega toimima esmase filtrina, kes märkavad riske enne, kui ettevõtteid kasutatakse piiriülestes skeemides.

Empiirilised leiud viitavad siiski sellele, et see ennetav roll ei toimi alati sisuliselt. Probleem ei seisne üksnes selles, et vahendajad jätavad üksikjuhtudel kohustusi täitmata, vaid selles, et nende majanduslik huvi on sageli seotud teenuste müügi ja klientide teenindamisega. See võib tekitada regulatiivse asümmeetria riigi ootuse ja vahendajate tegeliku stiimuli vahel: riik eeldab

riskikontrolli, samas kui teenusepakkuja ärimudel võib soosida võimalikult kiiret ja standardiseeritud ettevõtete loomist. Sellises olukorras võib hoolsusmeetmete rakendamine jääda formaalseks ning keskenduda nõutud andmete kogumisele, mitte kliendi tegeliku tegevuse ja riskiprofiili sisulisele hindamisele.

Tuvastamise etapis avaldub vahendajate roll eeskätt kahtlaste tegevusmustrite märkamises ja RAB-ile teatamises. Kuna vahendajad puutuvad sageli kokku kliendi ettevõtte loomise, haldamise, dokumentatsiooni ja majandustegevuse vormilise poolega, peaksid nad olema positsioonis, kus riskisignaale on võimalik märgata varajases etapis. Praktikas on nende teatamisaktiivsus aga madal, mistõttu oluline osa võimalikust riskiteabest ei jõua järelevalveasutusteni. See nõrgestab süsteemi tuvastamisvõimekust, sest riigi riskipilt sõltub osaliselt infost, mida erasektori väravahoidjad kas edastavad või jätavad edastamata.

Siin ilmneb Passase käsitlusega hästi haakuv süsteemne sünergia. Kui ettevõtte loomine, kontaktisikuteenus, raamatupidamine või tegevusloa taotlemine muutub standardiseeritud paketiks, võib see aidata anda piiriülesele tegevusele õiguspärase vormi ka siis, kui ettevõttel puudub tegelik seos Eestiga. Sellisel juhul saavad legaalsed osapooled kasu teenuste müügist, samal ajal kui nende loodud struktuure võidakse kasutada finantskuritegevuse, maksupettuste või sanktsioonidest kõrvalehoidmise toetamiseks. Passase mõttes ei tähenda see tingimata, et vahendajad osalevad teadlikult kuritegelikus tegevuses, vaid seda, et legaalne teenuseturg ja kuritegelikud võimalused võivad toimida vastastikku tugevdava süsteemina.

Reageerimise etapis seisneb riigi võimalus eelkõige vahendajate järelevalve tugevdamises, tegevuslubade kontrollis ning nõuete rikkumise korral tegevusloa kehtetuks tunnistamises. VASP-sektori kogemus näitab, et kui varasem raamistik võimaldas turule siseneda paljudel nõrga Eesti seosega ettevõtetel, tuli reageerimiseks tugevdada õigusraamistikku ja muuta nõudeid rangemaks. See ei puudutanud üksnes virtuaalvääringu teenusepakkujaid, vaid tõi laiemalt esile ka vahendajate rolli ettevõtete loomisel, tegevuslubade taotlemisel ja formaalse vastavuse kujundamisel. Kui teenusepakkujatele ja nende klientidele kehtestati selgemad nõuded, sai riik paremini hinnata, kas tegevusel on tegelik seos Eestiga ning kas kohustatud isikud täidavad rahapesu tõkestamise nõudeid sisuliselt.

Samas on reageerimine piiratud juhul, kui vahendaja roll jääb formaalselt õiguspärase teenuse osutamise tasandile. Kui teenusepakkuja on kogunud nõutud andmed ja täitnud minimaalsed vorminõuded, kuid ei ole sisuliselt hinnanud kliendi tegevuse eesmärki, võib rikkumise või hooletuse tõendamine olla keeruline. See näitab, et vahendajate puhul ei ole probleem üksnes regulatsiooni olemasolus, vaid selle praktilises rakendamises ja järelevalves. Väravahoidja roll

muutub tõhusaks alles siis, kui hoolsusmeetmed ei piirdu formaalse kontrolliga, vaid võimaldavad tegelikult tuvastada kliendi tegevuse sisu, seose Eestiga ja võimalikud riskimustrid.

Seega näitab professionaalsete vahendajate analüüs, et e-residentsuse süsteemi riskid ei kujune üksnes riigi ja e-residendi vahelises suhtes. Oluline osa riskidest tekib erasektori vahendajate kaudu, kes muudavad Eesti ettevõtluskeskkonna rahvusvahelistele klientidele praktiliselt kasutatavaks. Passase käsitluses toimivad nad legaalse ja illegaalse sfääri liidesena ning süsteemse sünergia kandjatena: nad võivad pakkuda täiesti seaduslikke teenuseid, kuid nende teenuste standardiseeritud ja formaalne kasutamine võib võimendada informatsioonilisi, regulatiivseid ja institutsionaalseid asümmeetriaid. Seetõttu sõltub e-residentsusega seotud riskide maandamine olulisel määral sellest, kas vahendajad täidavad oma väravahoidja rolli sisuliselt või jäävad osaks mehhanismist, mis võimaldab juriidiliste fassaadide loomist ja piiriüleste riskide varjamist.

Kokkuvõttes näitab kolme mehhanismi analüüs, et e-residentsusega seotud finantskuritegevuse riskid ei realiseeru ühe kindla süüteoliigi või üksikjuhtumi kaudu, vaid korduvate struktuursete mehhanismidena. Juriidiline vorm loob piiriülestele skeemidele usaldusväärse välise kuju, digitaalne identiteet ja jurisdiktsiooniline distants raskendavad tegeliku kontrolli ja vastutuse tuvastamist ning professionaalsed vahendajad muudavad need võimalused praktikas kasutatavaks. Olemasolevad regulatiivsed ja järelevalvemehhanismid võimaldavad riske osaliselt ennetada, tuvastada ja neile reageerida, kuid nende tõhusust piiravad informatsioonilised, regulatiivsed, jurisdiktsioonilised ja institutsionaalsed asümmeetriad. Seetõttu ei seisne süsteemi keskne piirang üksnes konkreetsete kontrollimeetmete puudulikkuses, vaid selles, et piiriülene digitaalne tegevuskeskkond liigub kiiremini kui territoriaalselt korraldatud järelevalve.

5.2. Regulatiivse süsteemi toimivus ja struktuursed piirangud

Eelnev mehhanismipõhine analüüs näitab, et e-residentsusega seotud riskide maandamiseks loodud regulatiivne ja järelevalveraamistik toimib eelkõige tingimuslikult. Süsteem töötab paremini olukordades, kus risk on seotud konkreetse isiku, staatuse, loa või Eestis nähtava ettevõttega. Selle piirid avalduvad aga juhtudel, kus tegelik tegevus, kontroll, rahavood või kahju paiknevad väljaspool Eesti vahetat jurisdiktsiooni. Seetõttu ei sõltu regulatiivse süsteemi tõhusus üksnes sellest, kas kontrollimehhanismid on olemas, vaid sellest, kas piiriülene risk muutub Eesti jaoks õigel ajal nähtavaks ja sekkumiseks piisavalt selgelt seostatavaks.

Kolmetasandilise mudeli vaates on kõige tugevamalt arenenud ennetuslik mõõde. PPA eelkontroll on muutunud rangemaks, negatiivsete otsuste osakaal on kasvanud ning süsteemi on täiendatud automaatse järelkontrolli ja asutuste vahelise riskiteabe kasutamisega. Samuti osalevad riskide ennetamises lisaks PPA-le ka MTA, RAB, KAPO ning erasektori kohustatud isikud. Samas jääb ennetuse piiriks see, et otsused tehakse menetluse ajal kättesaadava teabe põhjal. Kui info isiku varasema tausta, ärikeeldude, tegelike seoste või kavandatava tegevuse kohta paikneb välisriigis või ei ole haldusmenetluses kasutatav, ei saa eelkontroll täielikult hinnata hilisemat riskikäitumist. Seetõttu on ennetus küll tugevnenud, kuid jääb teatud juhtudel sõltuvaks formaalsetest ja standardiseeritud andmetest.

Tuvastamise etapis avaldub süsteemi peamine piirang selles, et e-residentsusega seotud riskid muutuvad Eesti jaoks sageli nähtavaks alles välisriikide päringute, rahapesukahtlusega teadete või rahvusvahelise õiguskaitsekoostöö kaudu. See ei tähenda, et Eesti asutustel puuduks tuvastamisvõimekus, vaid et riskide esmased jäljed ei pruugi paikneda Eesti andmeväljades. Kui ettevõtte pangakonto, kliendid, rahavood või tegelik juhtimine asuvad teistes jurisdiktsioonides, sõltub Eesti riskipilt sellest, kas ja kui kiiresti jõuab asjakohane teave välisriikidest või kohustatud isikutelt Eesti asutusteni.

Reageerimise puhul ilmneb sarnane piiratus. Eesti saab riskide realiseerumisel rakendada halduslikke ja järelevalvelisi meetmeid, näiteks tunnistada e-residendi digi-ID kehtetuks, piirata ligipääsu Eesti ettevõtluskeskkonnale, algatada maksualaseid kontrollimeetmeid või tühistada tegevusloa. Need meetmed võimaldavad lõpetada Eesti süsteemi edasise kasutamise riskantse isiku või ettevõtte poolt. Samas ei tähenda see alati kogu piiriülese skeemi sisulist menetlemist Eestis. Kui kannatanud, tõendid ja kuritegeliku tegevuse raskuskese paiknevad välisriigis, jääb Eesti roll sageli koostöö-, infoedastus- või haldusmeetmete rakendamise tasandile.

Sellest tulenevalt võib öelda, et ennetamise, tuvastamise ja reageerimise etapid ei ole omavahel täielikus tasakaalus. Ennetus on muutunud rangemaks, kuid sõltub piiratud andmetest; tuvastamine on olemas, kuid sageli hilineb ja välipäringutest sõltuv; reageerimine on operatiivne seal, kus Eesti saab sulgeda ligipääsu oma süsteemile, kuid piiratum seal, kus sisuline menetlus toimub teises jurisdiktsioonis. Seega ei seisne probleem üksikute meetmete puudumises, vaid selles, et piiriülene digitaalne tegevuskeskkond hajutab riskid mitme riigi, institutsiooni ja erasektori osapoole vahel.

Teoreetiliselt väljendub see Passase kirjeldatud kriminogeensetes asümmeetriates. Informatsiooniline asümmeetria avaldub selles, et vajalik teave isiku, ettevõtte, rahavoogude või tegelike kasusaajate kohta ei ole Eesti asutustele alati kättesaadav. Jurisdiktsiooniline

asümmeetria tekib siis, kui Eesti annab digitaalse identiteedi või juriidilise vormi, kuid tegevus ja kahju realiseeruvad mujal. Institutsionaalne asümmeetria seisneb vastutuse ja kontrolli jagunemises PPA, MTA, RAB-i, KAPO, EL-i koostöömehhanismide ja erasektori vahendajate vahel. Regulatiivne asümmeetria ilmneb eriti selgelt vahendajate puhul, kellelt riik eeldab sisulist hoolsust ja riskiteabe edastamist, kuid kelle majanduslik huvi võib olla seotud teenuste kiire ja standardiseeritud pakkumisega.

Neid asümmeetriaid ühendab Castellsi käsitluses paikade ruumi ja voogude ruumi lahknevus. E-residentsuse regulatiivne paradoks seisneb selles, et Eesti ekspordib digitaalset ligipääsu ja institutsionaalset usaldust piiriülesesse voogude ruumi, kuid järelevalve, menetlus ja vastutus toimivad endiselt valdavalt territoriaalses paikade ruumis. Registrid, haldusmenetlused ja asutuste pädevused on seotud Eesti jurisdiktsiooniga, samal ajal kui e-residentide ettevõtlus, makselahendused, kliendid ja rahavood võivad paikneda mitmes riigis. Seetõttu ei ole kontrolli objekt alati tervikuna Eesti kontrolliruumis.

Kokkuvõttes näitab regulatiivse süsteemi toimivuse analüüs, et e-residentsusega seotud riskide maandamine sõltub vähem üksikute kontrollimehhanismide olemasolust ja rohkem nende võimest ületada piiriülese digitaalse keskkonna struktuurseid asümmeetriaid. Süsteem toimib paremini seal, kus risk on andmetes nähtav, institutsionaalselt seostatav ja Eesti pädevuses käsitletav. Selle piirid avalduvad aga olukordades, kus risk liigub vahendajate, välisriikide makseteenuste, tegelike kasusaajate ja rahvusvaheliste tehinguahelate kaudu väljaspool Eesti vahetut kontrolli. Seetõttu ei ole keskne küsimus üksnes selles, kas regulatsioon on olemas, vaid selles, kas see suudab piiriüleses voogude ruumis tekkivad riskid piisavalt kiiresti ja sisuliselt nähtavaks teha.

Kokkuvõte

Käesoleva magistritöö uurimisprobleem lähtus asjaolust, et e-residentsus on loonud piiriülese digitaalse majandus- ja regulatiivse keskkonna, kus finantskuritegevuse riskide avaldumine ja maandamine ei piirdu ühe riigi tasandiga. E-residentsuse kaudu loodud ettevõtted võivad tegutseda mitmes jurisdiktsioonis, samal ajal kui nende juriidiline vorm, digitaalne identiteet ja osa järelevalvemehhanisme paiknevad Eestis. Selline struktuur tõstatab küsimuse, kas olemasolevad Eesti ja EL-i regulatiivsed ning järelevalvemehhanismid vastavad nende riskide tegelikule olemusele.

Töö eesmärk oli seostada empiiriliselt tuvastatud e-residentsusega seotud finantskuritegevuse riskimustrid ja institutsionaalsed praktikad kriminogeensete asümmeetriate teooriaga, et hinnata, millised struktuursed tegurid piiravad riskide ennetamist, tuvastamist ja neile reageerimist piiriüleses digitaalses keskkonnas. Sellest tulenevalt otsiti töös vastust kahele uurimisküsimusele: miks ja kuidas realiseeruvad e-residentsusega seotud finantskuritegevuse riskid kriminogeensete asümmeetriate kontekstis ning milliste regulatiivsete ja järelevalvemehhanismide kaudu neid riske Eesti ja EL-i raamistikus maandatakse.

Teoreetiliselt tugines töö eelkõige Passase kriminogeensete asümmeetriate käsitlemisele, mille abil selgitati, kuidas informatsioonilised, regulatiivsed, jurisdiktsioonilised ja institutsionaalsed ebakõlad võivad soodustada piiriülest kuritegevust. Seda täiendati Castelli võrgustikuühiskonna käsitlemisega, mis võimaldas mõtestada digitaalse ja piiriülese majandustegevuse ning territoriaalselt korraldatud järelevalve vahelist pinget. Regulatiivsete ja järelevalvemehhanismide toimivuse hindamisel kasutati ennetamise, tuvastamise ja reageerimise kolmetasandilist mudelit. Metoodiliselt põhines töö kvalitatiivsel uurimisstrateegial, ühendades dokumendianalüüsi ja poolstruktureeritud ekspertintervjuud PPA, RAB-i ja MTA ekspertidega.

Töö esimesele uurimisküsimusele vastates näitas analüüs, et e-residentsusega seotud finantskuritegevuse riskid realiseeruvad eeskätt piiriüleste struktuursete mehhanismide kaudu, mitte e-residendi staatuse kui sellise tõttu. E-residentsus ei loo finantskuritegevust iseenesest, kuid see võib pakkuda legaalseid vahendeid, mida kasutatakse piiriülestes skeemides tegevuse tegeliku sisu, kontrolli või kasusaajate varjamiseks. Empiirilises analüüsis ilmnesis riskid maksupettuste, rahapesu, VASP-sektori, sanktsioonidest kõrvalehoidmise, mittetulundussektori ning identiteedi- ja julgeolekuriskide kaudu. Neid juhtumeid ühendab asjaolu, et Eesti digitaalne identiteet, ettevõtte juriidiline vorm või tegevusluba võivad anda piiriülesele

tegevusele formaalse usaldusväärsuse, samal ajal kui tegelik majandustegevus, rahavood või kahju paiknevad teistes jurisdiktsioonides.

Analüüsi põhjal eristus kolm peamist riskide realiseerumise mehhanismi. Esiteks toimib Eesti ettevõtte juriidiline vorm teatud juhtudel „legaalse fassaadina“, mis annab välisriigis toimuvale tegevusele usaldusväärse EL-i õiguskeskkonnaga seotud vormi. See ilmnes nii käibemaksupettustes, rahapesuga seotud juhtumites, VASP-sektoris kui ka sanktsioonidest kõrvalehoidmise skeemides. Teiseks loob digitaalne identiteet koos jurisdiktsioonilise distantsiga varjatuse, kus formaalselt tuvastatud isikut või ettevõtet on keeruline siduda tegeliku tegevuse, kontrolli ja vastutusega. Kolmandaks mängivad keskset rolli professionaalsed vahendajad, kes muudavad Eesti ettevõtluskeskkonna praktiliselt kasutatavaks, kuid kelle hoolsus- ja teatamiskohustuse täitmine jääb empiiriliste juhtumite põhjal sageli formaalseks.

Teisele uurimisküsimusele vastates näitas töö, et Eesti ja EL-i regulatiivne raamistik sisaldab mitmeid riskide maandamise mehhanisme, kuid nende toimivus on piiratud ja tingimuslik. EL kujundab e-residentsusega seotud riskide normatiivset keskkonda digitaalse identiteedi, rahapesu tõkestamise, andmekaitse ja piiriülese õiguskaitsekoostöö kaudu, kuid ei teosta otsest järelevalvet e-residentsuse programmi kui Eesti riigisisese haldusmeetme üle. Seetõttu jääb riskide praktiline ennetamine, tuvastamine ja neile reageerimine valdavalt Eesti asutuste ning rahvusvahelise infovahetuse toimimise kanda.

Ennetamise tasandil on PPA eelkontroll muutunud rangemaks, kasutusele on võetud automaatne järelkontroll ning riskide hindamisse panustavad MTA, RAB, KAPO ja kohustatud isikud. Samas sõltub ennetus endiselt sellest, milline teave on haldusmenetluse käigus kättesaadav ja kontrollitav. Eriti oluliseks piiranguks on välisriikide karistusandmete, ärikeeldude, tegelike seoste ja kolmandate riikide riskiteabe ebaühtlane kättesaadavus.

Tuvastamise tasandil ilmnes, et riskid muutuvad sageli nähtavaks alles välisriikide päringute, rahapesukahtlusega teadete või rahvusvahelise koostöö kaudu. Probleem ei seisne niivõrd tuvastamisvõimekuse puudumises, vaid selles, et riskide esmased jäljed võivad paikneda väljaspool Eesti järelevalveulatust. Kui ettevõtte pangakonto, kliendid, rahavood või tegelik juhtimine asuvad teistes jurisdiktsioonides, sõltub riskipilt sellest, kas ja kui kiiresti jõuab asjakohane teave Eesti asutusteni.

Reageerimise tasandil seisneb Eesti peamine sekkumisvõimalus sageli halduslikes ja järelevalvelistes meetmetes, nagu digi-ID kehtetuks tunnistamine, tegevusloa tühistamine, maksualased kontrollimeetmed või julgeolekuriski korral sissesõidukeelu kehtestamine. Need

meetmed võimaldavad piirata Eesti digitaalse ja ettevõtluskeskkonna edasist kasutamist, kuid ei tähenda alati piiriülese skeemi sisulist menetlemist Eestis. Kui kannatanud, tõendid ja kuritegeliku tegevuse raskuskese paiknevad välisriigis, jääb Eesti roll sageli infoedastuse, rahvusvahelise koostöö ja ligipääsu lõpetamise tasandile.

Tulemused kinnitasid ka nelja analüütilises raamistikus käsitletud asümmeetria olulisust. Informatsiooniline asümmeetria avaldus riskiteabe puudulikus või hilineunud kättesaadavuses, jurisdiktsiooniline asümmeetria tegevuse ja kontrollivõimaluste paiknemises eri riikides, institutsionaalne asümmeetria vastutuse hajumises mitme asutuse ja tasandi vahel ning regulatiivne asümmeetria eeskätt erasektori vahendajate väravahoidja rolli piiratud toimimises.

Töö peamine järeldus on, et e-residentsusega seotud riskide keskne probleem ei seisne niivõrd konkreetsete kontrollimehhanismide puudustes, vaid piiriülese digitaalse tegevuskeskkonna ja territoriaalse järelevalve struktuurses lahknevuses. E-residentsus ekspordib Eesti institutsionaalset usaldust ja digitaalset ligipääsu globaalsesse voogude ruumi, samal ajal kui kontroll, menetlus ja vastutus toimivad endiselt suurel määral riigipõhises paikade ruumis. Seetõttu toimib süsteem paremini seal, kus risk on andmetes nähtav, Eesti pädevuses käsitletav ja seostatav konkreetse isiku, ettevõtte või loaga. Süsteemi piirid ilmnevad olukordades, kus risk on hajutatud mitme jurisdiktsiooni, erasektori vahendajate ja rahvusvaheliste rahavoogude vahel. Seetõttu eeldab riskide tõhus maandamine lisaks riigisisestele kontrollimehhanismidele ka toimivat piiriülest infovahetust, ennetust ja järelevalvekoostööd.

Laiemas tähenduses näitab töö, et e-residentsuse riskid on seotud Eesti strateegilise avatuse ja järelevalvevõimekuse vahelise pingega, mis asetub ka laiemasse EL-i siseturu konteksti. Piirideta digitaalne majandusruum loob olulisi võimalusi ettevõtluseks ja innovatsiooniks, kuid võib samal ajal suurendada võimalusi kasutada ära riikidevahelisi regulatiivseid ja järelevalvelisi erinevusi. E-residentsus ilmestab seda pinget selgelt, sest õiguspäraselt loodud digitaalne lahendus võib piiriüleses keskkonnas pakkuda vahendeid ka tegevuse tegeliku sisu, kontrolli või kasusaajate varjamiseks. Seetõttu on programmi edasise arengu seisukohalt keskne, kuidas riik määratleb oma riskiisu ning milliste mehhanismidega seob innovatsiooni, majandusliku kasu ja turvalisuse kaalutlused.

Edasistes uuringutes tuleks põhjalikumalt käsitleda erasektori vahendajate rolli, e-residentidega seotud ettevõtete tegelikku majanduslikku aktiivsust ning EL-i uue rahapesu tõkestamise raamistiku mõju e-residentsusega seotud riskide maandamisele. Samuti vajab täiendavat analüüsi see, kuidas tulevased tehnoloogilised lahendused, sealhulgas biomeetriline kaugtuvastus, mõjutavad e-residentsuse süsteemi kontrollivõimekust ja usaldusväärsust.

Kasutatud allikad

- Albanese, J. S. (2012). Deciphering the linkages between organized crime and transnational crime. *Journal of International Affairs*, 66(1), 1–16. https://www.researchgate.net/publication/318312132_Deciphering_the_Linkages_between_Organized_Crime_and_Transnational_Crime
- Bache, I. (2012). Multi-level governance in the European Union. In D. Levi-Faur (Ed.), *The Oxford handbook of governance* (lk 628–641). Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780199560530.013.0044>
- Black, J., & Baldwin, R. (2010). Really responsive risk-based regulation. *Law & Policy*, 32(2), 181–213. <https://doi.org/10.1111/j.1467-9930.2010.00318.x>
- Blue, A. (2020). Evaluating Estonian e-residency as a tool of soft power. *Place Branding and Public Diplomacy*. <https://doi.org/10.1057/s41254-020-00182-3>
- Boister, N. (2003). Transnational criminal law? *European Journal of International Law*, 14(5), 953–976. <https://doi.org/10.1093/ejil/14.5.953>
- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40. <https://doi.org/10.3316/QRJ0902027>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Castells, M. (2010). *The Rise of the Network Society* (2. trükk). Wiley-Blackwell. <https://doi.org/10.1002/9781444319514.ch2>
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.
- E-Residency. (s.a.-a). *E-residentsus*. Kasutatud 15.03.2026, <https://www.e-resident.gov.ee/et/>
- E-Residency. (s.a.-b). *E-Residency dashboard*. Kasutatud 15.03.2026, <https://www.e-resident.gov.ee/dashboard/>
- Ettevõtluse ja Innovatsiooni Sihtasutus (EIS). (2025). *E-residentsuse jätkustrateegia 2026–2029*. Kasutatud 14.03.2026, <https://www.e-resident.gov.ee/wp-content/uploads/2026/01/E-residentsuse-jatkustrateegia-2026-2029.pdf>
- Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/849, 20. mai 2015, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist, millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 648/2012 ning tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2005/60/EÜ ja komisjoni direktiiv 2006/70/EÜ. *Euroopa Liidu Teataja L141*. Kasutatud 11.03.2026, <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A32015L0849>

- Euroopa Parlamendi ja nõukogu direktiiv (EL) 2018/843, 30. mai 2018, millega muudetakse direktiivi (EL) 2015/849, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist, ning millega muudetakse direktiive 2009/138/EÜ ja 2013/36/EL. *Euroopa Liidu Teataja L 156*. Kasutatud 11.03.2026, <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A32018L0843>
- Euroopa Parlamendi ja nõukogu direktiiv (EL) 2024/1640, 31. mai 2024, mis käsitleb mehhanisme, mille liikmesriigid peavad sisse seadma finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamiseks, ning millega muudetakse direktiivi (EL) 2019/1937 ja muudetakse ning tunnistatakse kehtetuks direktiiv (EL) 2015/849. *Euroopa Liidu Teataja, OJ L*. Kasutatud 11.03.2026, https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=OJ:L_202401640
- Euroopa Parlamendi ja nõukogu määrus (EL) 2024/1620, 31. mai 2024, millega asutatakse rahapesu ja terrorismi rahastamise tõkestamise amet ning muudetakse määruseid (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010. *Euroopa Liidu Teataja, OJ L*. Kasutatud 11.02.2026, https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=OJ:L_202401620
- Euroopa Parlamendi ja nõukogu määrus (EL) 2024/1183, 11. aprill 2024, millega muudetakse määrust (EL) nr 910/2014 seoses Euroopa digiidentiteedi raamistiku kehtestamisega. *Euroopa Liidu Teataja, OJ L*, 30.04.2024. Kasutatud 11.03.2026, <https://eur-lex.europa.eu/eli/reg/2024/1183/oj>
- Europol. (2023). *Internet Organised Crime Threat Assessment 2023 (IOCTA)*. Europol. <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023>
- Europol. (2025). *European Union Serious and Organised Crime Threat Assessment 2025: The changing DNA of serious and organised crime (SOCTA)*. Publications Office of the European Union. <https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime>
- Financial Action Task Force (FATF). (2020). *Guidance on digital identity for customer due diligence*. FATF. <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf>
- Financial Action Task Force. (2022). *High-risk jurisdictions subject to a call for action – 21 October 2022*. <https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-october-2022.html>
- Financial Action Task Force. (2025). *Money laundering national risk assessment toolkit – Annexes A–C*. FATF. <https://www.fatf-gafi.org/en/publications/Methodsand trends/Money-Laundering-National-Risk-Assessment-Toolkit-Annexes.html>

- Financial Action Task Force (2012-2025), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, FATF, Paris, France. www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html
- Finantsinspektsiooni seadus (FIS) (2001; 2025). *RT I*, 08.07.2025, 27. Kasutatud 11.02.2026, <https://www.riigiteataja.ee/akt/FIS>
- Hardy, A. (2023). Digital innovation and shelter theory: Exploring Estonia's e-Residency, Data Embassy, and cross-border e-governance initiatives. *Journal of Baltic Studies*, 55(4), 793–810. <https://doi.org/10.1080/01629778.2023.2288118>
- Hoffmann, T., & Solarte-Vasquez, M. C. (2022). The Estonian e-residency programme and its role beyond the country's digital public sector ecosystem. *Revista CES Derecho*, 13(2), 184–204. <https://doi.org/10.21615/cesder.6772>
- International Organization for Standardization. (2018). *ISO 31000:2018 – Risk management – Guidelines*. Geneva: ISO. <https://www.iso.org/standard/65694.html>
- Isikut tõendavate dokumentide seadus (ITDS) (1999; 2025). *RT I*, 26.06.2025, 6. Kasutatud 11.02.2026, <https://www.riigiteataja.ee/akt/ITDS>
- Julgeolekuasutuste seadus (JAS) (2000; 2023). *RT I*, 14.03.2023, 25. Kasutatud 11.02.2026, <https://www.riigiteataja.ee/akt/JAS>
- Kaitsepolitseiameti põhimäärus (2014; 2025). *RT I*, 31.01.2025, 4. Kasutatud 12.02.2026, <https://www.riigiteataja.ee/akt/131012025004>
- Kaitsepolitseiamet. (2025). *Aastaraamat 2024–2025*. https://kapo.ee/sites/default/files/content_page_attachments/aastaraamat-2024-2025_0.pdf
- Kaitsepolitseiamet. (2026). *Aastaraamat 2025–2026*. https://kapo.ee/sites/default/files/content_page_attachments/aastaraamat-2025-2026.pdf
- Kalmus, V., Masso, A., & Linno, M. (2015). Kvalitatiivne sisuanalüüs. Allikas: Sotsiaalse Analüüsi Meetodite ja Metodoloogia õpibaas. Kasutatud 23.03.2026, <https://sisu.ut.ee/kvalitatiivne/kvalitatiivne-sisuanaluus/>
- Kimmo, M., Pappel, I., & Draheim, D. (2018). *E-residency as a nation branding case*. In Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance. Association for Computing Machinery. <https://doi.org/10.1145/3209415.3209447>
- Kotka, T., Vargas Alvarez del Castillo, C. I., & Korjus, K. (2015). *Estonian e-residency: Redefining the nation-state in the digital era* (Oxford Cyber Studies Programme Working Paper No. 3). University of Oxford.

- <https://www.ctga.ox.ac.uk/article/estonian-e-residency-redefining-nation-state-digital-era>
- Kotka, T., Vargas Alvarez del Castillo, C. I., & Korjus, K. (2016). Estonian e-Residency: Benefits, risk and lessons learned. In A. Kõ & E. Francesconi (Eds.), *Electronic Government and the Information Systems Perspective (EGOVIS 2016)* (lk 3–15). Springer. https://doi.org/10.1007/978-3-319-44159-7_1
- Laherand, M.-L. (2008). *Kvalitatiivne uurimisviis*. Tallinn: Infotrükk OÜ.
- Lips, S., Bharosa, N., & Draheim, D. (2020). *eIDAS implementation challenges: The case of Estonia and the Netherlands*. In A. Chugunov et al. (Eds.), *Digital Governance and E-Government: EGOSE 2020* (lk 75–89). Springer. https://doi.org/10.1007/978-3-030-67238-6_6
- Lips, S., Vinogradova, N., Krimmer, R., & Draheim, D. (2022). Re-shaping the EU digital identity framework. *dg.o 2022: Proceedings of the 23rd Annual International Conference on Digital Government Research*, 13–21. <https://doi.org/10.1145/3543434.3543652>
- Maksukorralduse seadus (MKS) (2002; 2025). *RT I, 02.10.2025, 4*. Kasutatud 12.02.2026, <https://www.riigiteataja.ee/akt/MKS>
- Masso, A., Kasapoglu, T., Tammpuu, P., & Calzada, I. (2024). *Datafied control and selection of digital identity: Estonian e-residency as “citizenship by connection”*. <https://zenodo.org/records/12666905>
- MONEYVAL. (2022). *Anti-money laundering and counter-terrorist financing measures Estonia. Fifth Round Mutual Evaluation Report: Estonia*. Council of Europe. <https://rm.coe.int/moneyval-2022-11-mer-estonia/1680a9dd97>
- Nye, J. S. Jr. (2004). Wielding soft power. *Harvard Magazine*, 106(1), 16–24. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/joe_nye_wielding_soft_power.pdf
- OpenAI. (2026). ChatGPT (06. aprill mudel), suur keelemudel, <https://chat.openai.com/>
- Passas, N. (2003). Cross-border Crime and the Interface between Legal and Illegal Actors. *Security Journal*, 16(1), 19–37. <https://doi.org/10.1057/palgrave.sj.8340123>
- Rahandusministeerium. (2021). 4.3. *E-residentsusega seonduvate riskide analüüs*. Eesti rahapesu ja terrorismi rahastamise siseriiklik riskihinnang 2020. Kasutatud 23.02.2026, <https://www.fin.ee/media/1774/download>
- Rahandusministeerium. (2025). *Rahapesu ja terrorismi rahastamise riiklik riskihinnang 2025*. Kasutatud 23.02.2026, https://www.fin.ee/sites/default/files/documents/2025-10/NRA%202025%20RP%20raport_01.10.pdf

- Rahapesu Andmebüroo. (2022a). *Virtuaalväeringu teenuse pakkujatega seonduvad riskid Eestis*. <https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#virtuaalvaaringu-tee>
- Rahapesu Andmebüroo. (2022b). *Tüpoloogiateade 1TT202212. Eesti käibemaksukohustuslase numbriga ettevõtete kasutamine maksupettuste ja rahapesu toimepanemisel välismaal*. Kasutatud 22.02.2026, <https://fiu.ee/sites/default/files/documents/2022-12/Tüpoloogiateade%201TT202212.pdf?utm>
- Rahapesu Andmebüroo. (2024a). *Äriühingute teenuse pakkujate välismaa seosega kliendid ja teenused Eestis*. Kasutatud 22.02.2026, <https://fiu.ee/sites/default/files/documents/2024-04/Äriühingute%20teenuse%20pakkujate%20välismaa%20seosega%20kliendid%20ja%20teenused%20Eestis.pdf>
- Rahapesu Andmebüroo. (2024b). *Välismaalase seosega ettevõtted – poolteist aastat hiljem*. Kasutatud 23.02.2026, <https://fiu.ee/sites/default/files/documents/2024-10/Välismaalase%20seosega%20ettevõtted%20poolteist%20aastat%20hiljem.pdf>
- Rahapesu Andmebüroo. (2024c). *Tüpoloogiateade 7TT202401: Vene ja Valgevene isikutega seotud Eesti juriidiliste isikute kasutamine sanktsioonidest hoidumiseks*. Kasutatud 22.02.2026, https://fiu.ee/sites/default/files/documents/2024-01/Tüpoloogiateade%207TT202401_1.pdf
- Rahapesu ja terrorismi rahastamise tõkestamise seadus (RahaPTS) (2007; 2025). *RT I, 14.03.2025, 23*. Kasutatud 11.02.2026, <https://www.riigiteataja.ee/akt/RahaPTS>
- Riigi Infosüsteemi Amet. (s.a). *Digitaalsed dokumendid: ID-kaart, digi-ID, elamisloakaart ja e-residendi digi-ID*. Kasutatud 06.02.2026, <https://www.id.ee/artikkel/digitaalsed-dokumendid-id-kaart-digi-id-elamisloakaart-ja-e-residendi-digi-id/>
- Riigikontroll. (2020). *E-residentsuse programmi tulemuslikkus: Riigikontrolli aruanne Riigikogule*. Riigikontroll. Kasutatud 22.02.2026, <https://www.riigikontroll.ee/tabid/215/Audit/2507/WorkerTab/Audit/WorkerId/97/language/et-EE/Default.aspx>
- Ristoja, L. S. (2026). *E-residendid töid mullu riigikassasse rekordilised 125 miljonit eurot*. E-Residency. Kasutatud 15.03.2026, <https://www.e-resident.gov.ee/et/blog/posts/e-residendid-toid-mullu-riigikassasse-rekordilised-125-miljonit-eurot/>
- Ryder, N. (2011). *Financial crime in the 21st century: Law and policy*. Edward Elgar Publishing.
- Sallam, M. S. H. A., Lips, S., & Draheim, D. (2022). Success and success factors of the Estonian e-residency from the state and entrepreneur perspective. In A. V. Chugunov et al. (Eds.), *Electronic Governance and Open Society: Challenges in Eurasia* (lk 291–304). Springer. https://doi.org/10.1007/978-3-031-04238-6_22

- Sullivan, C., & Burger, E. (2017). *E-residency and blockchain*. *Computer Law & Security Review*, 33(4), 470–481. <https://doi.org/10.1016/j.clsr.2017.03.016>
- Tammpuu, P., & Masso, A. (2018). *‘Welcome to the virtual state’: Estonian e-residency and the digitalised state as a commodity*. *European Journal of Cultural Studies*, 1–18. <https://doi.org/10.1177/1367549417751148>
- Tammpuu, P., & Masso, A. (2019). Transnational digital identity as an instrument for global digital citizenship: The case of Estonia’s e-residency. *Information Systems Frontiers*, 21, 621–634. <https://doi.org/10.1007/s10796-019-09908-y>
- Tammpuu, P., Masso, A., Ibrahim, M., & Abaku, T. (2022). Estonian e-residency and conceptions of platform-based state-individual relationship. *TRAMES: A Journal of the Humanities and Social Sciences*, 26(1), 3–21. <https://doi.org/10.3176/tr.2022.1.01>
- Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage Publications.

Lisad

LISA 1. INFORMEERIMISE JA TEADLIKU NÕUSOLEKU VORM

Hea uuringus osaleja!

Minu nimi on Syrli Siimar ja olen Tartu Ülikooli Johann Skytte poliitikauuringute instituudi tudeng. Kirjutan hetkel oma magistritööd pealkirjaga „*E-residentsuse kaudu ilmnevate finantskuritegevuse riskide realiseerumine ja maandamine Eesti ja Euroopa Liidu regulatiivses raamistikus*“. Tänan Teid, et nõustusite minu uurimistöösse panustama! Minu magistritöö eesmärk on tuvastada, kuidas e-residentsusega seotud kuritegevuse riskid on realiseerunud ning hinnata, kuivõrd suudavad Eesti ja Euroopa Liidu regulatiivsed ning järelevalvelised mehhanismid neid riske ennetada ja piirata.

Uuringu jaoks palun võimalust Teid ligikaudu 30-60 minuti vältel intervjuuerida. Intervjuu jaoks olen ette valmistanud küsimustiku ning vajadusel esitan täpsustavaid lisaküsimusi. Töös kasutatavaid andmeid (intervjueeritavate nimed, töökoha andmed, intervjuude salvestused, transkriptsioonid ja nõusolekulehed) kasutatakse vaid magistritöö tarbeks ning ei jagata kolmandatele osapooltele. Teie isikuandmeid ja saadud vastuseid töödeldakse kooskõlas andmekaitsevennõuetega. Intervjuu helisalvestist säilitatakse kuni 05.06.2026 vaid minu paroolidega turvatud arvutis. Transkriptsioon ja salvestis kustutatakse pärast lõputöö edukat kaitsmist (05.06.2026).

Intervjueeritavate isikuandmed (nimi ja ametikoht) on teada üksnes magistritöö autorile ning neid ei avaldata magistritöös ega muudes materjalides. Töö tekstis kasutatakse intervjueeritavatele viitamisel üldistatud nimetusi, mis tulenevad nende organisatsioonilisest kuuluvusest, näiteks „PPA ekspert“, „MTA ekspert“ jne.

Teil on igal ajahetkel õigus uuringus osalemisest loobuda ning nõuda, et Teilt kogutud andmeid uuringus ei kasutataks. Palun Teil nõusoleku tagasivõtmisest mind teavitada enne 01.05.2026, et jõuaksin magistritöö lõppversioonist andmed eemaldada.

Mind,, on informeeritud ülalmainitud uuringust, olen teadlik läbiviidava uurimistöö eesmärgist, uuringu metoodikast ja ajakulust.

Kinnitan oma nõusolekut selles osalemiseks allkirjaga.

Uuritava allkiri

Kuupäev, kuu, aasta

Intervjuuerija ja isikuandmete vastutav töötleja: Syrli Siimar (syrli.siimar@ut.ee)

LISA 2. INTERVJUUDE KÜSIMUSED

Küsimused Rahapesu Andmebüroo (RAB) eksperdile

1. Asutuse roll ja kokkupuude süsteemiga

1. Kuidas te kirjeldaksite oma asutuse rolli e-residentsuse ökosüsteemis ning milline on teie asutuse peamine kokkupuude e-residentidega või e-residentsusega seotud protsessidega?

2. Riskide avaldumine praktikas

2. Milliseid e-residentsusega seotud riskimustreid peate praegu kõige olulisemateks ning kas ja kuidas on need viimastel aastatel muutunud?

3. Kas teie analüüsides on e-residentidega seotud juhtumites kordunud teatud tüüpilised skeemid või ärimudelid ning millises rahapesu etapis (paigutamine, kihistamine või integreerimine) need kõige sagedamini avalduvad?

4. Kas e-residentidega seotud juhtumid jõuavad RAB-i pigem Eesti kohustatud isikute teadete kaudu või rahvusvaheliste päringute kaudu?

3. Riskide tuvastamine

5. Millised sektorid või teenusepakkujad (nt äriühingute teenusepakkujad, makseasutused, krüptoteenused) on e-residentidega seotud riskijuhtumites kõige sagedamini esinenud?

6. Kui keeruline on praktikas tuvastada e-residentidega seotud ettevõtete tegelikke kasusaajaid, eriti olukordades, kus majandustegevus toimub peamiselt väljaspool Eestit?

4. Institutsionaalne koostöö

7. Kuivõrd tõhus on riigisisene ja rahvusvaheline koostöö ja andmevahetus erinevate asutuste vahel e-residentsusega seotud riskide ennetamisel ja tuvastamisel?

5. Regulaatiivsed arengud

8. Kas teie hinnangul on praegune rahapesu tõkestamise raamistik piisav e-residentidega seotud riskide tuvastamiseks või esineb praktikas lünki, mis raskendavad analüüsi või sekkumist?

9. Milliseid seadusandlikke või institutsionaalseid muudatusi oleks teie hinnangul vaja, et e-residentidega seotud finantsriskide ennetamist ja järelvalvet tõhustada?

10. Kas on mõni aspekt e-residentsuse ja finantssüsteemi kokkupuutepunktis, millele peaks riskide kontekstis rohkem tähelepanu pöörama, kuid mida seni ei ole piisavalt käsitletud?

Küsimused Politsei ja Piirivalveameti (PPA) eksperdile

1. Asutuse roll ja kokkupuude süsteemiga

1. Kuidas te kirjeldaksite oma asutuse rolli e-residentsuse ökosüsteemis ning milline on teie asutuse peamine kokkupuude e-residentidega või e-residentsusega seotud protsessidega?

2. Riskide avaldumine praktikas, haldusmenetlus ja taustakontroll

2. Milliseid e-residentsusega seotud riskimustreid peate praegu kõige olulisemateks ning kas ja kuidas on need viimastel aastatel muutunud?
3. Millised riskikohad või probleemid ilmnevad kõige sagedamini e-residentsuse taotluste läbivaatamisel?
4. Kas praktikas on esinenud olukordi, kus taotluse läbivaatamisel esineb kahtlus võimaliku väärkasutuse suhtes, kuid kehtiv õiguslik raamistik ei võimalda teha negatiivset otsust?
5. Millised on peamised väljakutsed e-residentide taustakontrolli tegemisel?
6. Kuidas hindate olemasolevate andmekogude ja rahvusvaheliste infoallikate piisavust e-residentsuse taustakontrolli tegemisel? Milliseid täiendavaid volitusi, või andmeallikaid peate kõige enam vajalikuks?
7. Kuidas mõjutab taustakontrolli praktikat asjaolu, et haldusmenetluse raames ei ole võimalik teha päringuid näiteks Euroopa karistusregistrite süsteemi (ECRIS) ega tuvastada ärikeelu olemasolu? Milliseid muid kanaleid sellise info hankimiseks kasutatakse?
8. Kas teatud päritoluriikide või piirkondade puhul esineb e-residentsuse taotlustes või hilisemas kasutuses kõrgemat riskiprofiili?

4. Identiteedi kontroll ja võimalik väärkasutus

9. Milliseid peamisi riske näete e-residendi digi-ID võimaliku väärkasutuse kontekstis ning kas praktikas on ette tulnud olukordi, kus e-residendi digi-ID-d on väärkasutatud?

5. Järelkontroll ja seire

10. Alates 2022. aastast rakendab PPA automaatset järelkontrolli e-residentide suhtes. Kas see tähendab, et riskiteavet kontrollitakse regulaarselt kõigi e-residentide puhul ning millistel juhtudel viib selline kontroll täiendava menetluse või digi-ID kehtetuks tunnistamiseni?
11. Kuidas hindate e-residentsuse eel- ja järelkontrolli süsteemi tervikuna? Kuivõrd on võimalik peamisi riske tuvastada juba taotluse menetlemisel ning millised riskid ilmnevad pigem alles pärast digi-ID väljastamist?

6. Piiriülene koostöö ja jurisdiktsioon

12. Kuivõrd tõhus on riigisisene koostöö ja andmevahetus erinevate asutuste vahel e-residentsusega seotud riskide ennetamisel ja tuvastamisel?
13. Kuidas toimib praktikas koostöö välisriikide õiguskaitseorganitega olukordades, kus kuritegu on toime pandud väljaspool Eestit, kuid vahendina on kasutatud Eesti e-residendi ettevõtet?
14. E-residentidega seotud juhtumite puhul laekub Eestile märkimisväärselt välispäringuid, kuid siseriiklikke kriminaalmenetlusi praktiliselt ei ole. Mis on teie hinnangul selle peamised põhjused?
15. Kas teie hinnangul võib Eesti digi-ID või e-residendi staatus rahvusvahelises keskkonnas toimida usaldusmargina, mida võidakse mõnel juhul kasutada ka selleks, et luua näiline legitiimsus äritegevusele?

7. Tehnoloogia ja süsteemi areng

16. Kas tehnoloogilised arengud (nt tehisintellekt või süvavõltsingud) on mõjutanud isikusamasuse tuvastamise või dokumentide kontrolli riske e-residentsuse süsteemis?
17. Milliseid seadusandlikke, institutsionaalseid või tehnilisi muudatusi oleks teie hinnangul vaja, et e-residentsusega seotud riskide ennetamist ja tuvastamist tulevikus tõhustada?
18. Kas on mõni aspekt e-residentsuse süsteemis, millele peaks riskide kontekstis rohkem tähelepanu pöörama, kuid mida seni ei ole piisavalt käsitletud?

Küsimused Maksu ja Tolliametis (MTA) eksperdile

1. Asutuse roll ja kokkupuude süsteemiga

1. Kuidas te kirjeldaksite oma asutuse rolli e-residentsuse ökosüsteemis ning milline on teie asutuse peamine kokkupuude e-residentidega või e-residentsusega seotud protsessidega?

2. Riskide avaldumine praktikas

2. Milliseid e-residentsusega seotud riskimustreid peate praegu kõige olulisemateks ning kas ja kuidas on need viimastel aastatel muutunud?
3. Milliseid maksualaseid riskimustreid on MTA e-residentidega seotud ettevõtete puhul kõige sagedamini täheldanud (nt deklaratsioonide esitamata jätmine, ebareaalne käive või varifirmade kasutamine)?
4. Kas praktikas esineb olukordi, kus Eestis registreeritud e-residendi ettevõttel puudub sisuline majandustegevus Eestis? Milliseid riske see maksujärelevalve vaates tekitab?

3. Riskide tuvastamine ja maandamine

5. Millised kontrolli- või järelevalvemehhanismid toimivad teie hinnangul e-residentidega seotud maksualaste riskide tuvastamisel ja ennetamisel kõige tõhusamalt?
6. Millised indikaatorid või mustrid viitavad MTA praktikas sellele, et ettevõtet võidakse kasutada varifirmana piiriülestes skeemides?
7. Kui keeruline on praktikas hinnata e-residentidega seotud ettevõtete tegelikku majandustegevust olukordades, kus ettevõtte juhtimine või tegevus toimub peamiselt väljaspool Eestit?

4. Institutsionaalne koostöö

8. Kuivõrd tõhus on riigisisene koostöö ja andmevahetus erinevate asutuste vahel e-residentsusega seotud riskide tuvastamisel ja maandamisel?
9. Kuivõrd toetavad EL tasandi koostöömehhanismid e-residentidega seotud maksupettuste riskide tuvastamist? (VIES, Eurofisc, DAC)

5. Tehnoloogia ja regulatiivsed arengud

10. Kas tehnoloogilised arengud (nt digitaalsed ettevõtlusplatvormid, krüptovarad või uued makselahendused) on mõjutanud e-residentidega seotud maksualaste riskide tuvastamist?

6. Tulevik ja süsteemi areng

11. Kas teie hinnangul on praegune maksujärelevalve raamistik piisav e-residentidega seotud maksupettuste riskide tuvastamiseks või esineb praktikas lünki, mis seda raskendavad?
12. Milliseid seadusandlikke, institutsionaalseid või tehnilisi muudatusi oleks teie hinnangul vaja, et e-residentidega seotud maksualaste riskide ennetamist ja järelevalvet tõhustada?
13. Kas on mõni aspekt e-residentsuse ja maksusüsteemi kokkupuutepunktis, millele peaks riskide kontekstis rohkem tähelepanu pöörama, kuid mida seni ei ole piisavalt käsitletud?

Lihtlitsents

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks.

Mina, Syrli Siimar, annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose „E-residentsuse kaudu ilmnevate finantskuritegevuse riskide realiseerumine ja maandamine Eesti ja Euroopa Liidu regulatiivses raamistikus“, mille juhendaja on Mihkel Solvak:

1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace'is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
2. üldsusele kättesaadavaks tegemiseks ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace'i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
3. olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile;
4. kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Syrli Siimar

18.05.2026