TARTU ÜLIKOOL

ÕIGUSTEADUSKOND

Eraõiguse osakond

Ethel Jäärats

KREDIIDIASUTUSTE OMAVAHELINE INFOVAHETUS RAHAPESU TÕKESTAMISE EESMÄRGIL VAADELDUNA ISIKUANDMETE KAITSE PERSPEKTIIVIST

Magistritöö

Juhendajad

Dr. iur. Urmas Volens

Dr. iur. Karin Sein

Tallinn

2022

SISUKORD

SISSEJUHATUS

Euroopa Liit (edaspidi ka *EL*) on pühendunud võitlusele rahapesu ja terrorismi rahastamisega nii ELis kui ka kogu maailmas.[1] Rahapesu vastu võitlemiseks on EL välja töötanud tugeva õigusraamistiku, mida omakorda toetab Euroopa Kohtu kohtupraktika.[2] Tänapäeval töötlevad isikuandmeid riiklike institutsioonide kõrval üha suuremas ulatuses ka äriühingud (sh globaalse haardega suurkorporatsioonid), mistõttu ei pruugi andmesubjektid nende arengute taustal tajuda, milliseid nende isikuandmeid ja millises ulatuses töödeldakse ning kuidas ja kuivõrd on üldse võimalik oma õigusi efektiivselt kaitsta.[3]

Krediidiasutuste tegevus rahapesu ja terrorismi rahastamise tõkestamisel, pangasaladuse hoidmisel, isikuandmete kaitsmisel ning põhimakseteenuste pakkumisel on kiiresti muutuvas tehnoloogilises ja regulatiivses keskkonnas üsna keeruline, kuna eeldab eraõiguse, avaliku õiguse kui ka karistusõiguse normide põhjalikku tundmist; Euroopa Liidu aluslepingutes ja (otsekohalduvates) regulatsioonides sätestatud põhimõtete järgimist; rahvusvahelistes, liidusisestes ja siseriiklikes regulatsioonides, standardites ja muudes juhendmaterjalides orienteerumist ning põhiõigustega kaasnevate kollisioonidega toimetulekut (nt ettevõtlusvabadus *vs* andmekaitse).

2020. aastal ühinesid neli suuremat Eesti krediidiasutust (sh LHV, Swedbank, SEB ja Luminor), kelle turuosad kokku moodustavad ligi 90% Eesti pangandusturust, pilootprojektiga *AML Bridge*, mida arendab Eesti finantstehnoloogia ettevõte Salv Technologies OÜ. *AML Bridge* on teabe- ja andmevahetusplatvorm, mis võimaldab krediidiasutustel vahetada omavahel rahapesu tõkestamiseks vajalikku teavet kiirelt, turvaliselt ja usaldusväärse tehnilise lahenduse kaudu ning kooskõlas kehtivate rahapesu, pangasaladuse ja andmekaitse normidega. Pilootprojekti raames on Salv Technologies OÜ teinud koostööd mh Finantsinspektsiooni, Rahapesu Andmebüroo ja

[1] Euroopa Komisjoni seisukohalt peaks ELis olema ebaseadusliku raha suhtes nulltolerants. Vt Euroopa Komisjon. Komisjoni teatis tegevuskava kohta, mis käsitleb liidu terviklikku poliitikat rahapesu ja terrorismi rahastamise ärahoidmiseks. – ELT C 164, 13.05.2020, lk 21.

[2] Euroopa Kohus on tunnistanud, et rahapesu vastase võitluse eesmärk on seotud avaliku korra kaitsmisega, mis võib õigustada aluslepinguga tagatud põhivabaduste, sealhulgas teenuste ja kapitali vaba liikumise piiramist. Piirav meede peab olema proportsionaalne ehk taotletava eesmärgi saavutamiseks sobiv ega lähe selle saavutamiseks vajalikust kaugemale. Vt EKo C-212/11, *Jyske Bank Gibraltar Ltd versus Administración del Estado*, ECLI:EU:C:2013:270, p-d 64 ja 68 ning nendes viidatud kohtulahendid; vt ka C-190/17, *Lu Zheng versus Ministerio de Economía y Competitividad*, ECLI:EU:C:2018:357, p-d 37 ja 38 ning nendes viidatud kohtupraktika.

[3] Sein, K., Mikiver, M., Tupay, P. K. Pilguheit andmesubjekti õiguskaitsevahenditele uues isikuandmete kaitse üldmääruses. – Juridica 2018/2, lk 94.

Andmekaitse Inspektsiooniga.[4] Euroopa Komisjon on oma teatises rahapesu tõkestamise tegevuskava kohta rõhutanud järgmist: "Tehnoloogilised lahendused, mis võivad aidata parandada kahtlaste tehingute ja tegevuste avastamist, peavad olema kooskõlas rahapesuvastase võitluse ja terrorismi rahastamise tõkestamise rahvusvaheliste ja ELi standarditega ning vastama muudele ELi eeskirjadele, sealhulgas andmekaitse ja monopolidevastase võitluse valdkonnas."[5] Käesoleva magistritöö autor pooldab uute infotehnoloogiliste lahenduste kasutuselevõtmist rahapesu tõkestamise valdkonnas. Samas ei pruugi kehtiv õigusraamistik piisaval määral toetada krediidiasutuste omavahelist infovahetust rahapesu tõkestamise eesmärgil, kuna infovahetuse õiguslikud alused ja ulatus pole piisavalt selged ning üheselt mõistetavad, et tagada rahapesuvastaste meetmete ning andmekaitse põhimõtete ühetaoline käsitlemine ja rakendamine ning vähendada seeläbi isikuandmete õigustamatu töötlemise võimalusi (mh *AML Bridge* lahendust kasutades) ning selle võimalikke negatiivseid tagajärgi.

Kehtivate EL ja siseriiklike regulatsioonide kohaselt peavad krediidiasutused koguma uute ja olemasolevate klientide kohta taustainfot ning muud vajalikku teavet nii kliendisuhte loomisel kui ka kliendisuhte käigus, et kohaldada nende suhtes hoolsusmeetmeid[6] rahapesu ja terrorismi rahastamise tõkestamise seaduses[7] (edaspidi ka *RahaPTS*) sätestatud ulatuses, lähtudes seejuures riskipõhisest lähenemisest. Kõigil kohustatud isikutel on lubatud vahetada omavahel teavet rahapesu tõkestamise eesmärgil (mh hoolsusmeetmete kohaldamiseks), järgides seejuures õigusaktidest tulenevaid kohustusi ja piiranguid (RahaPTS § 16 lg 1), kuid üksnes krediidi- ja finantseerimisasutustel on õigus vahetada omavahel teavet kõrge riskiga klientide ja kuriteokahtlusega tehingute kohta rahapesu tõkestamise eesmärgil (RahaPTS § 51 lg 5). Piirangute mõttes tuleb krediidiasutuste omavahelist infovahetust reguleerivaid sätteid RahaPTS-s käsitleda ennekõike koosmõjus pangasaladust reguleerivate sätetega krediidiasutuste seaduses[8] (edaspidi ka

[4] Salv. Towards a New Standard in AML/CTF. The case for FinCrime Intelligence Sharing – an In-Depth Look at the AML Bridge Estonia Pilot. April 2021, lk 5-6. – Uute https://salv.com/assets/files/AML%20Bridge%20Estonia%20whitepaper.pdf (26.11.2021).
[5] Euroopa Komisjon. Komisjoni teatis tegevuskava kohta, mis käsitleb liidu terviklikku poliitikat rahapesu ja terrorismi rahastamise ärahoidmiseks (viide 1), lk 25.
[6] Bilali, G. Know Your Customer - Or Not. - University of Toledo Law Review 2012/43, lk 366.
[7] Rahapesu ja terrorismi rahastamise tõkestamise seadus. – RT I, 12.03.2022, 19.
[8] Krediidiasutuste seadus. – RT I, 29.03.2022, 5.

KAS) ning andmekaitset reguleerivate sätetega isikuandmete kaitse üldmääruses[9] (edaspidi ka *üldmäärus* või *IKÜM*).

Riskipõhise lähenemise kohaselt peavad krediidiasutused tuvastama, hindama ja aru saama nende tegevusega seotud rahapesu riskidest, et rakendada tõhusaid meetmeid nende maandamiseks.[10] Riskipõhine lähenemine jätab krediidiasutustele teatud otsustus- ja tegevusvabaduse (s.o diskretsiooniõiguse) rakendada hoolsusmeetmeid säästlikult ja efektiivselt ning suunata ressursse sinna, kus rahapesu risk on kõige suurem. Riskipõhine lähenemine lähtub loogikast, et hoolsusmeetmete loetelu on regulatsioonides standardiseeritud, kuid hoolsusmeetmete rakendamise viisi ja ulatuse valik peab sõltuma riskidest ning jääma lõpliku rakendaja (st krediidiasutuse) vastutada.[11] Vastavast loogikast lähtudes peaks krediidiasutustele jääma otsustusõigus ka rahapesu tõkestamise eesmärgil toimuva infovahetuse viisi ja ulatuse osas, kui järgida õigusaktidest tulenevaid kohustusi ja piiranguid. Pangasaladuse hoidmise kohustus ning isikuandmete kaitse nõuded on seejuures peamised piirangud, millega krediidiasutused peavad omavahelise infovahetuse puhul arvestama.

Seega on kehtivate rahapesuvastaste regulatsioonide kohaselt ning lähtudes rahapesu tõkestamise riskipõhisest lähenemisest krediidiasutustele jäetud suhteliselt suur otsustus- ja kaalutlusõigus oma riskiisu paika panemisel, kõrge riskiga klientide määratlemisel ning kahtlaste tehingute sisustamisel, kuid see muudab isikuandmete töötlemise ulatuse määratlemise keeruliseks olukorras, kus puuduvad üksikasjalikud juhised krediidiasutuste omavahelise infovahetuse kohta. Hoolimata teemakohase kirjanduse rohkusest on kontseptuaalseid või empiirilisi teadusuuringuid rahapesu ja terrorismi rahastamise tõkestamise alal rahastatud väga vähe (võrreldes nö kriminoloogia peavoolu valdkondadega)[12]. Tulemuseks on teaduspõhise käsitluse vähesus rahapesu tõkestamise valdkonnas, mis muudab infovahetuse ulatuse piiritlemise omakorda

[9] 27. aprilli 2016. aasta Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119, 04.05.2016, lk 1–88.

[10] FATF. Guidance for a Risk-Based Approach. The Banking Sector. October 2014, lk 6. – https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf (01.10.2021).

[11] Siclari, D. The New Anti-Money Laundering Law. First Perspectives on the 4th European Union Directive. New York: Palgrave Pivot 2016, lk 12-13; vt ka Rahapesu ja terrorismi rahastamise tõkestamise seaduse eelnõu 459 SE seletuskiri. 04.05.2017. - https://www.riigikogu.ee/tegevus/eelnoud/eelnou/fb03e20e-caf7-463d-9b60-ddf6021742b2/Rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20seadus (14.09.2021).

[12] Levi, M. Evaluating the Control of Money Laundering and Its Underlying Offences: The Search for Meaningful Data. – Asian Journal of Criminology 2020/15, lk 317.

keerulisemaks. Näiteks piirdub osade kuritegude puhul koosseis paari kirjareaga, kuid selle taga on kümneid tuhandeid lehekülgi teadustööd (nt mõrv ja mõrvarite profileerimine). Samas lähtub rahapesu tõkestamine sadadest normidest, kuid teaduslik käsitlus mh kurjategijate psühholoogia ja nende käitumismudelite kohta on suuresti olematu.[13] Tänase Rahapesu Andmebüroo juhi M. Mäekeri ning Finantsinspektsiooni juhatuse liikme A. Nõmme arvates võib teaduspõhise käsitluse puudumise üheks põhjuseks olla see, et rahapesu tõkestamise finantsvaldkonna regulatsioon põhineb suuresti raskesti kvalifitseeritaval sõnal „kahtlus“, mida tuleb sisustada pehmele teadusele tuginedes nagu majandus- ja ärisuhete toimimise põhimõtted, kus hoolsuse mõõdupuuks on leida tehingutest või toimingutes ratsionaalsus.[14] Kokkuvõttes nad leiavad, et teadusliku arusaama puudumise suurem põhjus on tõenäoliselt see, et rahapesu vastu võitlemisest on saanud ühisnimetaja, kus tegelik eesmärk on võitlus kuritegevuse vastu selle laiemas tähenduses.[15]

Krediidiasutuste omavaheline tõhus infovahetus rahapesu tõkestamise eesmärgil on krediidiasutustele kasulik ja vajalik eelkõige kahest aspektist. Esiteks, krediidiasutused kui kasumit teenivad äriühingud vähendavad efektiivse infovahetuse kaudu oma aja- ja ressursikulu, et hankida vajalikku teavet klientide suhtes hoolsusmeetmete kohaldamiseks (nt kliendi isikusamasuse, poliitilise taustaga isikute, tegelike kasusaajate tuvastamiseks jms). Teiseks, krediidiasutused kui sotsiaalselt vastutustundlikud ettevõtjad aitavad tõhusa infovahetusega kaasa kõrge riskiga klientide tuvastamisele, et vajadusel piirata nende ligipääsu finantsteenustele (v.a põhimakseteenused), samuti kuriteokahtlusega tehingute tuvastamisele, et aidata kaasa süütegude avastamisele ja tõkestamisele ning seeläbi vähendada rahandussüsteemi kasutamist rahapesu eesmärgil.

Ajavahemikul 2019-2021 täiendati mitmeid KAS ja RahaPTS sätteid, mis reguleerivad krediidiasutuste koostööd ja infovahetust rahapesu tõkestamise eesmärgil (nt RahaPTS § 16 lg 4 ja lg 5, RahaPTS § 51 lg 1) ning sellele rakenduvaid piiranguid (nt KAS § 88 lg 5^1 p 4). Krediidiasutuste infovahetuse peamised alused ja ulatuse riigisiseses õiguses määravad RahaPTS § 16 lõiked 1 ja 2 ning § 51 lõige 5. Vastavate sätete rakendamine on tekitanud aga mitmeid küsimusi, eelkõige kõrgema riskiga klientide ja kuriteokahtlusega tehingute mõiste defineerimise

[13] Mäeker, M, Nõmm, A. The AML Compliance Book. 150 Golden Rules. Tallinn: Tallinna Raamatutrükikoja OÜ 2020, lk 11-12.
[14] Mäeker, M., Nõmm, A. Pangasaladuse hoidjast politseinikuks: valikud rahapesu tõkestamisel. – Juridica 2020/8, lk 664.
[15] *Ibid*, lk 665.

osas ning sellest lähtuvalt isikuandmete töötlemise aluste ja ulatuses osas. Kehtiv õigusraamistik koos täiendavate juhistega peaks toetama vastavate mõistete sisustamist ning seadma täpsemad piirid isikuandmete töötlemise ulatusele krediidiasutuste omavahelise infovahetuse käigus rahapesu tõkestamise eesmärgil, et vähendada isikuandmete õigustamatu töötlemise võimalusi ning piiranguid finantsteenuste kättesaadavusele, kuna krediidiasutuste omavahelise infovahetuse käigus edastatud teabe põhjal suureneb oht, et kõrgema riskiga klientidega lõpetatakse ärisuhted ning suletakse nende pangakontod (ingl *de-risking*). Käesoleva töö eesmärk on analüüsida kehtivat õigusraamistikku eelkõige isikuandmete kaitse perspektiivist, et selgitada välja, kas rahapesu tõkestamise eesmärgil toimuva krediidiasutuste omavahelise infovahetuse õiguslikud alused ja ulatus on piisavalt selgelt määratletud ning üheselt mõistetavad, et kaitsta füüsilisi isikuid isikuandmete õigustamatu töötlemise eest. Käesolevas töös ei ole analüüsitud uut EL rahapesuvastast paketti, mis sisaldab mh otsekohalduva määruse vastuvõtmist ning Rahapesu ja Terrorismi Rahastamise Tõkestamise Ameti (AMLA) loomist[16], lisaks muudatusi seoses rahapesu andmebüroode koostöö ja infovahetusega[17], kuid ei pruugi kaasa tuua olulisi muudatusi kohustatud isikute omavahelise infovahetuse osa, kuigi lõppastmes ei ole see ka välistatud.

Eesti õiguskirjanduses on rahapesu ja andmekaitse temaatika leidnud üha rohkem käsitlust ja kajastamist, sh ajakirja Juridica rahapesuteemalises erinumbris (2020/8) ning viimastel aastatel rahapesu ja andmekaitse teemadel kaitstud magistritöödes. Samas pole autorile teada ühtegi magistritööd, mis oleks põhjalikult käsitlenud krediidiasutuste omavahelist infovahetust rahapesu tõkestamise eesmärgil vaadelduna isikuandmete kaitse perspektiivist. T. Kihuoja magistritöös on analüüsitud isikuandmete töötlemise õiguslikke aluseid ning isikuandmete kaitse õiguse riiveid rahapesuvastaste hoolsusmeetmete kohaldamisel krediidiasutustes.[18] Isikuandmete töötlemise õiguslikud alused ja ulatus hoolsusmeetmete kohaldamiseks ning krediidiasutuste omavaheliseks infovahetuseks ei pruugi kattuda, isegi kui andmetöötlus toimub rahapesu tõkestamise eesmärgil,

[16] Euroopa Komisjon. Ettepanek: Euroopa Parlamendi ja Nõukogu Määrus, millega asutatakse rahapesu ja terrorismi rahastamise tõkestamise amet ning muudetakse määruseid (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010. COM(2021) 421 final, 2021/0240(COD). Brüssel, 20.7.2021. - https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52021PC0421&from=EN (01.04.2022).

[17] European Commission. Factsheet: Stronger EU Rules to Fight Financial Crime. July 2021. - https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/210720-anti-money-laundering-countering-financing-terrorism-factsheet_en.pdf (01.04.2022).

[18] Kihuoja, T. Isikuandmete kaitse õiguse riived rahapesu ja terrorismi rahastamise tõkestamiseks kohaldatavate hoolsusmeetmete käigus ning õiguslikud alused isikuandmete töötlemiseks krediidiasutustel. Magistritöö. Tartu: TÜ õigusteaduskond 2021.

kuna esimesel juhul on tegemist seadusest tuleneva kohustuse täitmisega ning teisel juhul seadusandja poolt krediidiasutustele antud võimalusega isikuandmeid täiendavalt töödelda. Sellest tulenevalt on isikuandmete töötlemise aluste ja ulatuse käsitlus erinev. P. Rummi magistritöös on analüüsitud andmesubjekti kaitset profiilianalüüsil põhinevate automatiseeritud otsuste tegemisel krediidiasutuses.[19] Isegi kui profiilianalüüsi kasutakse lisaks kliendi krediidivõimelisuse hindamisele ka muude profiilide loomiseks (nt riskiprofiil)[20], peab kõrgema riskiga klientide kohta teabe avaldamine teistele krediidiasutustele lähtuma rahapesu tõkestamise eesmärgist ning arvestama andmetöötluse piirangutega (sh pangasaladus, isikuandmete kaitse jms), mitte lähtuma profiilianalüüsi tulemustest, mis võib peegeldada kliendi kõrgemat riskiastet.

Rahapesu tõkestamise temaatika puudutab otseselt või kaudselt nii eraisikuid, äriühinguid kui ka avaliku sektori asutusi ja organisatsioone (sh järelevalveasutusi, õiguskaitseasutusi, rahvusvahelisi organisatsioone jt), sõltuvalt nende majandus-, kutse- või ametitegevusest valitud sektoris või igapäevaselt kasutatavatest maksevahenditest (sh sularaha, elektroonilised maksevahendid, virtuaalvääringud jpt). Arvestades magistritöö mahtu ja eesmärki on autor keskendunud üksnes ühele rahapesu tõkestamise temaatikaga seotud aspektile ehk krediidiasutuste omavahelisele infovahetusele rahapesu tõkestamise eesmärgil, käsitledes infovahetuse õiguslikke aluseid ja ulatust lähtudes isikuandmete kaitse perspektiivist. Seoses sellega analüüsitakse töös vaid füüsiliste isikutega seotud krediidiasutuste omavahelist infovahetust rahapesu tõkestamise eesmärgil. Juriidilistel isikutel puudub eraelu ning isikuandmed, mida kaitsta, mistõttu ei kuulu juriidilised isikud põhiseaduse PS § 26 ega üldmääruse kohaldumisalasse. Juriidilised isikud saavad isikuandmete kaitse osas tugineda põhiõiguste harta artiklile 7 (*era- ja perekonnaelu puutumatus*) ja artiklile 8 (*isikuandmete kaitse*) ning seeläbi ka üldmäärusele, kui juriidilise isiku ametliku nime kaudu on võimalik tuvastada üks või mitu füüsilist isikut.[21] Samas kohaldub üldmäärus kõigile Eestis äriregistrisse kantud füüsilisest isikust ettevõtjatele, kuna äriseadustiku[22] (edaspidi ÄS) § 8 lõike 1 kohaselt peab füüsilisest isikust ettevõtja ärinimi sisaldama ettevõtja ees- ja perekonnanime, välja arvatud füüsilisest isikust talupidaja puhul, kui ärinimes sisaldub talu nimi (ÄS § 8 lg 2). Järelikult saavad äriühingu omanikud ärinime valides otsustada, kas ja kuivõrd

[19] Rummi, P. Andmesubjekti kaitse profiilianalüüsil põhinevate automatiseeritud otsuste tegemise regulatsiooni rakendamisel krediidiasutuste tingimuste näitel. Magistritöö. Tallinn: TÜ õigusteaduskond 2020.
[20] *Ibid*, lk 31.
[21] Liidetud kohtuasjad EKo C-92/09 ja C-93/09, *Volker und Markus Schenke GbR ja Hartmut Eifert vs Land Hessen*, ECLI:EU:C:2010:662. p 52-53.
[22] Äriseadustik. – RT I, 12.03.2022, 12.

üldmäärus neile kohaldub.[23] Andmekaitse nõuded kuuluvad igal juhul kohaldamisele, kui äriühingud edastavad üksteisele isikustatud andmeid (nt krediidiasutused omavahelise infovahetuse käigus rahapesu tõkestamise eesmärgil).

Magistritöös on läbivalt kasutatud mõistet *rahapesu tõkestamine*, et tähistada nii rahapesu kui ka terrorismi rahastamise tõkestamist (ingl lühend *AML/CTF*), kuna enamus RahaPTS kirjeldatud meetmetest puudutab mõlemat valdkonda. Samas ei käsitleta magistritöös detailselt terrorismi rahastamisega seonduvat. Samuti on töös kasutatud mõisteid *pank* ja *krediidiasutus* sünonüümidena, lähtudes krediidiasutuste seaduses määratletud terminitest (s.o pank kui krediidiasutus, vt KAS 3. ptk).

Magistritöö üldine eesmärk on välja selgitada rahapesu tõkestamise eesmärgil toimuva krediidiasutuste omavahelise infovahetuse regulatsiooni olemus, vajadus ja eesmärgid vaadelduna isikuandmete kaitse perspektiivist. Regulatsiooni tähenduse, toimimise ja probleemkohtade selgitamisel ning analüüsimisel lähtutakse töös järgmistest uurimisküsimustest:

(1) Millisel õiguslikul alusel ja millises ulatuses on lubatud isikuandmete töötlemine krediidiasutuste omavahelise infovahetuse käigus rahapesu tõkestamise eesmärgil?
(2) Milliste põhimõtete ja piirangutega peavad krediidiasutused arvestama isikuandmete töötlemisel krediidiasutuste omavahelise infovahetuse käigus rahapesu tõkestamise eesmärgil?

Töö esialgsed hüpoteesid on järgmised:

(1) Rahapesu tõkestamise eesmärgil toimuva krediidiasutuste omavahelise infovahetuse õiguslikud alused ja ulatus pole regulatsioonides ja neid selgitavates juhistes piisavalt üksikasjalikult ja üheselt mõistetavalt määratletud, et kaitsta füüsilisi isikuid isikuandmete õigustamatu töötlemise ja selle võimalike negatiivsete tagajärgede eest.
(2) Rahapesu tõkestamise eesmärgil toimuv krediidiasutuste omavaheline infovahetus võib vähendada füüsiliste isikute ligipääsu finantsteenustele, kuna edastatud teabe põhjal suureneb oht, et krediidiasutused hakkavad vältima riske nende maandamise asemel (ingl *de-risking*) ning sulgevad pangakontod ja lõpetavad ärisuhted kõrgema riskiga klientidega.

[23] Kihuoja, T. (viide 18), lk 20.

Käesoleva magistritöö autori eesmärgiks oli analüüsida kehtivat õigust ning selle tähendust krediidiasutuste ja andmesubjektide perspektiivist, samuti võimalikke lahendusi ja ettepanekuid muudatuste sisseviimiseks regulatsioonidesse ja/või neid täiendavatesse juhistesse, mistõttu on töö kirjutamisel kasutatud dogmaatilist meetodit.

Magistritöö kirjutamisel on allikatena läbivalt kasutatud kehtivaid regulatsioone; liidu komisjoni, parlamendi ja nõukogu seisukohti, institutsioonide arvamusi ja ettepanekuid; erinevate organisatsioonide standardeid ja muid juhiseid; kodumaist ja rahvusvahelist õiguskirjandust; Eesti, Euroopa Kohtu ning Euroopa Inimõiguste Kohtu praktikat. Rahapesu ja andmekaitse temaatika on viimased paarkümmend aastat pakkunud kogu maailmas kõneainet, mistõttu viitab autor ka enne 2000. aastat avaldatud allikatele.

Magistritöö struktuur lähtub töö eesmärgist, uurimisküsimustest ja hüpoteesidest. Töö koosneb kolmest peatükist. Esimeses peatükis otsib autor vastust küsimusele, millised RahaPTS ning KAS sätted reguleerivad krediidiasutuste omavahelist infovahetust rahapesu tõkestamise eesmärgil ja milliste piirangutega peavad krediidiasutused seejuures arvestama. Teises peatükis keskendub autor küsimusele, millisel õiguslikul alusel ja millises ulatuses on lubatud isikuandmete töötlemine krediidiasutuste omavahelise infovahetuse käigus rahapesu tõkestamise eesmärgil ning milliste põhimõtetega tuleb andmetöötluse puhul arvestada. Kolmandas peatükis uuritakse krediidiasutuste omavahelist infovahetust kuriteokahtlusega tehingute ja kõrgema riskiga klientide osas, kuna tegemist on piisavalt määrtlemata õigusmõistetega, mis muudab keerulisemaks ka isikuandmete töötlemise õiguslike aluste ja ulatuse määratlemise. Samuti on analüüsitud finantsteenustele ligipääsu piiramise probleemi, mida krediidiasutuste omavaheline infovahetus võib võimendada tänu määratlemata õigusmõistetele ning üksikasjalike regulatsioonide ja juhiste puudumisele.

Märksõnad: rahapesu, andmekaitse, isikuandmed

1 KREDIIDIASUTUSTE OMAVAHELISELE INFOVAHETUSELE KOHALDUV REGULATSIOON SEOSES RAHAPESU TÕKESTAMISEGA

1.1 Rahapesu tõkestamise õiguslik raamistik

Viimase paari aastakümne jooksul on rahapesu ja terrorismi rahastamise tõkestamise temaatika olnud pidevalt päevakorral, sh erinevate terrorirünnakute (nt 9/11 USA-s jt), rahapesuskandaalide (nt Danske Bank A/S Eesti filiaali tegevusloa tühistamine jt) ning muude lekitamisjuhtumite tõttu (nt *Wikileaks*, *Panama Papers* jt). Käesolevas töös pole käsitletud rahapesu kujunemislugu ega rahapesuvastaste meetmete teket ja arengut, kuna magistritöö maht on piiratud ning vastavaid teemasid on oma magistritöös põhjalikult käsitlenud I. Tibar [24]. Töö autor analüüsib kehtivat õigust, keskendudes rahapesu tõkestamise regulatsioonide, nende seletuskirjade või kommentaaride, standardite ja muude juhendmaterjalide puhul eelkõige nüanssidele, mis puudutavad krediidiasutuste omavahelist infovahetust rahapesu tõkestamise eesmärgil ning pangasaladuse ja isikuandmete kaitse regulatsioonidest tulenevaid piiranguid.

K. Pikknurme magistritöös on tabavalt väljendanud mõtet rahapesu tõkestamise õigusraamistiku pideva täiendamisvajaduse kohta: „Hoolsusmeetmed on alati olnud oma ajastu peegelpilt võttes arvesse selle aja infotehnoloogilisi võimalusi ja praktikas esinevaid probleeme. Selleks, et kurjategijatel ei õnnestuks karistuseta pääseda, tuleb pidevalt täiendada ja täiustada kehtivat rahapesu tõkestamise regulatiivset raamistikku.“[25] Rahapesuvastane töökond (edaspidi FATF) võttis 1990. a vastu 40 soovitust[26], mis olid suunatud rahapesu tõkestamisele, ning 2001. a 9 erisoovitust[27], mis olid suunatud terrorismi rahastamise tõkestamisele. FATFi põhimõtetele tugines kehtestas Euroopa Liit järgemööda kolm rahapesuvastast direktiivi – 1991. a esimese

[24] Tibar, I. Rahapesu: kujunemislugu ja koosseis Eesti karistusõiguses. Magistritöö, Tartu Ülikooli õigusteaduskond 2007, lk 11-17.
[25] Pikknurm, K. Investeerimisühingu vastavuskontrolli teostaja ja juhatuse vastutus rahapesu tõkestamisel Eesti õigusruumis. – Tallinn: TÜ õigusteaduskond 2018, lk 12.
[26] FATF. The Forty Recommendations of the Financial Action Task Force on Money Laundering. Paris, 1990. - http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf (20.10.2021).
[27] FATF. FATF IX Special Recommendations. October 2001 (incorporating all subsequent amendments until February 2008). Paris, 2008. - http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf (20.10.2021).

(91/308/EMÜ, kehtetu alates 14.12.2005)[28], 2001. a teise (2001/97/EÜ, kehtetu alates 14.12.2005)[29] ning 2005. a kolmanda rahapesuvastase direktiivi (2005/60/EÜ, kehtetu alates 25.06.2017)[30]. Vastavate direktiividega laiendati rahapesu kuritegude ja kohustatud isikute ringi (sh väljapoole finantssektorit), hõlmati terrorismi rahastamise tõkestamine, võeti kasutusele riskipõhine lähemine, millega karmistati rahapesu riski maandamiseks kohaldatavaid hoolsusmeetmeid, ning ühtlustati FATF soovituste ühetaolist rakendamist liikmesriikides.[31]

2012. a vastu võetud ja 2022.a viimati uuendatud FATF soovitused sätestavad kõikehõlmava ja tervikliku raamistiku meetmetest, mida riigid peaksid rakendama võitluses rahapesu ja terrorismi rahastamise ning massihävitusrelvade leviku rahastamise vastu.[32] 2015. a maikuus võttis EL vastu neljanda rahapesu ohtu käsitleva direktiivi (EL) 2015/849 (edaspidi ka *AMLD4*)[33], milles rõhutas vajadust viia liidu õigusaktid kooskõlla FATF soovituste ja muude rahvusvaheliste organite instrumentidega (AMLD4 pp 4). Sisuliselt tähendas see nõuet kohandada FATF soovitustes toodud rahvusvahelised standardid liidu siseturu vajadustele vastavaks.[34] AMLD4 väljatöötamisel rõhutati ka riskipõhise lähenemise ning kliendi suhtes kohaldatavate hoolsusmeetmete tõhustamise vajadust, mis omakorda tähendas suurema hulga isikuandmete kogumist ja säilitamist. Böszörmenyi jt hinnangul on see problemaatiline, kuna võib viia sekkumiseni isiku eraellu Euroopa Liidu põhiõiguste harta[35] (edaspidi ka *põhiõiguste harta*) artikli 8 tähenduses (st isikuandmete kaitse põhiõiguse riiveni).[36] AMLD4 põhjenduspunkt 43 tõstab selgelt esile liidu

[28] 10. juuni 1991. aasta Euroopa Ühenduste Nõukogu direktiiv 91/308/EMÜ rahandussüsteemi rahapesu eesmärgil kasutamise vältimise kohta. – ELT 09/1. kd, 28.12.2001, lk 153-158. Direktiiv kaotas kehtivuse 14.12.2005.

[29] 4. detsembri 2001. a Euroopa Parlamendi ja Nõukogu direktiiv 2001/97/EÜ, millega muudetakse Nõukogu direktiivi 91/308/EMÜ rahandussüsteemi rahapesu eesmärgil kasutamise vältimise kohta. – Euroopa Ühenduste Teataja L 344, lk 76-81. Direktiiv kaotas kehtivuse 14.12.2005.

[30] 26. oktoobri 2005. aasta Euroopa Parlamendi ja Nõukogu direktiiv 2005/60/EÜ rahandussüsteemi rahapesu ja terrorismi rahastamise eesmärgil kasutamise vältimise kohta. – ELT L 309, 25.11.2005, lk 15-36. Direktiiv kaotas kehtivuse 25.06.2017.

[31] Sarapuu, T. Piiriülese investeerimisteenuse osutamine ja kliendi isikusamasuse tuvastamine. Magistritöö. Tallinn: TÜ õigusteaduskond 2015, lk 24.

[32] FATF. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations. Updated March 2022. Paris, 2012-2022, lk 7. - http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (01.04.2022).

[33] 20. mai 2015. aasta Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2015/849, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist ning millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 648/2012 ja tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2005/60/EÜ ja komisjoni direktiiv 2006/70/EÜ. – ELT L 141, 30.06.2021, lk 73-117.

[34] Tellisaar, L. Tegelike kasusaajate registri ülesanne rahapesu tõkestamisel. Magistritöö, Tallinn: TTÜ majandusteaduskond 2018, lk 18.

[35] Euroopa Liidu põhiõiguste harta. – ELT C 202, 07.06.2016, lk 389-405.

[36] Böszörmenyi, J., Schweighofer, E. A Review of Tools to Comply with the Fourth EU Anti-Money Laundering Directive. International Review of Law, Computers & Technology 2015/ 29 (1), lk 66 ja 71.

andmekaitsealaste õigusaktide ja põhiõiguste hartas kinnistatud põhiõiguste kaitsmise olulisuse, sh vajaduse järgida liidu õigust AMLD4 kooskõlla viimisel FATF muudetud soovitustega.

2018. a võttis EL vastu viienda rahapesuvastase direktiivi (EL) 2018/843 (edaspidi ka *AMLD5*)[37], mis laiendas mh AMLD4 kohaldamisala virtuaalvääringute ja ametlike vääringute vahetamise teenuse pakkujatele ja rahakotiteenuse pakkujatele ning hõlmas virtuaalvääringute kõikvõimalikud kasutusviisid (AMLD5 pp 8 ja 10). AMLD5 kohustas äriühinguid ja muid juriidilisi isikuid koguma ja hoidma asjakohast, täpset ja ajakohastatud teavet tegelikult kasu saava omaniku kohta ning liikmesriike tagama juurdepääsu vastavale teabele riiklikes registrites (pp 20-21, 25 jj), järgides seejuures andmekaitse nõudeid (pp 38 jt). Käesoleva magistritöö seisukohalt on oluline AMLD5 põhjenduspunkt 46, mis ütleb järgmist: „Kurjategijad liigutavad ebaseaduslikku tulu selle avastamise vältimiseks paljude finantsvahendajate kaudu. Seetõttu tuleb krediidiasutustel ja finantseerimisasutustel lubada vahetada teavet mitte üksnes kontserni liikmete vahel, vaid ka teiste krediidiasutuste ja finantseerimisasutustega, järgides siseriiklikus õiguses sätestatud andmekaitsenorme.“ Seega suunab AMLD5 otseselt tähelepanu krediidiasutuste ja finantseerimisasutuste omavahelise infovahetuse vajalikkusele rahapesu tõkestamise eesmärkide saavutamisel.

2018. a võttis EL vastu ka kuuenda rahapesuvastase direktiivi (EL) 2018/1673 (edaspidi ka *AMLD6*)[38], mille eesmärgiks oli võidelda rahapesu vastu kriminaalõiguse abil, võimaldades pädevatel asutustel teha piiriülest koostööd tõhusamalt ja kiiremini (AMLD6 pp 1). Direktiivi kohaselt peaksid liikmesriigid üksteist rahapesu puudutavates kriminaalmenetlustes võimalikult palju aitama ning tagama, et teabevahetus oleks tõhus ja kiire ning kooskõlas liikmesriigi õiguse ja liidu kehtiva õigusraamistikuga (AMLD6 pp 9). Lisaks kehtestati AMLD6-ga rahapesukuritegude määratlemise ning nende kuritegude eest mõistetavate karistuste miinimumnõuded (art 1 lg 1, pp 13), samuti võimalus võtta teatud rahapesuga seotud tegevuste eest vastutusele juriidilisi isikuid (art 7).

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

[38] 23. oktoobri 2018. aasta Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2018/1673 rahapesu vastu võitlemise kohta kriminaalõiguse abil. – ELT L 284, lk 22-30.

AMLD4 ja selles sätestatud rahapesuvastased üldpõhimõtted olid aluseks uue RahaPTS tervikteksti loomisele, mis jõustus 26. oktoobril 2017. a ja mida on täiendatud AMLD5 ja AMLD6 sätete ülevõtmisega riigisisesesse õigusesse. Lisaks peavad krediidiasutused oma tegevuses arvestama FATF soovitusi[39], Euroopa Pangandusjärelevalve (edaspidi ka EBA) jt asjakohaseid juhiseid, eelkõige EBA suuniseid riskitegurite kohta (viimati uuendatud märtsis 2021)[40] ning riskipõhise järelevalve suunised[41]. Eestis annab Finantsinspektsioon (edaspidi *FI*) välja soovitusliku iseloomuga juhendeid finantssektori tegevust reguleerivate õigusaktide selgitamiseks või finantsjärelevalve subjektide suunamiseks vastavalt finantsinspektsiooni seaduse[42] (edaspidi FIS) § 57 lõikele 1. Kuigi FI juhendid on soovitusliku iseloomuga, kehtib nende puhul *täidan või selgitan* põhimõte, mille kohaselt peab järelevalvesubjekt vajadusel suutma põhjendada, miks ta mõnda juhendi punkti ei rakenda või teeb seda osaliselt. Seega on soovituslike standardite ja juhendite täitmine krediidiasutuste poolt enamasti üksnes näiliselt vabatahtlik.[43] Finantsinspektsiooni soovituslikus juhendis pole kohustatud isikute omavahelist infovahetust rahapesu tõkestamise eesmärgil põhjalikult käsitletud. Üsna üldsõnaliselt on selgitatud kohustusi seoses kontsernisisese rahapesuvastase teabevahetusega (p 3.9.3.4.), isikuandmete kaitse ja andmete konfidentsiaalsusega (p 3.9.3.5.) ning kõrge riskiga või kolmanda riigi respondentasutustega seotud infovahetusega (p 4.9.6.7.).[44]

---

[39] Riigikohtu lahendi 3-20-332/39 järgi on FATF-i juhised sätestatud küll soovitustena, kuid nende sisuline täitmine on kõigile maailma riikidele kohustuslik. Kui riik ei täida vastavaid soovitusi, ohustab teda nn halli nimekirja panemine või rahvusvahelistest organisatsioonidest väljaheitmine. Vt RKHKo 24.03.2022, 3-20-332/39, p 6.3.

[40] European Banking Authority (EBA). Suunised, mis on koostatud direktiivi (EL) 2015/849 artikli 17 ja artikli 18 lõike 4 alusel, milles käsitletakse kliendi suhtes rakendatavaid hoolsusmeetmeid ning tegureid, mida krediidi- ja finantseerimisasutused peaksid arvestama, kui hindavad üksikute ärisuhete ja juhutehingute rahapesu ja terrorismi rahastamise riski (edaspidi „rahapesu ja terrorismi rahastamise riskitegurite suunised“), millega tunnistatakse kehtetuks ja asendatakse suunised JC/2017/37. EBA/GL/2021/02, 1. märts 2021. - https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20ML-TF%20risk%20factors%20%28revised%29%202021-02/Translations/1016926/Guidelines%20ML%20TF%20Risk%20Factors_ET.pdf (14.09.2021).

[41] European Supervisory Authorities (ESAs). Joint Guidelines on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis. The Risk-Based Supervision Guidelines. Joint Guidelines. ESAs 2016 72, 16 November 2016. - https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1663861/7159758d-8337-499e-8b12-e34911f9b4b6/Joint%20Guidelines%20on%20Risk-Based%20Supervision%20%28ESAS%202016%2072%29.pdf?retry=1 (14.09.2021).

[42] Finantsinspektsiooni seadus. – RT I, 29.03.2022, 8.

[43] Vt täiendavat analüüsi soovituslike juhendite vabatahtliku rakendamise osas: Jäärats, E. Pankade diskretsiooniõigus tunne-oma-klienti põhimõtte täitmisel ning selle negatiivsed tagajärjed. Uurimistöö. Tallinn: TÜ õigusteaduskond 2019, lk 13.

[44] Finantsinspektsioon. Finantsinspektsiooni soovituslik juhend „Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks“.

Rahapesu on esinenud aastasadu, kuid kriminoloogias on rahapesu eraldiseisva instituudina ja erikäsitlusena üsna hiline nähtus.[45] Rahapesu koosseis on sätestatud karistusseadustiku[46] §-s 394. RKKK lahendi 3-1-1-97-10 p 24 järgi tuleb rahapesu koosseisu tõlgendamisel lähtuda RahaPTS §-st 1, mille kohaselt on RahaPTS eesmärk tõkestada Eesti Vabariigi rahandussüsteemi ning majandusruumi kasutamist rahapesuks ja terrorismi rahastamiseks. Rahapesu koosseisu eesmärgiks on seega kaitsta riigi rahandus- ja majandussüsteemi kuritegelikku päritolu rahavoogude negatiivse mõju eest, samuti pärssida kuritegelike struktuuride mõjuvõimu kasvu.[47] Rahapesuga seotud rahavoogudel on majandussüsteemile destabiliseeriv mõju, mis kahjustab riigi reputatsiooni ning mõjutab seeläbi kõiki riigis tegutsevaid ettevõtjaid, eelkõige finantssektoris tegutsevaid ettevõtjaid.[48] Käesoleva magistritöö seisukohalt on olulised rahapesualaste süütegudega (vt KarS §-d 394-394[1]) seotud selgitused karistusseadustiku kommenteeritud väljaandes[49], kuna need aitavad määratleda rahapesu mõistet ja rahapesuga seotud eelkuritegusid ning seeläbi sisustada krediidiasutuste omavahelist infovahetust kuriteokahtlusega tehingute osas, mida võimaldab RahaPTS § 51 lõige 5 (vt põhjalikumat käsitlust 3. peatükist).

Käesolevas alapunktis esitati lühidalt üldine rahapesu tõkestamise õigusraamistik, rõhutades seejuures nüansse, mis puudutavad rahapesu tõkestamise eesmärgil toimuvat teabevahetust nii krediidiasutuste kui ka järelevalveasutuste vahel. Edaspidises analüüsis keskendub magistritöö autor nende sätete analüüsimisele liidu õiguses ja riigisiseses õiguses, mis reguleerivad krediidiasutuste omavahelist infovahetust rahapesu tõkestamise eesmärgil. Järgmises alapunktis

Kehtestatud Finantsinspektsiooni juhatuse 26.11.2018. a otsusega nr 1.1-7/172, p 3.9.3.4. ja p 3.9.3.5., lk 22; p 4.9.6.7., lk 66. - https://www.fi.ee/sites/default/files/2018-11/FI_AML_Soovituslik_juhend.pdf (14.09.2021).

[45] Rahapesu vastu võitlemise alguseks võib pidada pangasaladuse seaduse (ingl *Banking Secrecy Act*) kehtestamist USA-s 1970. aastal, millega pandi füüsilistele isikutele, krediidiasutustele ja muudele finantsasutustele mh andmete säilitamise ja sularaha tehingute raporteerimise kohustus. Pangasaladuse seaduse vastuvõtmist USA-s peetakse ajalooliselt märgiliseks, kuna sellega anti „pangaraamatud" võimude kätte, kui see peaks olema vajalik avalike ülesannete täitmiseks. 1986. aastal võeti USA-s vastu rahapesu kontrolli seadus (ingl *Money Laundering Control Act*), millega muudeti rahapesu föderaalkuriteoks. Vt Mäeker/Nõmm (2020) (viide 14), lk 663; vt ka FinCen. History of Anti-Money Laundering Laws. U.S. Treasury, The Financial Crimes Enforcement Network. - https://www.fincen.gov/history-anti-money-laundering-laws#:~:text=The%20BSA%20was%20established%20in,tools%20to%20combat%20money%20laundering (08.03.2022).

[46] Karistusseadustik. – RT I, 21.05.2021, 9.

[47] RKKKm 11.04.2011, 3-1-1-97-10, p 24.

[48] Mäeker/Nõmm (2020) (viide 14), lk 664.

[49] Tibar, I. (koost.). KarS §-d 394-394[1], lk 1114-1127. – Sootak, J., Pikamäe, P. (koost). Karistusseadustik. Kommenteeritud väljaanne. 5., täiend. ja ümbertööt. vlj. Tallinn: Juura 2021.

käsitletakse krediidiasutuste omavahelise infovahetuse õiguslikke aluseid ja ulatust ning nendega seotud probleemkohti.

1.2 Krediidiasutuste omavahelise infovahetuse õiguslikud alused

Rahapesuvastaste direktiivide põhimõtted on RahaPTS kaudu riigisisesesse õigusesse üle võetud. Krediidiasutuste omavahelist infovahetust rahapesu tõkestamise eesmärgil reguleerivad peamiselt kaks RahaPTS paragrahvi – RahaPTS § 16 (*Koostöö ja infovahetus*) ning RahaPTS § 51 (*Teate konfidentsiaalsus*, eelkõige RahaPTS 51 lõige 5). Peamine krediidiasutuste omavahelise infovahetuse õiguslik alus riigisiseses õiguses on RahaPTS § 16 lõige 1, mille kohaselt võivad kohustatud isikud (mh krediidiasutused) teha rahapesu tõkestamisel omavahel koostööd, sh edastada või vahetada teavet ning vastata päringutele mõistliku aja jooksul, järgides õigusaktidest tulenevaid kohustusi ja piiranguid. Krediidiasutuste omavahelise infovahetuse kohustuste ja piirangute puhul on ennekõike silmas peetud pangasaladuse hoidmise kohustust ja isikuandmete kaitsmise vajadust ning nendest lähtuvaid piiranguid.

Pangasaladust reguleerib krediidiasutuste seaduse § 88, mis mh sätestab pangasaladuse mõiste (KAS § 88 lg 1 ja 2), pangasaladuse kolmandatele isikutele avaldamise tingimused (KAS § 88 lg 3 jj) ning pangasaladuse tähtajatu hoidmise kohustuse (KAS § 88 lg 7). Pangasaladusena käsitatakse KAS § 88 lõike 1 mõistes kõiki andmeid ja hinnanguid, mis on krediidiasutusele teatavaks saanud tema või teise krediidiasutuse kliendi kohta. Pangasaladusena on seega käsitatavad ka klientide kohta kogutud isikuandmed, milleks on igasugune teave tuvastatud või tuvastatava füüsilise isiku (edaspidi ka andmesubjekt) kohta üldmääruse artikli 4 punkti 1 tähenduses. Üldjuhul laieneb krediidiasutustele avaldatud andmetele pangasaladuse tähtajatu hoidmise kohustus ja vastutus (KAS § 88 lg 7), mistõttu võivad krediidiasutused avaldada klienti puudutava pangasaladuse kolmandatele isikutele üksnes piiratud juhtudel ning kooskõlas KAS § 88 sätetega. Pangasaladuse avaldamise piiranguid seoses krediidiasutuste omavahelise infovahetusega on analüüsitud alapunktis 1.3.1.

Isikuandmete kaitse perspektiivist seab krediidiasutuste omavahelisele infovahetusele kohustusi ja piiranguid siseriiklikus õiguses otsekohalduv Euroopa Liidu isikuandmete kaitse üldmäärus (edaspidi ka IKÜM või üldmäärus), mis muuhulgas sätestab isikuandmete töötlemise põhimõtted ja õiguslikud alused. Liikmesriigid võivad täpsustada üldmääruse sätete kohaldamist siseriiklikus õiguses, kui isikuandmete töötlemine on vajalik juriidilise kohustuse täitmiseks (IKÜM art 6 lg 1

p c) või avalikes huvides oleva ülesande täitmiseks (IKÜM art 6 lg 1 p e). Selleks võivad liikmesriigid määrata kindlaks isikuandmete töötlemise konkreetsed nõuded ja teised meetmed, et tagada isikuandmete seaduslik ja õiglane töötlemine (IKÜM art 6 lg 2). Kuigi rahapesu tõkestamist käsitatakse ennekõike avaliku huvi küsimusena üldmääruse ja RahaPTS mõistes, rõhutavad mõlemad regulatsioonid isikuandmete kaitsmise vajadust (IKÜM pp 19 ja art 6 lg 1 p e, RahaPTS § 48 lg 2). RahaPTS rakendamisel kogutud isikuandmeid on seetõttu lubatud töödelda üksnes rahapesu tõkestamise eesmärgil, mitte turunduslikel ega muudel eesmärkidel (RahaPTS § 48 lg 2). Isikuandmete kaitse perspektiivist on piirangute eesmärgiks ennekõike vältida krediidiasutuste infovahetuse käigus isikuandmete töötlemist õigusliku aluseta või ulatuses, mis pole proportsionaalne taotletava õiguspärase eesmärgiga (IKÜM art 6 lg 3).

Krediidiasutuste omavahelist infovahetust rahapesu tõkestamise eesmärgil reguleerib lisaks RahaPTS § 51 lõige 5, mille kohaselt võivad krediidi- ja finantseerimisasutused omavahel vahetada teavet kõrge riskiga klientide ja kuriteokahtlusega tehingute kohta rahapesu või terrorismi rahastamise tõkestamise eesmärgil. Siinkohal tuleb märkida, et RahaPTS § 51 lõige 5 on krediidiasutuste infovahetuse õigusliku alusena riigisiseses õiguses üsna raskesti sisustatav ja mitmeti mõistetav säte. Küsimusi tekitab nii sätte asukoht (RahaPTS 5. peatükk), infovahetuse üldnormi (RahaPTS § 16 lg 1) ja erinormi (RahaPTS § 51 lg 5) vahekord kui ka sättes sisalduvad määratlemata õigusmõisted (sh kõrge riskiga klient, kuriteokahtlusega tehing), mida on analüüsitud magistritöö 3. peatükis. Lähtudes käesoleva magistritöö teemast, taandub lõppkokkuvõttes kõik küsimusele, millisel õiguslikul alusel ja millises ulatuses võivad krediidiasutused isikuandmeid töödelda omavahelise infovahetuse käigus rahapesu tõkestamise eesmärgil, sh kõrgema riskiga klientide puhul ning kuriteokahtlusega tehingute tuvastamisel.

Käesoleva alapunkti eesmärgiks oli välja tuua peamised sätted siseriiklikus õiguses, mis reguleerivad krediidiasutuste omavahelist infovahetust rahapesu tõkestamise eesmärgil, samuti viidata probleemkohtadele, mida töös põhjalikumalt analüüsitakse. Järgnevas alapeatükis käsitletakse kahte olulist piirangut, millega krediidiasutused peavad omavahelises infovahetuses arvestama – pangasaladuse hoidmise kohustus ning RAB teate konfidentsiaalsus rahapesu kahtluse korral. Isikuandmete kaitse õiguslikku raamistikku ning isikuandmete töötlemise õiguslikke aluseid ja ulatust analüüsitakse põhjalikumalt järgmises peatükis.

1.3 Krediidiasutuste omavahelise infovahetuse piirangud

1.3.1 Pangasaladuse avaldamise piirangud

Krediidiasutuste tegevus on tugeva avalik-õigusliku regulatsiooniga ärivaldkond kogu maailmas. Euroopa Liidu liikmesriikidel on keelatud kasutada pangasaladuse regulatsiooni rahapesu tõkestamise meetmetest kõrvalehoidmiseks ning kehtestada võib üksnes rahapesuvastastest direktiividest rangemaid sätteid.[50] R. Raa ja K. Siibaku arvates seisneb pangasaladuse idee selles, et iga üksikisik on oma varanduslike suhete peremees, mis üldjuhul tähendab seda, et kellelgi pole õigust isiku varanduslike suhete kohta midagi põhjalikumalt teada saada ega tema nõusolekuta või õigusliku aluseta nende kohta midagi välja uurida. Vastav põhimõte jääb kehtima ka olukordades, kus isik korraldab oma varanduslikke suhteid panga kaasabil.[51] Kui vaadelda pangasaladusena käsitletavate andmete saladuses hoidmise kohustust krediidiasutuse poolt kui ühte isiku põhiõigust, on igakordsel isiku kohta käivate andmete avaldamisel tegemist selle isiku põhiõiguse riivega.[52]

Krediidiasutuse usaldusväärsuse tagab ühelt poolt teadmine, et klienti puudutavad andmed on pangasaladusena kindlalt kaitstud, ning teiselt poolt asjaolu, et krediidiasutus on tarvitusele võtnud meetmed riiklike asutuste omaalgatuslikuks teavitamiseks rahapesu kahtluse tuvastamisel, et hoida panga tegevus võimalikult läbipaistvana. Samas võib krediidiasutuste äri teatud määral pidurdada õigusaktidest tulenev liigne riigipoolne surve pangasaladuse avaldamiseks ning rahapesureeglite rakendamisele kaasaaitamiseks.[53] Tõenäoliselt suureneb ka edaspidi erinevate järelevalve- ja õiguskaitseorganite vaheline koostöö ja teabevahetuse nii riigisiseselt kui ka riikide üleselt, mis veelgi suurendab sekkumist finantsasutuste poolt kaitstavasse pangasaladusse.

Pangasaladuse tähtajatu hoidmise kohustus ning pangasaladuse kolmandale isikule avaldamise tingimused on sätestatud KAS §-s 88. KAS § 88 lõike 3 järgi on krediidiasutusel õiguse avaldada klienti puudutav pangasaladus kolmandale isikule, kui pangasaladuse avaldamise õigus või kohustus tuleneb vastavas paragrahvis sätestatust (p l), klient on andnud pangasaladuse avaldamiseks nõusoleku (p 2) või pangasaladuse avaldamine on vajalik kliendi osalusel sõlmitud

[50] Liivat, E. Pangasaladuse kontseptsiooni muutumine ajas. Bakalaureusetöö. Magistritöö. Tallinn: TÜ õigusteaduskond 2013, lk 12-13.
[51] Raa, R., Siibak, K. Pangasaladus. – Juridica 2002/3, lk 172.
[52] Liivat, E. (viide 50), lk 16.
[53] Liivat, E. (viide 50), lk 24-25.

lepingu täitmiseks või kliendi taotluse alusel algatatud lepingu sõlmimisele eelnevate meetmete võtmiseks (p 3). Üldjuhul ei lähtu krediidiasutuste õigus avaldada pangasaladus teistele krediidiasutustele rahapesu tõkestamise eesmärgil kliendi nõusolekust (KAS § 88 lg 3 p 2) ega lepingu täitmise või lepingu sõlmimisele eelnevate meetmete võtmise vajadusest (KAS § 88 lg 3 p 3). Enamusel juhtudel tuleneb krediidiasutuse õigus avaldada klienti puudutav pangasaladus kolmandale isikule rahapesu tõkestamise eesmärgil paragrahvis 88 sätestatust (KAS § 88 lg 3 p 1). Vastavat seisukohta toetavad KAS § 88 lisatud viited krediidiasutuste infovahetust puudutavatele sätetele RahaPTS-is (sh RahaPTS § 16 ja § 51).

Nimelt võimaldab KAS § 88 lõige 5^1 krediidiasutusel kirjalikus või kirjalikku taasesitamist võimaldavas vormis esitatud järelepärimise vastusena avaldada pangasaladuse järgmistele isikutele:

- oma emaettevõtjale, kes vajab pangasaladuseks olevaid andmeid konsolideeritud aruannete koostamiseks (p 1);
- krediidiasutusega samasse konsolideerimisgruppi kuuluvale finantseerimisasutusele või teisele krediidiasutusele, kes vajab andmeid kliendi maksekohustuste täitmise ajaloo kohta krediidiriski kapitalinõuete arvutamiseks ja vastutustundliku laenamise põhimõtte rakendamiseks (p 2);
- krediidiasutusega samasse konsolideerimisgruppi kuuluvale ettevõtjale, kes vajab pangasaladuseks olevaid andmeid RahaPTS-is sätestatud hoolsusmeetmete kohaldamiseks, ning teisele isikule RahaPTS § 51 rakendamiseks vajalikus ulatuses (p 3);
- RahaPTS-is nimetatud kohustatud isikutele sama seaduse §-s 16 sätestatud alustel ja korras (p 4).

Krediidiasutuste infovahetuse mõttes on olulised eelkõige kaks viimast punkti, mis võimaldavad pangasaladuse avaldada kolmandale isikule ka väljaspool krediidiasutusega seotud konsolideerimisgruppi. Siinkohal tuleb rõhutada, et RahaPTS § 16 lõige 1 võimaldab rahapesu tõkestamise eesmärgil omavahel koostööd teha ja infot vahetada kõigil RahaPTS §-s 2 nimetatud kohustatud isikutel. Samas RahaPTS § 51 lõige 5 võimaldab üksnes krediidi- ja finantseerimisasutustel vahetada omavahel teavet kõrge riskiga klientide ja kuriteokahtlusega tehingute kohta rahapesu tõkestamise eesmärgil. Seega on teatud rahapesu tõkestamise juhtudel kohustatud isikute ring, kellega võib pangasaladusega kaitstud teavet vahetada, oluliselt piiratum.

1.3.2 Teate konfidentsiaalsus rahapesu kahtluse korral

Teine oluline krediidiasutuste omavahelise infovahetuse piirang puudutab rahapesu ja terrorismi rahastamise kahtlusest teavitamise kohustust. RahaPTS § 49 lõike 1 kohaselt peab krediidiasutus viivitamata teavitama Rahapesu Andmebürood (edaspidi ka *RAB*) majandustegevuse käigus tuvastatud tegevustest või asjaoludest, mille tunnused osutavad kuritegelikust tegevusest saadud tulu kasutamisele, terrorismi rahastamisele või sellega seotud kuritegude toimepanemisele või sellise tegevuse katsetele või mille puhul tal on kahtlus või ta teab, et tegemist on rahapesu või terrorismi rahastamisega või sellega seotud kuritegude toimepanemisega. Seejuures keelab RahaPTS § 51 lõige 1 krediidiasutusel, selle struktuuriüksusel, juhtorgani liikmel ja töötajal teavitada isikut, selle isiku tegelikku kasusaajat, esindajat või kolmandat isikut nende kohta RAB-ile esitatud teatest, sellise teate esitamise plaanist või esitamise toimumisest, samuti RAB ettekirjutusest või kriminaalmenetluse alustamisest. RahaPTS § 51 lõike 2 kohaselt ei rakendata vastavat keeldu mh teabe esitamisel pädevatele järelevalveasutustele ja õiguskaitseasutustele, samasse kontserni kuuluvate krediidiasutuste ja finantseerimisasutuste omavahelisele teabevahetusele, samuti krediidiasutuse või finantseerimisasutusega samasse kontserni kuuluvatele asutustele ja filiaalidele, kui kontsernis kohaldatakse kontserniüleseid protseduurireegleid ja põhimõtteid. Teabevahetuse keeldu ei rakendata seaduses sätestatud juhtudel ka olukorras, kus see puudutab sama isikut ja sama tehingut, milles osaleb kaks või enam kohustatud isikut, kes on mh krediidiasutused või finantseerimisasutused (RahaPTS § 51 lg 3). Järelikult peavad krediidiasutused üldjuhul hoidma konfidentsiaalsena teavet kuriteokahtlusega tehingute kohta ning teavitama sellistest tehingutest pädevaid järelevalveasutusi ja õiguskaitseasutusi. Kontsernisiseselt on krediidiasutuste infovahetus rahapesu tõkestamise eesmärgil aga oluliselt vähem piiratud, eriti juhul kui infovahetus toimub samasse kontserni kuuluvate krediidiasutuste ja finantseerimisasutuste vahel. Nii pangasaladuse avaldamist võimaldavad sätted (KAS § 88 lg 5^1) kui ka RAB teate konfidentsiaalsuse nõudest möödaminekut võimaldavad sätted (RahaPTS § 51 lg 2 ja 3) viitavad asjaolule, et krediidiasutuste infovahetuse ulatus pangasaladuse ja kuriteokahtlusega teabe avaldamisel kolmandale isikule sõltub olulisel määral sellest, kas tegemist on krediidiasutusega samasse kontserni kuuluva kolmanda isikuga (sh krediidiasutusega) ning kas rakendatakse kontserniüleseid protseduurireegleid ja põhimõtteid. FI soovituslik juhend rõhutab, et kontserni puhul peavad kontserniülesed protseduurireeglid hõlmama mh meetmeid ja korda kontsernisisese rahapesu ja terrorismi rahastamise tõkestamise alase teabe

vahetamiseks. „See hõlmab nii informatsiooni vahetamist hoolsusmeetmetega ning rahapesu ja terrorismi rahastamise riski juhtimisega seoses, hõlmates nii kahtlaste ja ebaharilike tehingute ning asjaolude analüüsi kui ka rahapesu andmebüroodele esitatud teadet ennast ja selle aluseks olevaid dokumente.“[54]

Teisalt võimaldab RahaPTS § 51 lõige 5 krediidiasutustel ja finantseerimisasutustel vahetada omavahel teavet kõrge riskiga klientide ja kuriteokahtlusega tehingute kohta rahapesu tõkestamise eesmärgil ning seda isegi juhul, kui krediidiasutused ja finantseerimisasutused ei kuulu samasse kontserni. Vastava sätte alusel peaks teabevahetuse ulatus piirduma üksnes kõrge riskiga klientide ja kuriteokahtlusega tehingutega, kuid neid mõisteid on juba iseenesest keeruline kui mitte võimatu üheselt mõistetavalt sisustada. Nimelt sõltub kõrge riskiga klientide määratlemine suuresti krediidiasutuse sisestest protseduurireeglitest ja riskihinnangutest. Kuriteokahtlusega tehingu mõiste sisustamine on aga keeruline juba seetõttu, et rahapesu kuriteo toimumise eelduseks on muu kuriteo ehk eelkuriteo toimepanemine.[55] Seejuures võib eelkuriteoks olla iga KarS eriosas sätestatud kuritegu[56], millest on saadud rahapesu objekt[57] ehk kuritegeliku tegevuse tulemusel saadud vara (st kriminaaltulu)[58].

S.-H. Evestus leiab, et seadusandja mõistab RahaPTS rahapesu mõistes sätestatud *kuritegeliku tegevuse* all eelkuriteo toimepanemist nii täideviija kui ka osavõtjana, jättes samas kuritegeliku tegevuse mõiste selgelt avamata.[59] Laialt määratletud kuritegeliku tegevuse mõiste ning sellega seotud eelkuritegude ring muudab krediidiasutuste tegevuse kuriteokahtlusega tehingu mõiste sisustamisel, vastavate tehingute tuvastamisel, kahtluste kontrollimisel ja põhjendamisel keeruliseks ning ajamahukaks. See võib takistada nii teatamiskohustuse täitmist RahaPTS § 49 lõike 1 alusel kui ka krediidiasutuste omavahelist infovahetust RahaPTS 51 lõike 5 alusel.

RahaPTS § 14 lg 1 p 3 kohaselt peab krediidiasutus kehtestama protseduurireeglid, mis sisaldavad mh metoodikat ja juhendit, kui kohustatud isikul tekib rahapesu ja terrorismi rahastamise kahtlus

[54] Finantsinspektsiooni soovituslik juhend (viide 44), p 3.9.3.4., lk 22.
[55] KarS Komm (2021)/Tibar, I. (viide 49), § 394 komm. 9.1., lk 1116.
[56] Evestus, S.-H. Eelkuriteo sisustamine rahapesukuriteo puhul. Rahapesu mõiste Eesti karistusõiguses. – Juridica 2015/5, lk 363.
[57] Täpsustavalt tuleb mainida, et tänane kohtupraktika seostab rahapesu vaid kriminaaltulu tootvate kuritegudega, mitte rahapesule eelneva kriminaaltulu mittetootva tegevusega (nt dokumendi võltsimine teadmata päritoluga vara õigustamiseks). Vt KarS Komm (2021)/Tibar, I. (viide 49), § 394 komm. 9.2., lk 1117.
[58] KarS Komm (2021)/Tibar, I. (viide 49), § 394 komm. 11, lk 1119.
[59] Evestus, S.-H. (viide 56), lk 360-361.

(edaspidi *rahapesu kahtlus*) või on tegemist ebatavalise tehingu või asjaoluga, samuti RahaPTS §-s 49 sätestatud teatamiskohustuse täitmise juhendit. Rahapesu Andmebüroo „Juhend kahtlaste tehingute tunnuste kohta“[60] annab kohustatud isikutele omakorda juhised RahaPTS § 49 sätestatud teatamiskohustuse täitmiseks. Näiteks põhjendatud rahapesu kahtluse[61] korral tuleb RAB-ile esitada *rahapesu või rahapesuga seotud muu kuriteo kahtlusega teade* (edaspidi *rahapesukahtlusega teade*) ning tehingut teha ega ärisuhet luua ei tohi.[62] Samas peavad krediidiasutused esitama RAB-ile *ebahariliku tehingu teate* või *ebahariliku tegevuse teate*, kui isikult saadud majanduslike või eluliselt usutavate selgitustega pole suudetud ebaharilikku tehingut või tegevust ära põhjendada, kuid tehingut või ärisuhet võib jätkata (v.a. rahapesu kahtluse korral). Kui juhtumi asjaoludest sõltuvalt põhjustavad ebahariliku tegevuse või toimingu tunnused rahapesu kahtluse, siis tuleb esitada rahapesukahtlusega teade.[63]

Kahjuks ei täpsusta RAB juhend, mil määral peab rahapesu kahtlus olema põhjendatud ja/või tõendatud, et käsitleda ebaharilikku tehingu või tegevuse tunnuseid põhjendatud rahapesu kahtlusena, mille tulemusel tekib krediidiasutusel kohustus esitada rahapesukahtlusega teade RAB-ile. Pigem viitab RAB juhend sellele, et kohustatud isikud peavad koostama sisemised protseduurireeglid, kus on mh toodud näiteid erinevate RAB teadete liikide juurde, lähtudes peamistest rahapesu ja terrorismi rahastamise riskidest ja ohtudest konkreetses valdkonnas.[64] Arusaadavalt on seadusandjal ja muudel pädevatel asutustel (sh RAB, FI) üsna keeruline sisustada *rahapesu kahtluse* mõistet ning välja töötada universaalseid indikaatoreid, tüpoloogiaid või rahapesuskeeme, mis oleksid asjakohased ja/või rakendatavad võimalikult suure hulga kohustatud isikute puhul. Vastavalt seadusele ja muudele juhistele peavad krediidiasutused olema ise võimelised lähtuvalt oma tegevusvaldkonna, ärimudeli ja kliendibaasi riskist sisustama rahapesu kahtluse mõistet, tuues näiteid ja põhjendusi, ning looma protseduurid tegutsemiseks põhjendatud rahapesu kahtluse korral (sh RAB teavitamiseks ja infovahetuseks teiste krediidiasutustega).

[60] Rahapesu Andmebüroo. Juhend kahtlaste tehingute tunnuste kohta. Kinnitatud 06.05.2019. https://www.politsei.ee/files/Rahapesu/juhendkahtlastetehingutetunnustekohta.pdf?222a84e8fa (20.01.2021).
[61] RAB juhendi järgi on *rahapesu kahtlus* asjaolud või teadmine, mis viitavad sellele, et tehing või tegevus on suunatud rahapesu toimepanemisele või kuritegelikul teel saadud vara varjamisele ning hoolsusmeetmete rakendamisega ei ole kahtlust kõrvaldatud. Vt RAB juhend (viide 60), p 4, lk 1.
[62] RAB juhend (viide 60), p 16, lk 3-4 ja lk 6.
[63] *Ibid*, p 17-18, lk 4.
[64] RAB juhend (viide 60), p 2, lk 1.

Hoolimata krediidiasutuste sisemistest protseduurireeglitest ja rakendatavatest meetmetest, peaks krediidiasutustele siiski olema üheselt arusaadav:

- kas rahapesukahtlusega teate esitamine on eelduseks, et vahetada teavet teiste krediidiasutustega kuriteokahtlusega tehingute osas;
- kas rahapesukahtlusega teade tuleb esitada enne teiste krediidiasutuste teavitamist kuriteokahtlusega tehingutest või tohib seda teha ka viivitamata pärast krediidiasutuste omavahelist infovahetust;
- kas ebaharilike tehingute ja tegevuste osas toimub krediidiasutuste omavaheline infovahetus samal õiguslikul alusel ja ulatuses, kui kuriteokahtlusega tehingute puhul.

Riigisisesed pädevad asutused peaksid kasutama kogutud teadmisi, kogemusi ja praktikat, et välja töötada võimalikult täpsed juhiseid, mis hõlbustaksid kohustatud isikute tegevust rahapesu tõkestamisel (sh teatamiskohustuse täitmisel ja vabatahtliku infovahetuse korral). Kindlasti on seda juba varasemalt tehtud ning tehakse ka edaspidi, arvestades rahapesu temaatika aktuaalsust. Näiteks on RAB panustanud 2019. aastal Egmont Group'i[65] alustatud projekti „*Conclusions from Large Scale Cross-Border Money Laundering Schemes*", mille eesmärk on ühendada eri riikide rahapesu andmebüroode teadmised ja praktika, et koondada lähenemisviisid piiriüleste rahapesuvoogude võrgustike ja mustrite tuvastamiseks, analüüsida andmeid ning töötada välja indikaatoreid, tüpoloogiaid, näidisjuhtumeid ja muid vahendeid, millega hõlbustada rahapesu tõkestamist.[66] Lisaks rahapesu andmebüroode vahelisele infovahetusele võiks nii seadusandja kui ka järelevalveasutused pöörata suuremat tähelepanu krediidiasutuste omavahelise infovahetuse nõuete ja ulatuse täpsustamisele kas regulatsioonides, nende kommentaarides või eraldiseisvates juhistes. Probleemi aktuaalsust ning vajadust täpsemate juhiste järgi peegeldab ka viimastel aastatel märkimisväärselt kasvanud Euroopa Liidu liikmesriikide vahel piiriülese levitamise teel saadetud teadete ehk XBD-de arv (nt 2017. a 20, 2018. a 1703, 2019. a 4037, 2020. a 7206), mille puhul on RAB leidnud, et riikide info edastamise praktika ja teadete sisukus on ebaühtlane. RAB arvates, mida automatiseeritumalt ja ühtlustatumalt teadete ja spontaanse info vahetamise süsteem

[65] Egmont Group on ülemaailmne organisatsioon, mis pakub organisatsiooni liikmetest rahapesu andmebüroodele platvormi, et vahetada turvaliselt teadmisi ja finantsteavet, et võidelda rahapesu, terrorismi rahastamise ja nendega seotud eelkuritegude vastu. Vt Egmont Group. Organization and Structure. - https://egmontgroup.org/about/organization-and-structure/ (01.03.2022).

[66] Rahapesu Andmebüroo. Aastaraamat 2020. Ülevaade Rahapesu Andmebüroo tegevusest 2020. aastal. RAB: Tallinn 2021. - https://fiu.ee/aastaraamatud-ja-uuringud/aastaraamatud#item-1 (01.03.2021).

Euroopa Liidu liikmesriikide vahel toimib, seda rohkem saab kasu rahapesu tõkestamise süsteem.[67] Kindlasti aitaks sellele eesmärgile kaasa krediidiasutuste omavahelise infovahetuse ühtlustamine ja automatiseerimine.

Eesti suuremad krediidiasutused on selles suunas juba konkreetseid samme astunud. Nimelt ühinesid neli suuremat Eesti krediidiasutust (sh LHV, Swedbank, SEB ja Luminor) 2020. aastal pilootprojektiga *AML Bridge*, mida arendab Eesti finantstehnoloogia ettevõte Salv Technologies OÜ. Tegemist on teabe- ja andmevahetusplatvormiga, mis võimaldab krediidiasutuste omavahelist infovahetust rahapesu tõkestamise eesmärgil kooskõlas kehtivate rahapesu, pangasaladuse ja andmekaitse normidega.[68] Samas leiab käesoleva töö autor, et krediidiasutuste omavahelise infovahetuse konkreetseid nõudeid, ulatust ja meetmeid pole rahvusvahelistes ja riigisisestes regulatsioonides ning neid täiendavates juhiste piisavalt üksikasjalikult kindlaks määratud, kuigi seda võimaldaksid teha üldmääruse artikli 6 lõiked 2 ja 3, mistõttu ei pruugi tänane õigusraamistik tagada isikuandmete seaduslikku ja õiglast töötlemist krediidiasutuste omavahelise infovahetuse käigus rahapesu tõkestamise eesmärgil. Salv Technologies OÜ on samuti välja toonud, et pilootprojekti suurimaks väljakutseks on kliendiandmete kasutamise ulatuse määratlemine ehk millisel määral on isikuandmete töötlemine rangelt vajalik ja proportsionaalne, mistõttu aitaks valdkonnaülesed suunised muuta rahapesu tõkestamise eesmärgil toimuva infovahetuse õigusraamistiku selgemaks.[69]

RahaPTS § 51 lõige 5 on krediidiasutuste omavahelise infovahetuse mõttes võtmetähtsusega säte siseriiklikus õiguses, mille sisustamise osas vajaks krediidiasutused täpsemaid juhiseid kas Rahapesu Andmebüroolt või Andmekaitse Inspektsioonilt (edaspidi ka *AKI*). Lisaks eelnevale oleksid täiendavad RAB või AKI juhised selguse loomisel abiks sellistes olukordades, mil põhjendatud rahapesu kahtlus osutub nt RAB-ile edastatud teabe analüüsi ja kontrolli tulemusel põhjendamatuks (vt RahaPTS § 54 lg 3) ning peatatud tehing teostatakse tavapärasel viisil. Kas sellisel juhul tekib vastutaval töötlejal kohustus teavitada kõiki infovahetuses osalenud krediidiasutusi põhjendamata rahapesu kahtlusest ning kohustus taastada andmesubjekti esialgne riskiprofiil (v.a muu mõjuva põhjuse olemasolul, mille tõttu käsitatakse andmesubjekti ka edaspidi

[67] RAB aastaraamat 2020 (viide 66), lk 12 ja 21.
[68] Salv AML Bridge (viide 4), lk 5-6.
[69] *Ibid*, lk 8.

kõrge riskiga kliendina)? Kahjuks puuduvad kehtivates regulatsioonides, nende kommentaarides ning muudes juhistes selgitused, kuidas peaksid krediidiasutused taolistes olukordades tegutsema.

Krediidiasutuste infovahetust kõrgema riskiga klientide ning kuriteokahtlusega tehingute osas on põhjalikumalt käsitletud magistritöö 3. peatükis. Järgnevalt on analüüsitud isikuandmete töötlemisele kohalduvat regulatsiooni (sh andmetöötluse põhimõtteid, õiguslikke aluseid ja ulatust) seoses krediidiasutuste omavahelise infovahetusega rahapesu tõkestamise eesmärgil.

2 ISIKUANDMETE TÖÖTLEMISELE KOHALDUV REGULATSIOON SEOSES KREDIIDIASUTUSTE OMAVAHELISE INFOVAHETUSEGA RAHAPESU TÕKESTAMISE EESMÄRGIL

2.1 Isikuandmete kaitse õiguslik raamistik

Alates veebipõhise kaubanduse algusest 1990ndatel on andmetöötlus ettevõtete ja eraisikute vahelistes suhetes märkimisväärselt kasvanud ning riigi osakaal isikuandmete töötlemisel kahanenud.[70] Erasektori ja avaliku sektori suurem suutlikkus andmeid ulatuslikult koguda ja töödelda on tekitanud olulisi ja keerukaid probleeme, mis asetavad privaatsusküsimused kõikjal maailmas üha enam avaliku arutelu keskmesse. Samas leiavad Bogdanov jt, et oleme küll teadlikumad digitaalse teabega seotud riskidest ja selle mõjust isikuandmete töötlemisele, kuid vähesed on teadmised privaatsuskaitse tehnoloogiatest ja nende rakendamisest ning era- ja avalikus sektoris süsteemide talitluse kavandamisest viisil, et töödeldav andmehulk oleks võimalikult väike ning kataks vaid eesmärgi saavutamiseks vajaliku.[71]

T. Ilusa arvates rõhutatakse Euroopa andmekaitseõiguses eelkõige üksikisiku privaatsuse kaitse vajadust, kuna privaatsust peetakse üheks põhiliseks inimõiguseks, samaväärseks õigustega eneseteostusele, mõttevabadusele ning sõnavabadusele.[72] Teisalt väärtustavad inimesed kogu maailmas üha enam oma andmete privaatsust ja turvalisust (sh see mõjutab nende tarbimisotsuseid ja veebikäitumist), mistõttu ei piirdu nõudlus isikuandmete kaitse järele üksnes Euroopa Liiduga.[73] Tänaseks on üldmäärus muutnud Euroopa-stiilis privaatsuse kaitse ülemaailmse turunormiks.[74]

[70] Tikk, E. Informatsioonilise enesemääratlemise rahvusvahelis-õiguslik raamistik, sisustamine Eesti õiguses ja selle praktilisest kohaldamisest veebikeskkonnas. Tartu: Tartu Ülikool 2004, lk 24.
[71] Bogdanov, D., Siil, T. Infotehnoloogilised võimalused põhiõiguste kaitsel. – Juridica 2020/8, lk 474.
[72] Ilus, T. Isikuandmete kaitse olemus ja arengusuunad. – Juridica 2002/VII, lk 442.
[73] Euroopa Komisjon. Komisjoni teatis Euroopa Parlamendile ja Nõukogule. Andmekaitse kodanike võimestajana ja ELi valmistumine digiüleminekuks – isikuandmete kaitse üldmääruse kohaldamise kaks esimest aastat. COM(2020) 264 final. Brüssel, 24.6.2020, lk 2-3. - https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52020DC0264&from=EN (15.02.2021).
[74] Hartzog, W., Richards, N. Privacy's Constitutional Moment and the Limits of Data Protection. – Boston College Law Review 2020/61 (5), lk 1690.

Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni[75] (edaspidi ka *EIÕK*) artiklist 8 tulenev privaatsusõiguse kaitse on andmekaitsereeglite põhiline lähtekoht.[76] Euroopa Liidu põhiõiguste harta artikkel 8 lõige 1 ja Euroopa Liidu toimimise lepingu (konsolideeritud versioon 2016)[77] artikkel 16 lõige 1 sätestavad, et igaühel on õigus oma isikuandmete kaitsele. Isikuandmete kaitse põhiõiguslikku olemust rõhutab ka isikuandmete kaitse üldmäärus[78] kui keskne isikuandmete kaitset reguleeriv õigusakt Euroopa Liidus. Eesti Vabariigi põhiseaduse[79] (edaspidi ka *PS*) mõttes kuulub isikuandmete kaitse PS § 26 kohaldumisalasse, mis käsitleb perekonna- ja eraelu puutumatust.[80] Õigust isikuandmete kaitsele on tunnustanud nii Euroopa Inimõiguste Kohus[81], Euroopa Kohus[82] kui ka Riigikohus[83] mitmetes oma lahendites.

Andmekaitsereeglid peavad tagama, et igasugune isikuandmete töötlemine oleks seaduslik ja õiglane (IKÜM pp 39), kuna isikuandmete töötlemisega võidakse sekkuda andmesubjekti õigusesse eraelu puutumatuse kaitsele.[84] Samas pole õigus isikuandmete kaitsele ega eraelu austamisele absoluutne õigus, vaid seda tuleb tasakaalustada ja kooskõlastada muude õigustatud huvide ja õigustega, kas siis teiste inimeste huvidega (erahuvid) või kogu ühiskonna huvidega (avalikud huvid).[85] Andmekaitse Inspektsiooni koostatud isikuandmete töötleja üldjuhendi järgi võib ühe inimese õigus eraelule põrkuda teise inimese sõna- ja teabevabadusega, eneseteostusvabadusega ja ettevõtlusvabadusega, mistõttu tuleb põhiõigusi konkreetses olukorras

---

[75] Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2010, 14, 54.

[76] Seejuures leiab T. Ilus, et privaatsus on osutunud ammendavalt defineerimatuks mõisteks ning EIÕK artikli 8 kohaldamise praktika järgi pole vastava sätte sisu ühesel määratletav. Vt Ilus, T. Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste Kohtu lahendite valguses. – Juridica 2005/VIII, lk 520.

[77] Euroopa Liidu toimimise lepingu konsolideeritud versioon. – ELT C 202, 07.06.2016, lk 55.

[78] Üldmääruse põhjenduspunkti 1 kohaselt on füüsiliste isikute kaitse isikuandmete töötlemisel põhiõigus.

[79] Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.

[80] Jaanimägi, K. (koost.). PS § 26 komm. 24. – Madise, Ü. (toim) jt. Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne. Komm vlj. Tallinn: Juura 2020. – https://pohiseadus.ee/ (01.10.2022).

[81] EIK on liidetud kohtuasjades 30562/04 ja 30566/04 rõhutanud isikuandmete kaitse fundamentaalset tähtsust era- ja perekonnaelu austamise tagamisel. Vt Liidetud kohtuasjad EIKo 30562/04 ja 30566/04, *S. and Marper v. the United Kingdom*, p 103 ja p 125.

[82] EK rõhutab liidetud kohtuasjades C-293/12 ja C-594/12 põhiõiguste harta artiklis 8 ette nähtud isikuandmete kaitse põhiõiguse olemust. Vt liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd (C-293/12) vs Minister for Communications, Marine and Natural Resources jtn ning Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl* jt, ECLI:EU:C:2014:238, p 36 ja 40.

[83] Riigikohus on 2016. a lahendis 3-3-1-84-15 rõhutanud, et füüsiliste isikute kaitse isikuandmete töötlemisel on käsitatav põhiõigusena, viidates seejuures EL põhiõiguste harta artikli 8 lõikele 1. Vt RKHKo 10.06.2016, 3-3-1-84-15, p 21.

[84] Euroopa andmekaitseõiguse käsiraamat. 2018. aasta väljaanne. Luxembourg: Euroopa Liidu Väljaannete Talitus 2020, lk 38. - https://www.echr.coe.int/Documents/Handbook_data_protection_EST.pdf (15.01.2022).

[85] Euroopa andmekaitseõiguse käsiraamat (viide 84), lk 39.

kaaluda.[86] EL õiguskorras on põhiõiguste hartaga kaitstud põhiõiguste (sh isikuandmete kaitse) piiramine seaduslik üksnes juhul, kui see on kooskõlas õigusaktidega; arvestatakse asjaomase õiguse olemust; kohaldatakse proportsionaalsuse põhimõtet, see on vajalik ja taotletakse ELi tunnustatud üldist huvi pakkuvaid eesmärke või on vajadus kaitsta teiste isikute õigusi ja vabadusi.[87] Üldmääruse artikli 23 lõikes 1 on loetletud üldhuvi eesmärgid, mille puhul peetakse üksikisikute õiguste piiramist õiguspäraseks, kui selline piirang arvestab põhiõiguste ja -vabaduste (sh isikuandmete kaitse) olemust ning on vajalik ja proportsionaalne. Üldhuvi eesmärkide loetelus on mh riigi julgeolek ja riigikaitse; avalik julgeolek; süütegude tõkestamine, uurimine, avastamine; liidu või liikmesriigi majanduslik või finantshuvi; rahvatervis ja sotsiaalkindlustus jms.[88] Rahapesu tõkestamine lähtub avaliku huvi eesmärgist (s.o süütegude ennetamine ja avastamine), mistõttu võib sekkumine üksikisiku põhiõigustesse olla õiguspärane, kui krediidiasutused töötlevad isikuandmeid rahapesu tõkestamise eesmärgil.

2.2 Isikuandmete töötlemisega seotud mõisted ja põhimõtted üldmääruses

Neljanda rahapesuvastase direktiivi 2015/849 (edaspidi *AMLD4*) kehtiva redaktsiooni artikli 41 lõike 1 järgi kohaldatakse AMLD4 raames toimuvale isikuandmete töötlemisele üldmäärust ning määrust (EL) 2018/1725[89]. Üldmääruse artikli 4 punkti 1 kohaselt on isikuandmeteks igasugune teave tuvastatud või tuvastatava füüsilise isiku (andmesubjekti) kohta. Tuvastatav füüsiline isik on sama punkti järgi isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal.

RahaPTS-is reguleerivad krediidiasutuste omavahelise infovahetust rahapesu tõkestamise eesmärgil peamiselt RahaPTS § 16 lõiked 1 ja 2 ning RahaPTS § 51 lõige 5, mis võimaldavad krediidiasutustel vahetada omavahel teavet mh kliendi või juhutehingus osaleva isiku

[86] Andmekaitse Inspektsioon. Isikuandmete töötleja üldjuhend. Kinnitatud 31.05.2018, muudetud 28.09.2018 ja 19.03.2019, lk 7. - https://www.aki.ee/sites/default/files/dokumendid/isikuandmete_tootleja_uldjuhend.pdf (21.10.2021).
[87] Euroopa andmekaitseõiguse käsiraamat (viide 84), lk 37.
[88] Liidetud kohtuasjad EIKo nr 30562/04 ja nr 30566/04, *S. ja Marper vs. Ühendkuningriik*, 08.12.2008, p 125.
[89] 23. oktoobri 2018. aasta Euroopa Parlamendi ja Nõukogu määrus (EL)2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ. – ELT L 295, 21.11.2018, lk 39-98.

isikusamasuse kohta, tegeliku kasusaaja ning riikliku taustaga isiku, tema pereliikme või lähedase kaastöötaja kohta, samuti kõrge riskiga klientide ja kuriteokahtlusega tehingute kohta. Vastavad sätted viitavad asjaolule, et üldjuhul eeldab krediidiasutuste omavaheline infovahetus rahapesu tõkestamise eesmärgil isikuandmete töötlemist. Isegi kui tegelikke kasusaajaid ning isikute riiklikku tausta puudutav teave on oma iseloomult avalik, mille suhtes ei saa esineda ootust privaatsusele[90], pole krediidiasutustel võimalik vastavat teavet omavahel vahetada ilma isikuandmeid töötlemata.

Isikuandmete töötlemine on üldmääruse artikli 4 punkti 2 kohaselt isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum, nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine. Isikuandmete töötlemise mõiste on üldmääruse artikli 4 punktis 2 määratletud üsna laialt, hõlmates põhimõtteliselt mistahes tegevusi isikuandmetega. Krediidiasutuste omavahelise infovahetuse üldalus siseriiklikus õiguses on RahaPTS § 16 lõike 1, mis annab kohustatud isikutele võimaluse teha omavahel koostööd rahapesu ja terrorismi rahastamise tõkestamisel, sh edastada või vahetada teavet ning vastata päringutele mõistliku aja jooksul, järgides õigusaktidest tulenevaid kohustusi ja piiranguid. Vastav säte ei piira krediidiasutuste omavahelise infovahetuse käigus teostatavaid andmetöötluse toiminguid, mis võivad mh hõlmata nii päringu koostamiseks kui ka päringule vastamiseks vajaliku teabe kogumist, korrastamist, dokumenteerimist, edastamist, säilitamist jms. Sisuliselt kõiki toiminguid isikuandmetega, mida krediidiasutused teevad seoses omavahelise infovahetusega rahapesu tõkestamise eesmärgil, tuleks käsitleda isikuandmete töötlemisena.

Kuigi põhimõtted on oma olemuselt üldised, jättes konkreetsetes situatsioonides rakendamisel teatud tõlgendamisruumi ja valikuvabaduse, otsustati Euroopa Liidu tasandil siseturu andmekaitseõiguse kehtestamisel rakendada üksikasjalikumaid eeskirju, et liikmesriikide andmekaitse tase oleks ühtlane.[91] Üldmääruse järgi tuleks andmekaitse põhimõtteid kohaldada

[90] Rahapesu ja terrorismi rahastamise tõkestamise seaduse ja teiste seaduste muutmise seaduse eelnõu 130 SE seletuskiri. 19.12.2019, lk 13. - https://www.riigikogu.ee/tegevus/eelnoud/eelnou/69421167-7e69-4383-b2f8-b9f2912a13e6/Rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20seaduse%20ja%20teiste%20seaduste%20muutmise%20seadus (15.01.2022).

[91] Euroopa andmekaitseõiguse käsiraamat (viide 84), lk 139.

igasuguse andmesubjekti puudutava teabe suhtes (IKÜM pp 26) ning isikuandmete igasugune töötlemine peaks olema seaduslik ja õiglane (IKÜM pp 39). Isikuandmete töötlemise üldpõhimõtted on kehtestatud üldmääruse artiklis 5 ning need kehtivad mistahes isikuandmete töötlemise puhul. Artikli 5 lõike 1 kohaselt peab isikuandmete töötlemine:

- olema seaduslik, õiglane ja andmesubjektile läbipaistev (punkt a);
- toimuma kindlaksmääratud ning õiguspärastel eesmärkidel (punkt b);
- piirduma võimalikult väheste andmete kogumisega (punkt c);
- tagama isikuandmete õigsuse ning vajaduse korral ajakohasuse (punkt d);
- tagama isikuandmete säilitamise andmesubjekti tuvastamist võimaldaval kujul üksnes seni, kuni see on vajalik isikuandmete töötlemise eesmärgi täitmiseks (punkt e);
- tagama isikuandmete töötlemise viisil, mis garanteerib andmete asjakohase turvalisuse (punkt f).

Lisaks näeb artikli 5 lõige 2 ette, et andmekaitse põhimõtete järgimise eest vastutab ning nende täitmist peab tõendama vastutav töötleja ehk iga krediidiasutus, kes rahapesu tõkestamise eesmärgil toimuvas infovahetuses osaleb ning isikuandmete töötlemise toiminguid teeb. Käesoleva töö autor peab oluliseks analüüsida selliseid sätteid siseriiklikus õiguses (sh KAS ja RahaPTS), mis aitavad seoses krediidiasutuste omavahelise infovahetusega ning lähtudes rahapesu tõkestamise eesmärgist sisustada isikuandmete töötlemise põhimõtteid, määratlevad isikuandmete töötlemise õigusliku aluse ning piiravad isikuandmete töötlemise ulatust.

Krediidiasutuste omavahelise infovahetuse seisukohalt on *eesmärgikohasuse põhimõte* (IKÜM art 5 lg 1 p b) üks olulisemaid isikuandmete töötlemise põhimõtteid. Eesmärgikohasuse põhimõtte järgi võivad krediidiasutused koguda isikuandmeid täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel (nt hoolsusmeetmete kohaldamiseks rahapesu tõkestamise eesmärgil) ning ei või neid isikuandmeid hiljem töödelda viisil, mis on nende eesmärkidega vastuolus (nt ärilistel eesmärkidel AMLD4 artikli 41 lõike 2 järgi või turunduslikel eesmärkidel RahaPTS § 48 lõike 1 järgi). Üldmääruse põhjenduspunkti 50 kohaselt on isikuandmete muudel eesmärkidel töötlemine lubatud üksnes juhul, kui töötlemine on kooskõlas isikuandmete algse kogumise eesmärkidega. Sellisel juhul võib isikuandmete esialgse töötlemise õiguslik alus olla ka isikuandmete edasise töötlemise õiguslikuks aluseks. Näiteks koguvad krediidiasutused kliendi kohta teavet hoolsusmeetmete kohaldamiseks rahapesu tõkestamise eesmärgil (nö algne

töötlemise eesmärk) ning kasutavad vastavat teavet ärisuhte seire teostamiseks kogu ärisuhte jooksul (nö edasise töötlemise eesmärk). Mõlemal juhul töötlevad krediidiasutused isikuandmeid avalikes huvides oleva ülesande täitmiseks ehk andmetöötluse õiguslikuks aluseks on üldmääruse artikli 6 lõike 1 punkt e (vt ka IKÜM pp 19, RahaPTS § 48 lg 2).

Üldmääruse põhjenduspunktis 50 on täiendavalt selgitatud, et vastutaval töötlejal peaks olema lubatud üldist avalikku huvi pakkuvatel olulistel eesmärkidel isikuandmeid edasi töödelda olenemata eesmärkide vastavusest, nt teatada võimalikest süütegudest või avalikku julgeolekut ähvardavatest ohtudest ning edastada selleks isikuandmeid pädevale asutusele. Taoline isikuandmete edastamine on vastutava töötleja õigustatud huvides, kuid on lubatud üksnes juhul, kui isikuandmete töötlemine ühildub õigusliku, kutsealase või muu siduva saladuse hoidmise kohustusega. Krediidiasutused koguvad isikuandmeid mh rahapesu tõkestamise eesmärgil, mis juba olemuslikult sisaldab süütegude tõkestamise, uurimise ja avastamise eesmärki (IKÜM pp 19). Samuti on krediidiasutused kohustatud täitma RAB teatamiskohustust (RahaPTS § 49 lg 1) ning järgima tähtajatu pangasaladuse hoidmise kohustust (KAS § 88 lg 7). Kuna rahapesu tõkestamine on üldist avalikku huvi pakkuv oluline eesmärk, siis järeldab autor, et isikuandmete algse töötlemise eesmärgid ei pea alati olema kooskõlas edasise töötlemise eesmärkidega. Seega ei pea isikuandmete algse ja edasise töötlemine eesmärgid ka krediidiasutuste omavahelise infovahetuse korral olema alati vastavuses, kui andmetöötlus toimub rahapesu tõkestamise eesmärkidel ning andmetöötlus jääb regulatsioonidega lubatud piiridesse.

Teiseks oluliseks isikuandmete töötlemise põhimõtteks krediidiasutuste omavahelise infovahetuse seisukohalt on *võimalikult väheste andmete kogumine* (IKÜM art 5 lg 1 p c, edaspidi ka *minimaalsuse põhimõte*), mille järgi peavad isikuandmed olema asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt. Kahjuks pole isikuandmete töötlemise ulatust rahapesu tõkestamise ja andmekaitse regulatsioonides ning juhistes piisavalt üksikasjalikult määratletud, mistõttu on keeruline vastavat põhimõtet järgida ehk piiritleda, millised isikuandmed on olulised ning rangelt vajalikud rahapesu tõkestamise eesmärgi saavutamiseks krediidiasutuste omavahelise infovahetuse käigus. Samuti on mitmed RahaPTS-is kasutatavad mõisted raskesti tõlgendatavad või piisavalt määratlemata (nt kuriteokahtlusega tehing, kõrgema riskiga klient), mistõttu võib osutuda keeruliseks kaitsta füüsilisi isikuid isikuandmete õigustamatu töötlemise eest. Täna krediidiasutuste omavahelises infovahetuses asjakohaseks, oluliseks, vajalikuks peetud isikuandmed ja nende töötlemise ulatus võib valdkonna

regulatsioonide, juhiste ja kohtupraktika arenedes osutuda ebaproportsionaalseks või lausa lubamatuks. Sarnased arengud on toimunud rahapesu tõkestamise valdkonnas, kus varasemalt tavapärast tuleb täna hinnata kui kahtlast.[92] Mainekahju ja regulatiivsete sanktsioonide kartuses on krediidiasutused oluliselt vähendanud oma riskiisu kõrgema riskiga klientide osas, mis teatud juhtude on kaasa toonud riskide vältimise nende maandamise asemel (ingl *de-risking*) ning finantsteenustele juurdepääsu piiramise kõrgema riskiga klientidele[93] (vt täiendavalt p 3.2.3).

„Finantsasutused omavad enamikul juhtudel väga kaasaegseid infosüsteeme ja tehnoloogiat, mis võimaldab neil kergesti hallata, töödelda ja edastada väga suurt hulka informatsiooni. Kui edastatava info kriteeriumid on liiga laialt piiritletud ja hõlmavad paljusid eri info tahke, võib info edastamise tulemus olla hoopis teistsugune kui oodatud“, leiab I. Ulst.[94] Hoolimata sellest, et krediidiasutused peavad kehtestama sisemised protseduurireeglid erinevate riskide (sh andmetöötluse riskide) maandamiseks, võivad krediidiasutuste omavahelist infovahetust reguleerivad sätted siseriiklikus õiguses osutuda praktikas *kasutamatuks*, kui edastatava teabe kriteeriume regulatsioonides, nende seletuskirjades või järelevalveasutuste juhenditest täpsemalt ei piiritleta. Magistritöö kolmandas peatükis on täiendavalt analüüsitud krediidiasutuste omavahelist infovahetust kuriteokahtlusega tehingute ja kõrgema riskiga klientide osas, et tuua välja probleemid regulatsioonides kasutatavate mõistete, andmetöötluse õiguslikke aluste ja ulatuse osas.

2.3 Isikuandmete töötlemise õiguslikud alused ja ulatus krediidiasutuste omavahelise infovahetuse korral

Krediidiasutused peavad oma klientide suhtes kohaldama hoolsusmeetmeid (sh tunne-oma-klienti põhimõtet, edaspidi ka KYC) nii ärisuhte loomisel kui ka selle käigus. Ühelt poolt küsivad pangad kui eraõiguslikud juriidilised isikud ning kasumile orienteeritud ettevõtjad oma klientidelt teavet nende vajadustele vastavate pangateenuste pakkumiseks (nn KYC eraõiguslik eesmärk). Teisalt koguvad pangad kui sotsiaalselt vastutustundlikud ettevõtjad klientide kohta teavet rahvusvaheliste ja siseriiklike regulatsioonide täitmiseks, et mh tõkestada rahapesu, terrorismi

[92] Mäeker/Nõmm (2020) (viide 14), lk 661.
[93] Lowe, R. J. Anti-Money Laundering – the Need for Intelligence. – Journal of Financial 2017/24 (3), lk 473.
[94] Ulst, I. Rahapesu ja terrorismi finantseerimine: regulatiivsed aspektid ja finantssüsteemi kaitsmine. – Juridica 2003/7, lk 506.

rahastamist, korruptsiooni[95] ja muid majanduskuritegusid (nn KYC avalik-õiguslik eesmärk).[96] Krediidiasutused peavad kogutud isikuandmeid töötlema kooskõlas kohaldatavate andmekaitsenormidega, mis muuhulgas tähendab seda, et isikuandmete töötlemiseks peab alati olema seaduslik alus ning järgida tuleb isikuandmete töötlemise põhimõtteid ja nendest tulenevaid piiranguid (sh eesmärgi piirang, võimalikult väheste andmete kogumine jms). Krediidiasutuste koostöö ja infovahetuse mõttes on isikuandmete töötlemise aluste, eesmärgi ja ulatuse piiritlemine oluline, et vältida isikuandmete põhjendamatut töötlemist ning tagada, et pangasaladusega kaitstud teavet avaldatakse kolmandatele isikutele (sh teistele krediidiasutustele) üksnes seadusega sätestatud alustel ja ulatuses.

Krediidiasutused peavad oma klientide suhtes kohaldama hoolsusmeetmeid (sh tunne-oma-klienti põhimõtet, edaspidi ka *KYC*) nii ärisuhte loomisel kui ka selle käigus. Ühelt poolt küsivad pangad kui eraõiguslikud juriidilised isikud ning kasumile orienteeritud ettevõtjad oma klientidelt teavet nende vajadustele vastavate pangateenuste pakkumiseks (nn KYC eraõiguslik eesmärk). Teisalt koguvad pangad kui sotsiaalselt vastutustundlikud ettevõtjad klientide kohta teavet rahvusvaheliste ja siseriiklike regulatsioonide täitmiseks, et mh tõkestada rahapesu, terrorismi rahastamist, korruptsiooni ja muid majanduskuritegusid (nn KYC avalik-õiguslik eesmärk). Krediidiasutused peavad kogutud isikuandmeid töötlema kooskõlas kohaldatavate andmekaitsenormidega, mis muuhulgas tähendab seda, et isikuandmete töötlemiseks peab alati olema seaduslik alus ning järgida tuleb isikuandmete töötlemise põhimõtteid ja nendest tulenevaid piiranguid (sh eesmärgi piirang, võimalikult väheste andmete kogumine jms). Krediidiasutuste koostöö ja infovahetuse mõttes on isikuandmete töötlemise aluste, eesmärgi ja ulatuse piiritlemine oluline, et vältida isikuandmete põhjendamatut töötlemist ning tagada, et pangasaladusega kaitstud teavet avaldatakse kolmandatele isikutele (sh teistele krediidiasutustele) üksnes seadusega sätestatud alustel ja ulatuses.

Seaduslikkuse põhimõte (IKÜM art 5 lg 1 p a) on üks isikuandmete töötlemise üldpõhimõtetest, mis kehtib igasuguse isikuandmete töötlemise korral. Üldmääruse põhjenduspunktide 39 ja 40 kohaselt peab igasugune isikuandmete töötlemine olema seaduslik ja õiglane, mille tagamiseks

[95] Näiteks on krediidiasutusel, finantseerimisasutusel ning notaril korruptsioonivastase seaduse § 16 lg 4 p 4 kohaselt õigus tutvuda ametiisiku huvide deklaratsioonis sisalduvate andmetega RahaPTS-st tulenevate nõuete täitmiseks. Vt Korruptsioonivastane seadus. – RT I, 13.04.2021, 4.

[96] Jäärats, E. (viide 43), lk 16.

tuleb isikuandmeid töödelda kas asjaomase andmesubjekti nõusolekul või muul õiguslikul alusel, mis on sätestatud õigusaktis. Isikuandmete töötlemine vastavalt õiguslikule alusele muudab töötlemise õiguspäraseks. Vastavad õiguslikud alused on loetletud üldmääruse artiklis 6 (tavaliste isikuandmete korral) ja artiklis 9 (eriliiki isikuandmete või delikaatsete andmete korral).[97]

Seaduslikkuse põhimõtte kohaselt peab isikuandmete töötlemine vastama vähemalt ühele üldmääruse artikli 6 lõike 1 punktides a-f toodud õiguslikule alusele (sh õiguslikus aluses määratud ulatuses). Vastavalt üldmääruse artikli 6 lõikele 1 on isikuandmete töötlemine seaduslik, kui:

a) andmesubjekt on andnud nõusoleku töödelda oma isikuandmeid ühel või mitmel konkreetsel eesmärgil;
b) isikuandmete töötlemine on vajalik andmesubjekti osalusel sõlmitud lepingu täitmiseks või lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt andmesubjekti taotlusele;
c) isikuandmete töötlemine on vajalik vastutava töötleja juriidilise kohustuse täitmiseks;
d) isikuandmete töötlemine on vajalik andmesubjekti või mõne muu füüsilise isiku eluliste huvide kaitsmiseks;
e) isikuandmete töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks (edaspidi ka *töötlemine avalikes huvides*);
f) isikuandmete töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral, välja arvatud juhul, kui sellise huvi kaaluvad üles andmesubjekti huvid või põhiõigused ja -vabadused, mille nimel tuleb kaitsta isikuandmeid, eriti juhul kui andmesubjekt on laps (edaspidi ka *töötlemine õigustatud huvides*).

Võrdväärse kaitstuse taseme tagamiseks kõigis liikmesriikides näeb üldmääruse artikkel 6 ette ammendava ja piirava loetelu juhtudest, millal isikuandmete töötlemist võib pidada seaduslikuks, ning liikmesriigid ei saa lisada artiklile 6 uusi isikuandmete töötlemise seaduslikkust puudutavaid kriteeriume ega kehtestada nõudeid olemasoleva kuue kriteeriumi ulatuse muutmiseks.[98] Sarnaselt andmekaitsedirektiivi[99] artiklile 7 saab üldmääruse artikli 6 lõike 1 kohaselt eristada isikuandmete

[97] Euroopa andmekaitseõiguse käsiraamat (viide 84), lk 140.
[98] Liidetud kohtuasjad EKo C-468/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) vs. Administración del Estado*, ECLI:EU:C:2011:777, punkt 30 ja 32.
[99] Andmekaitsedirektiiv 95/46/EÜ küll asendati üldmäärusega (EL) 2016/679, kuid üldmääruse põhjenduspunkti 9 kohaselt on andmekaitsedirektiivi eesmärgid ja põhimõtted endiselt ajakohased. Vt ka 24. oktoobri 1995. aasta Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – EÜT L 281, 20.11.2003, lk 31-50. Direktiiv kaotas kehtivuse 24.05.2018.

töötlemist nõusoleku alusel (IKÜM art 6 lg 1 p a), mis üldmääruse nõudeid järgides annab andmesubjektile kontrolli oma andmete töötlemise üle ehk võimaluse mõjutada andmetöötlust[100], ning töötlemist ülejäänud õiguslikel alustel (IKÜM art 6 lg 1 p-d b-f), kui töötlemine „on vajalik"[101] konkreetsete eesmärkide saavutamiseks (nt andmesubjektiga sõlmitud lepingu täitmiseks, vastutava töötleja juriidilise kohustuse täitmiseks vms).[102] Mõnel andmetöötluse juhul pole välistatud ka mitme õigusliku aluse samaaegne kasutamine tingimusel, et neid kasutatakse õiges kontekstis[103] ning andmete töötlemine on kooskõlas vastavate õiguslike alustega. Seega peavad krediidiasutused omavahelises infovahetuse korral, mis toimub rahapesu tõkestamise eesmärgil, töötlema isikuandmeid ühel või mitmel üldmääruse artikli 6 lõikes 1 loetletud õiguslikul alusel. Samas ei pruugi kõige asjakohasema õigusliku aluse valik olla alati ilmne, eriti kui isikuandmete töötlemine toimub nõusoleku alusel (punkt a) või andmesubjekti osalusel sõlmitud lepingu täitmiseks (punkt b), samuti kui töötlemine toimub avalikes huvides oleva ülesande täitmiseks (punkt e) või õigustatud huvi korral (punkt f).

Krediidiasutuse kohustuseks on mistahes andmetöötlustoimingu algatamisel (sh infovahetuseks teiste krediidiasutustega) välja selgitada asjakohane isikuandmete töötlemise õiguslik alus. Andmetöötluse õiguslike aluste valikut krediidiasutuste omavahelise infovahetuse korral aitab mõnevõrra piiritleda RahaPTS § 48 lõige 2, mille järgi on krediidiasutustel lubatud RahaPTS rakendamisel kogutud isikuandmeid töödelda üksnes rahapesu tõkestamise eesmärgil, mida käsitatakse avaliku huvi küsimusena üldmääruse mõistes, ning neid andmeid ei tohi täiendavalt töödelda viisil, mis ei vasta nimetatud eesmärgile (nt turunduslikel eesmärkidel). Ühelt poolt viitab RahaPTS § 48 lõige 2 eesmärgikohasuse põhimõttele (IKÜM art 5 lg 1 p b), mille järgi peaksid isikuandmete töötlemise konkreetsed eesmärgid olema selged ja õiguspärased ning need tuleks

[100] Artikli 29 alusel asutatud andmekaitse töörühm. Arvamus 15/2011 nõusoleku määratluse kohta. 01197/11/ET, WP187, 13.07.2011, lk 8.

[101] Üldmääruse artikli 6 lõike 1 punktides b-f sätestatud vajalikkuse mõiste tõlgendamisel tuleb lähtuda ELK otsuses C-524/06 (p 52) esitatud seisukohast, mille järgi ei või vajalikkuse mõistel olla sõltuvalt liikmesriigist erinev sisu, kuna eesmärgiks on tagada kõigis liikmesriikides võrdne kaitse. Tegemist on ühenduse õiguse autonoomse mõistega, mida tuleb tõlgendada nii, et see oleks täielikult kooskõlas andmekaitsedirektiivi eesmärgiga, mis on määratletud selle artikli 1 lõikes 1. Vt EKo C-524/06, *Heinz Huber vs. Bundesrepublik Deutschland* [suurkoda], ECLI:EU:C:2008:724, punkt 52.

[102] Artikli 29 alusel asutatud andmekaitse töörühm. Arvamus 06/2014 andmete vastutava töötleja õigustatud huvide mõiste kohta direktiivi 95/46/EÜ artikli 7 tähenduses. 844/14/ET, WP 217, 09.04.2014, lk 13.

[103] Arvamus 15/2011 nõusoleku määratluse kohta (viide 100), lk 7-8; vt ka Andmekaitse Inspektsioon (AKI). Pankade seire seoses isikuandmete töötlemisega nõusoleku alusel ja lepingu täitmiseks. Isikuandmete kaitse seaduse täitmise seire. Tallinn: Andmekaitse Inspektsioon 2013, lk 1. - https://www.aki.ee/sites/default/files/seired/Pankade_seire2013.pdf (09.03.2022).

kindlaks määrata andmete kogumise ajal (IKÜM pp 39). Euroopa andmekaitseõiguse käsiraamatu (edaspidi ka *käsiraamat*) järgi võib õiguspärane eesmärk olla kas mõni eelmises alapeatükis nimetatud avalikest huvidest või teiste isikute õiguste ja vabaduste kaitsmine.[104] Nii käsiraamatu kui ka üldmääruse (pp 19) kohaselt lähtub rahapesu tõkestamine avaliku huvi eesmärgist, milleks on mh kuritegude avastamine ja ennetamine, mistõttu peetakse isikuandmete töötlemist vastaval eesmärgil õiguspäraseks (vt lisaselgitusi eespool). Seega on krediidiasutuste omavaheline infovahetus rahapesu tõkestamise eesmärgil õiguspärane eesmärk isikuandmete töötlemiseks.

Teiselt poolt viitab RahaPTS § 48 lõige 2 isikuandmete töötlemise ühele võimalikule õiguslikule alusele (st töötlemine avalikes huvides), mis iseenesest ei välista andmetöötlust muudel õiguslikel alustel (nt juriidilise kohustuse täitmiseks, õigustatud huvid korral), kui eesmärgiks on rahapesu tõkestamine. Näide andmetöötluse eesmärkide kokkusobivusest, kuid õigusliku aluse erinevusest on ärisuhte seire teostamine RahaPTS § 20 lõike 1 punkti 6 alusel (st töötlemine avalikes huvides) ning selle käigus tuvastatud rahapesukahtlusega tehingutest RAB teavitamine RahaPTS § 49 lõike 1 alusel (st töötlemine juriidilise kohustuse täitmiseks).

Käesoleva magistritöö autori arvates on rahapesu tõkestamise eesmärgil toimuva krediidiasutuste omavahelise infovahetuse korral kõige asjakohasemad isikuandmete töötlemise õiguslikud alused töötlemine avalikes huvides (IKÜM art 6 lg 1 p e) ning töötlemine õigustatud huvides (IKÜM art 6 lg 1 p f), eriti kui tegemist on tavapäraste isikuandmetega üldmääruse artikli 4 punkti 1 mõistes (nt isiku nimi, sünniaeg, kontonumber vms), mitte eriliiki isikuandmetega üldmääruse artikli 9 lõike 1 mõistes (nt rassiline või etniline päritolu, usulised veendumused või poliitilised vaated, geneetilised andmed või terviseandmed vms), mille töötlemine on keelatud, välja arvatud üldmääruses lubatud konkreetsetel juhtudel. Vastavat järeldust toetab asjaolu, et tegemist on krediidiasutuste õigusega vahetada omavahel pangasaladusega kaitstud teavet rahapesu tõkestamise eesmärgil, mitte õigusaktist tuleneva vastavasisulise kohustusega. RahaPTS seletuskirja 130 SE järgi on koostöö tegemine rahapesu tõkestamise eesmärgil kohustatud isikutele antud võimalus (mitte kohustus), kuid samal eesmärgil koostöö tegemine järelevalve- ja korrakaitseasustustega on kohustatud isikutele seadusega pandud kohustus (mitte võimalus).[105]

[104] Euroopa andmekaitseõiguse käsiraamat (viide 84), lk 41.
[105] RahaPTS seletuskiri 130 SE (viide 90), lk 13-14.

Näiteks on krediidiasutused *kohustatud* teavitama RAB rahapesu ja terrorismi rahastamise kahtlusega tegevusest või asjaoludest RahaPTS § 49 lõike 1 alusel (st täitma seadusjärgset teatamiskohustust) ning hoidma konfidentsiaalsena asjaolu, et isiku kohta on esitatud teade RAB-ile § 51 lõike 1 alusel. Samas on krediidiasutustel *õigus* vahetada omavahel teavet kõrge riskiga klientide ja kuriteokahtlusega tehingute kohta rahapesu tõkestamise eesmärgil vastavalt RahaPTS § 51 lõikele 5. Seega pole krediidiasutuste omavahelise infovahetuse puhul andmetöötluse õiguslikuks aluseks juriidilise kohustuse täitmine (IKÜM art 6 lg 1 p c), mistõttu seda töös põhjalikumalt ei käsitleta. Samuti pole krediidiasutuste omavahelise infovahetuse puhul asjakohased isikuandmete töötlemise õiguslikud alused nõusolek (IKÜM art 6 lg 1 p a), lepingu täitmine (IKÜM art 6 lg 1 p b) ega eluliste huvide kaitse (IKÜM art 6 lg 1 p d), kui eesmärgiks on rahapesu tõkestamine, mistõttu neid käesolevas töös ei analüüsita. Järgnevates alapunktides on analüüsitud kahte kõige asjakohasemat isikuandmete töötlemise õiguslikku alust, kui krediidiasutused vahetavad omavahel teavet rahapesu tõkestamise eesmärgil, st isikuandmete töötlemist avalikes huvides oleva ülesande täitmiseks ning õigustatud huvi korral.

Isikuandmete töötlemise ulatust krediidiasutuste omavahelise koostöö ja infovahetuse puhul ei ole seadusandja pidanud vajalikuks detailselt reguleerida. Arvatavasti on üheks põhjuseks kohustatud isikute suur arv ning nende tegutsemisvaldkondade olulised erinevused. Samas on Euroopa Kohus erinevates otsustes rõhutanud, et andmete töötlemise vajalikkuse tingimuse puhul tuleb meeles pidada, et isikuandmete kaitse erandite ja piirangute puhul tuleb piirduda rangelt vajalikuga.[106] Sisuliselt tähendab see, et krediidiasutused peavad tasakaalustatult kaaluma liidu eesmärke rahapesu tõkestamisel ja füüsiliste isikute õigusi isikuandmete kaitsel[107] ning piirduma omavahelises infovahetuses rangelt vajalikuga, isegi kui andmetöötlus toimub avalikes huvides rahapesu tõkestamise eesmärgil. Näiteks on üheks isikuandmete töötlemise ulatust reguleerivaks sätteks siseriiklikus õiguses RahaPTS § 51 lõige 5, mis võimaldab krediidiasutustel vahetada omavahel teavet kõrgema riskiga klientide ja kuriteokahtlusega tehingute kohta rahapesu tõkestamise eesmärgil, kuid edastatava teabe osas „*rangelt vajalikuga piirdumiseks*“ puuduvad piisavalt detailsed juhised, millele isikuandmete töötlemisel tugineda. Teiseks isikuandmete

[106] Liidetud kohtuasjad EKo C-92/09 ja C-93/09 (viide 21), p 86; EKo C-473/12, *Institut professionnel des agents immobiliers (IPI) vs. Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte*, EU:C:2013:715, p 39; EKo C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde vs. Rīgas pašvaldības SIA „Rīgas satiksme“*, ECLI:EU:C:2017:336, p 30.

[107] Nguyenm, C. L. Preventing the Use of Financial Institutions for Money Laundering and the Implications for Financial Privacy. – Journal of Money Laundering Control 2018/21 (1), lk 56-57.

töötlemise ulatust reguleerivaks sätteks siseriiklikus õiguses on RahaPTS § 16 lõige 2, mille kohaselt võivad kõik kohustatud isikud omavahel vahetada teavet, mida üks neist vajab ja mida teine on hankinud RahaPTS § 20 lõike 1 punktides 1, 3 või 5 tuleneva hoolsusmeetme kohaldamiseks, järgides RahaPTS-s sätestatud piiranguid ja hea usu põhimõtet, kuid sõltumata üheski muus seaduses sätestatud panga-, äri-, ameti-, kutse- või muu saladuse hoidmise kohustusest või info jagamise piirangust. Sisuliselt võimaldab vastav säte krediidiasutustel ilma pangasaladuse hoidmise kohustuseta vahetada teiste kohustatud isikutega järgmist teavet:

- kliendi või juhuti tehtavas tehingus osaleva isiku isikusamasuse tuvastamiseks ning esitatud teabe kontrollimiseks (RahaPTS § 16 lg 2 koosmõjus § 20 lg 1 p 1);
- tegeliku kasusaaja tuvastamiseks ja tema isikusamasuse kontrollimiseks (RahaPTS § 16 lg 2 koosmõjus § 20 lg 1 p 3);
- teabe hankimiseks asjaolu kohta, kas isik on poliitilise taustaga isik, tema pereliige või lähedaseks kaastöötajaks peetav isik (RahaPTS § 16 lg 2 koosmõjus § 20 lg 1 p 5).

RahaPTS seletuskirja 130 SE kohaselt on tegelikke kasusaajaid ja isikute riiklikku tausta puudutav teave oma iseloomult avalik, mistõttu ei saa selle suhtes esineda ootust privaatsusele. Vastava sätte kontekstis viitavad „*käesolevas seaduses sätestatud piirangud*“ kohustusele hoida konfidentsiaalsena asjaolu, et isiku suhtes on esitatud teade Rahapesu Andmebüroole vastavalt RahaPTS § 51 lõikele 1.[108] Avalikkusele mitte kättesaadavate andmete osas on Euroopa Kohus jõudnud liidetud kohtuasjas EKo C-468/10 ja C-469/10 järgmisele järeldusele: „Erinevalt nimelt avalikkusele kättesaadavates allikates esinevatest andmetest kaasneb nende andmete töötlemisega, mis avalikkusele kättesaadavad ei ole, vältimatult see, et sellest alates teab andmesubjekti eraelu puudutavat infot vastutav töötleja ning vajadusel andmeid saav kolmas isik või kolmandad isikud. Seda harta artiklites 7 ja 8 sätestatud andmesubjekti õiguste raskemat riivet tuleb võtta selle õiglases väärtuses arvesse, kui seda kaalutakse vastutava töötleja või andmeid saava kolmanda isiku või kolmandate isikute õigustatud huviga.“[109] Käesoleva töö autor on seisukohal, et rahapesu tõkestamise eesmärgil toimuva krediidiasutuste omavahelise infovahetuse õiguslikud alused ja ulatus pole regulatsioonides piisavalt üksikasjalikult ja üheselt mõistetavalt määratletud, eriti avalikkusele mitte kättesaadavate andmete osas, et kaitsta füüsilisi isikuid isikuandmete

[108] RahaPTS seletuskiri 130 SE (viide 90), lk 13.
[109] Liidetud kohtuasjad EKo C-468/10 ja C-469/10 (viide 98), p 45.

õigustamatu töötlemise ning põhiõiguste riive eest. Vastavat järeldust toetab andmetöötluse õiguslike aluste ja ulatuse analüüs järgnevates alapunktides ning kuriteokahtlusega tehingute ja kõrgema riskiga klientide osas magistritöö 3. peatükis.

Järgnevas kahes alapunktis analüüsitakse krediidiasutuste omavahelise infovahetuse seisukohalt kahte kõige asjakohasemat andmetöötluse õiguslikku alust – töötlemist avalikes huvides oleva ülesande täitmiseks (IKÜM art 6 lg 1 p e) ning õigustatud huvi korral (IKÜM art 6 lg 1 p f).

2.3.1 Isikuandmete töötlemine avalikes huvides oleva ülesande täitmiseks

Avalikku võimu saab teostada väga paljudel erinevatel viisidel (vt üldhuvi eesmärkide loetelu eespool). Üldmääruse põhjenduspunkti 45 järgi peavad isikuandmete töötlemise alus ja eesmärk olema sätestatud liidu või liikmesriigi õigusaktis, kui töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks. Vastava õigusliku aluse sätestab üldmääruse artikkel 6 lõige 1 punkt e, mille kohaselt on isikuandmete töötlemine seaduslik mh juhul, kui isikuandmete töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks. Rahapesu tõkestamise eesmärgile viitab üldmääruse põhjenduspunkt 19, mille kohaselt toimub isikuandmete töötlemine rahapesuvastaste meetmete rakendamiseks krediidiasutuste kui eraõiguslike asutuste poolt avalikes huvides oleva ülesande täitmiseks (edaspidi ka *töötlemine avalikes huvides*). Siseriiklikult rõhutab vastavat isikuandmete töötlemise alust ja eesmärki RahaPTS § 48 lõige 2, mille järgi võivad krediidiasutused RahaPTS rakendamisel kogutud isikuandmeid töödelda üksnes rahapesu ja terrorismi rahastamise tõkestamise eesmärgil, mida käsitatakse avaliku huvi küsimusena üldmääruse mõistes. Nii RahaPTS seletuskirjas (130 SE)[110] kui ka FIS seletuskirjas (326 SE)[111] on välja toodud, et avalikes huvides on ka see, kui isikud, kes on seaduse kohaselt kohustatud kohaldama hoolsusmeetmeid, saavad omavahel vahetada selleks vajalikku informatsiooni. Seejuures on seletuskirjas 130 SE rõhutatud, et hoolsusmeetmete kohaldamine kohustatud isikute poolt on esmaseks rahapesuvastaseks kaitseliiniks.[112]

Seega lähtub krediidiasutuste tegevus rahapesu tõkestamise eesmärgil eelkõige avaliku huvi eesmärgist, kui krediidiasutused kohaldavad oma klientide suhtes hoolsusmeetmeid ning

[110] RahaPTS seletuskiri 130 SE (viide 90), lk 14.
[111] Finantsinspektsiooni seaduse ja teiste seaduste muutmise seaduse eelnõu 326 SE seletuskiri. 08.02.2021, lk 11. - https://www.riigikogu.ee/tegevus/eelnoud/eelnou/adf3f17b-4142-451e-bed3-15ebc706458f/Finantsinspektsiooni%20seaduse%20ja%20teiste%20seaduste%20muutmise%20seadus (15.01.2022).
[112] RahaPTS seletuskiri 130 SE (viide 90), lk 12.

vahetavad sel eesmärgi omavahel vajalikku informatsiooni. Samas leiab käesoleva magistritöö autor, et isegi kui isikuandmete algse ja edasise töötlemise eesmärgid kattuvad (st töötlemine toimub rahapesu tõkestamise eesmärgil), ei pruugi vastava eesmärgiga seotud andmetöötlus toimuda alati samal õiguslikul alusel (st avalikes huvides oleva ülesande täitmiseks), kuigi see pole ka välistatud. Samuti ei pruugi olla välistatud mitme õigusliku aluse samaaegne kasutamine tingimusel, et neid kasutatakse õiges kontekstis.[113] Nimelt ütleb üldmääruse põhjenduspunkt 50, et liidu või liikmesriigis õiguses sätestatud õiguslik alus isikuandmete töötlemiseks võib olla ka edasise töötlemise õiguslikuks aluseks. Eesmärkide kokkusobivuse väljaselgitamiseks peab vastutav töötleja võtma mh arvesse mistahes seoseid algse eesmärgi ja kavandatava edasise töötlemise eesmärgi vahel, isikuandmete kogumise konteksti, eelkõige andmesubjekti ja vastutava töötleja vahelisel suhtel põhinevaid andmesubjekti mõistlikke ootusi andmete edasise kasutamise suhtes, isikuandmete laadi, kavandatava edasise töötlemise tagajärgi andmesubjekti jaoks ning asjakohaste kaitsemeetmete olemasolu nii esialgsetes kui ka kavandatavates edasistes isikuandmete töötlemise toimingutes. Seega peab krediidiasutus andmetöötlustoimingu algatamisel alati leidma aega asjakohase õigusliku aluse väljaselgitamiseks[114], samuti peab krediidiasutus suutma tõendada töötlemistoimingute vastavust üldmäärusele.[115]

Siinkohal tuleb rõhutada, et andmete töötlemise seaduslikkuseks peab see olema proportsionaalne taotletava õiguspärase eesmärgi suhtes. Andmesubjekti seisukohalt ei pruugi andmetöötlus alati olla õiglane ega rahapesumeede proportsionaalne, kui algselt hoolsusmeetmete kohaldamiseks kogutud teavet edastatakse valimatult teistele krediidiasutustele rahapesu tõkestamise eesmärgil, samuti kui krediidiasutuste omavaheline infovahetus puudutab teavet kõrgema riskiga klientide ja rahapesukahtlusega tehingute kohta, mis on raskesti sisustatavad õigusmõisted. Ebaselgete või raskesti sisustatavate õigusmõistete korral on isikuandmete töötlemise õigusliku aluse ja ulatuse täpsustamine regulatsioonides ja/või juhendites (hädа)vajalik, et vältida krediidiasutuste omavahelises infovahetuses isikuandmete põhjendamata töötlemist ning andmesubjekti põhiõiguste riivet.

[113] Arvamus 15/2011 nõusoleku määratluse kohta (viide 100), lk 7-8.
[114] Artikli 29 alusel asutatud andmekaitse töörühm. Suunised määruse (EL) 2016/679 kohase nõusoleku kohta. 17/ET, WP 259 rev. 01, 28.11.2017, muudetud 10.04.2018, lk 8.
[115] Euroopa andmekaitseõiguse käsiraamat (viide 84), lk 118.

Autori arvates peaksid krediidiasutused rahapesu tõkestamise eesmärgil toimuvas infovahetuses lähtuma sarnastest põhimõtetest, millest lähtuvad rahapesu andmebürood rahvusvahelises infovahetuses. RahaPTS seletuskirja 459 SE järgi on rahapesu andmebüroode infovahetuse põhialuseks põhimõte, mille kohaselt ühelt rahapesu andmebüroolt teisele edastatav teave ei ole vabaks kasutamiseks, vaid sellele kehtestab infot edastav riik asjakohased piirangud nii kasutamiseks kui ka levitamiseks.[116] Krediidiasutuste infovahetuse käigus edastatava teabe kasutamise ja levitamise ulatust ning piiranguid tuleks seega täpsustada riigisiseses õiguses, mida võimaldab muuhulgas üldmäärus. Üldmääruse artikli 6 lõike 2 kohaselt kui isikuandmete töötlemine toimub avalikes huvides, võivad liikmesriigid kehtestada konkreetsemad sätted, mis määravad üksikasjalikumalt kindlaks isikuandmete töötlemise konkreetsed nõuded ja meetmed, et tagada seaduslik ja õiglane töötlemine. Üldmääruse artikli 6 lõike 3 järgi võib isikuandmete töötlemise õiguslik alus sisaldada erisätteid, et kohandada üldmääruse sätete kohaldumist.

Vastavad erisätted võivad sisaldada üldtingimusi, mis reguleerivad vastutava töötleja poolt isikuandmete töötlemise seaduslikkust, töödeldavate andmete liiki, asjaomaseid andmesubjekte, üksuseid, kellele võib isikuandmeid avaldada, ja avaldamise põhjuseid, eesmärgi piirangut, säilitamise aega ning isikuandmete töötlemise toiminguid ja -menetlusi, sh meetmeid seadusliku ja õiglase töötlemise tagamiseks jms. Erisätted peaksid seejuures olema asjakohased ja piisavalt täpsed ning võimaldama krediidiasutustel aru saada, millises ulatuses on isikuandmete edastamine kolmandale isikule lubatud, et täita samaaegselt kahte vastuolulist eesmärki – tõkestada efektiivselt rahapesu ning tagada kõrgetasemeline isikuandmete kaitse. Ühelt poolt tuleb rahapesu tõkestamiseks kohaldada klientide suhtes hoolsusmeetmeid nii ärisuhte loomisel, ärisuhte väliselt tehingute juhuti tegemisel kui ka ärisuhte käigus (RahaPTS § 19 ja § 20), mis eeldab klientide ja nende tehingutega kohta võimalikult suures ulatuses teabe (sh isikuandmete) kogumist ja töötlemist. RahaPTS seletuskirja 507 SE järgi parandab tehingute tegemisel hoolsusmeetmetega kogutav informatsioon ja selle säilitamine rahapesu ja terrorismi rahastamise tõkestamist, avastamist ja uurimist ning piiravate meetmete rakendamist.[117] Teisalt tuleb isikuandmete töötlemisel tagada, et kogutakse võimalikult vähe andmeid (IKÜM art 5 lg 1 p c) täpselt ja selgelt

[116] RahaPTS seletuskiri 459 SE (viide 11), lk 13.
[117] Rahapesu ja terrorismi rahastamise tõkestamise seaduse ja teiste seaduste muutmise seaduse eelnõu 507 SE seletuskiri. 10.01.2021, lk 11. - https://www.riigikogu.ee/tegevus/eelnoud/eelnou/ffe848a6-7b78-43cf-b106-720915882205/Rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20seaduse%20ja%20teiste%20seaduste%20muutmise%20seadus (25.02.2022).

kindlaksmääratud ning õiguspärastel eesmärkidel (IKÜM art 5 lg1 p b). Isegi kui isikuandmete töötlemise eesmärk on selge (st rahapesu tõkestamine), siis puuduvad selged juhised, kuidas tagada võimalikult väheste andmete töötlemine krediidiasutuste omavahelise infovahetuse käigus. Kuigi üldmääruse artikkel 6 lõige 3 võimaldab kehtestada konkreetsemad sätted siseriiklikus õiguses ka krediidiasutuste omavahelise infovahetuse täpsustamiseks, siis pole seadusandja ega järelevalveasutused üksikasjalikke juhiste andmist vajalikuks pidanud. Võib-olla pole ka turuosalised regulatsioonide ja juhendite täiendamise vajadust seadusandjale ja/või järelevalveasutustele piisavalt kommunikeerinud, kuna olulises mahus (peaaegu) reaalajas toimuvat infovahetust krediidiasutuste vahel pettuste ja rahapesu tõkestamiseks pole tänaseni toimunud. Selles mõttes on Salv Technologies OÜ poolt algatatud pilootprojekt *AML Bridge* (vt selgitusi sissejuhatusest) samm õiguse suunas, kuna võimaldab neljal Eesti suuremal krediidiasutusel vahetada omavahel teavet pettuste ja rahapesu tõkestamiseks kiiremini ja efektiivsemalt, kui hetkel toimub RAB-ile esitatud teadetele tagasiside andmine. Täiendav analüüs kuriteokahtlusega tehingute ning RAB teadete osas on esitatud järgmises peatükis.

2.3.2 Isikuandmete töötlemine õigustatud huvi korral

Üldmäärus sätestab kuus õiguslikku alust isikuandmete töötlemiseks, sh töötlemine õigustatud huvides (IKÜM art 6 lg 1 p f), mis lisaks avalikes huvides andmetöötlusele on üks kahest peamisest isikuandmete töötlemise alusest, kui krediidiasutused vahetavad omavahel teavet rahapesu tõkestamisel eesmärgil. Andmete töötlemise seaduslikkuse seisukohalt on oluline sisustada „huvi“ mõiste. See erineb „eesmärgi“ mõistest, kuigi on sellega tihedalt seotud. Artikli 29 andmekaitse töörühm juhib oma avamuses tähelepanu vastavale erinevusele: „Andmekaitse valdkonnas on eesmärk konkreetne põhjus, miks andmeid töödeldakse: andmetöötluse aluseks olev otstarve või kavatsus. Huvi seevastu esindab vastutava töötleja võimalikku laiemat seost töötlemisega või kasu, mida vastutav töötleja töötlemisest saab või mida ühiskond võib saada.“[118] Euroopa andmekaitseõiguse käsiraamat[119] ja üldmääruse põhjenduspunkt 47 näevad ette, et õigustatud huvi tuleb iga kord hoolikalt hinnata, lisaks eeldab isikuandmete töötleja üldjuhend[120] õigustatud huvi põhjendamist. Teisisõnu peab krediidiasutus kui isikuandmete töötleja suutma põhjendada seost kogutavate andmete ja nende töötlemise eesmärgi vahel, kuna töötlemine on üksnes vahend

[118] Arvamus 06/2014 õigustatud huvide mõiste kohta (viide 102), lk 23.
[119] Euroopa andmekaitseõiguse käsiraamat (viide 84), lk 153.
[120] AKI. Isikuandmete töötleja üldjuhend (viide 86), lk 44.

eesmärgi saavutamiseks.[121] Seega peab vastutav töötleja enne andmetöötlust hoolikalt ja tulemuslikult hindama, kas tal on andmetöötluseks õigustatud huvi, kas töötlemine on selle õigustatud huvi jaoks vajalik ning kas sellise huvi kaaluvad konkreetsel juhul üles andmesubjektide huvid ning põhiõigused ja -vabadused.[122]

Kui vastutava töötleja õigustatud huvi on tuvastatud, siis tuleb seda tasakaalustada andmesubjekti huvide või põhiõigustega.[123] Tasakaalustamiseks peab õigustatud huvi olema sõnastatud piisavalt selgelt, kuna piisav pole huvi, mis on liiga ebamäärane või spekulatiivne. Kui töötleja huvi ei ole õigustatud, siis ei saa tasakaalustamist kasutada, kuna andmetöötluse õigusliku alusega seotud esimene eeldus pole täidetud. Artikli 29 andmekaitse töörühma arvamuse järgi võib mh üheks õigustatud huvi näiteks olla pettuse, teenuste kuritarvitamise või rahapesu takistamine. Eelnevast järeldub, et rahapesu tõkestamise eesmärk võimaldab andmetöötlust ka õigustatud huvides. Õigustatud huvi tuvastamisega ei saa anda hinnangut aga sellele, kas krediidiasutuse huvid kaaluvad ülesse andmesubjekti huvid ja õigused või mitte.[124] Lähtudes eelnevast analüüsist, on selleks vaja läbi viia huvide tasakaalustamine. Autor on nõus seisukohaga, et üldmääruse artikli 6 lõike 1 punkti f „ei tohi pidada õiguslikuks aluseks, mida saab kasutada üksnes harva haruldastes ja ettenägematutes olukordades hädaabinõuna või viimase võimalusena, kui ükski muu alus ei kehti. Samuti ei tohiks seda pidada eelistatud võimaluseks ega laiendada põhjendamatult selle kasutusala eeldusel, et see on vähem piirav kui ülejäänud alused. Pigem on see isikuandmete töötlemise seaduslikkuse teiste alustega võrdväärne.“[125]

Üldmääruse artikli 6 lõige 1 punkt f võimaldab muuhulgas isikuandmete töötlemist *kolmanda isiku* õigustatud huvi alusel. Euroopa Kohus (edaspidi ka *EK*) selgitas kohtuasjas C-13/16, et andmekaitsedirektiivi artikkel 7 p f (tänane IKÜM art 6 lg 1 p f) ei näe ise ette kohustust, vaid väljendab võimalust töödelda isikuandmeid (nt avalikustada vajalikke andmeid kolmandale isikule, kel on olemas õiguspärane huvi).[126] Lisaks rõhutas EK, et andmekaitsedirektiiviga ei ole selline avalikustamine vastuolus juhul, kui seda tehakse riigisisese õiguse alusel ja järgides kõnealuses sättes ette nähtud tingimusi.[127] Krediidiasutuste omavaheline infovahetus rahapesu

[121] *Ibid*, lk 22.
[122] Arvamus 06/2014 õigustatud huvide mõiste kohta (viide 102), lk 43.
[123] *Ibid*, lk 49.
[124] *Ibid*, lk 24.
[125] *Ibid*, lk 48.
[126] EKo C-13/16 (viide 106), p 26.
[127] *Ibid*, p 27 ja 34.

tõkestamise eesmärgil on siseriikliku õiguse alusel krediidiasutustele antud võimalus vahetada pangasaladusega kaitstud teavet kolmandate isikutega, mitte vastav seadusjärgne kohustus (vt lisaselgitusi eespool). Siinkohal tuleb rõhutada, et RahaPTS § 16 lõige 1 ja RahaPTS § 51 lõige 5 võimaldavad krediidiasutuste *omavahelist* infovahetust (sh päringute edastamist ja neile vastamist), mis sisuliselt tähendab seda, et algatus infovahetuseks võib tulla mistahes krediidiasutuse poolt, kuid õigustatud huvi olemasoluks peab infovahetus lähtuma rahapesu tõkestamise eesmärgist. Seega annab üldmäärus krediidiasutusele võimaluse avalikustada vajalikku teavet teistele krediidiasutustele kui kolmandatele isikutele, kellel on olemas õiguspärane huvi, mida krediidiasutus peab iga kord andmetöötluse algatamisel hindama. Õigustatud huvi hindamiseks on mainitud kohtuasjas välja toodud kolm kumulatiivset tingimust, mille täitmisel on isikuandmete töötlemine õigustatud huvi alusel seaduslik:

1. Andmete avaldamine peab olema vajalik kolmanda isiku õigustatud huvide teostamiseks;
2. Isikuandmete töötlemine peab toimuma õigustatud huvide teostamiseks;
3. Andmesubjekti põhiõigused ja -vabadused ei tohi olla vastutava töötleja või kolmandate isikute õigustatud huvide suhtes ülimuslikud.[128]

Huvide tasakaalustamisel peavad krediidiasutused arvesse võtma järgmisi tegureid: a) vastutava töötleja õigustatud huvi hindamine, b) mõju andmesubjektidele, c) esialgne tasakaal, d) täiendavad kaitsemeetmed, mida vastutav töötleja võtab andmesubjektidele avalduva põhjendamatu mõju vältimiseks.[129] Selleks, et krediidiasutuse õigustatud huvi oleks kaalukam, peab andmete töötlemine olema asjaomase põhiõiguse kasutamiseks vajalik ja proportsionaalne.[130]

Vastanduvate õiguste ja huvide kaalumisel peab krediidiasutus lähtuma iga üksikjuhtumi konkreetsetest asjaoludest[131] (mitte abstraktsest olukorrast), võttes arvesse andmesubjekti mõistlikke ootusi[132], andmesubjekti õiguste rikkumise raskust ning teatud juhtudel ka tema vanust.[133] Andmesubjekti mõistlike ootuste puhul tuleb arvestada seda, kas andmesubjekt võis andmete kogumise ajal ja kontekstis mõistlikkuse piires eeldada, et isikuandmeid võidakse teatud otstarbel töödelda (IKÜM pp 47). Käesoleva töö autori arvates peavad andmesubjektid

[128] *Ibid*, p 28.
[129] Arvamus 06/2014 õigustatud huvide mõiste kohta (viide 102), lk 33.
[130] *Ibid*, lk 34.
[131] EKo C-13/16 (viide 106), p 31.
[132] Arvamus 06/2014 õigustatud huvide mõiste kohta (viide 102), lk 43.
[133] Euroopa andmekaitseõiguse käsiraamat (viide 84), lk 154.

krediidiasutusega ärisuhet luues arvestama rahapesu tõkestamise meetmete kohaldamisega nende suhtes nii kliendisuhte algatamisel kui ka kogu kliendisuhte jooksul. See tähendab, et kogu teavet kliendi kohta (sh tehingupõhist teavet) võivad krediidiasutused kasutada kliendisuhte pideva seire teostamiseks rahapesu tõkestamise eesmärgil, mistõttu ei saa andmesubjektil olla mõistlikku ootust, et tema isikuandmeid samal eesmärgil täiendavalt ei töödelda. Pigem on küsimus selles, kas andmesubjekti huvid ja põhiõigused kaaluvad teatud andmetöötluse olukorras ülesse krediidiasutuste huvid töödelda isikuandmeid rahapesu tõkestamise eesmärgil (nt teabe edastamisel kahtlaste tehingute ja kõrgema riskiga klientide kohta teistele krediidiasutustele). Hea tava kohaselt tuleb õigsustatud huvi „hindamine dokumenteerida piisava üksikasjalikkusega ja läbipaistvalt, et asjakohased sidusrühmad, sealhulgas andmesubjektid ja andmekaitseasutused ning lõppkokkuvõttes kohtud, saaksid vajaduse korral kontrollida, et tehtud on terviklik ja nõuetekohane hindamine.“[134] Eelnevast võib järeldada, et õigustamatu andmetöötluse vältimiseks ning andmesubjekti kaitsva meetmena peaksid krediidiasutused omavahelise infovahetuse käigus piisava põhjalikkusega dokumenteerima nii õigustatud huvi olemasolu kui ka erinevate huvide tasakaalustamise tulemused.

Kokkuvõttes on õigustatud huvi pigem erandlik ning peaaegu alati vaieldav andmetöötluse alus, mida üldjuhul tasakaalustab nõue teavitada inimest tema kohta käivast andmetöötlusest (IKÜM art 13 ja 14).[135] Vastavate sätete järgi sõltub andmesubjekti teavitamiskohustus omakorda sellest, kas teave on kogutud andmesubjektilt või mitte. Viimasel juhul puudub teavitamiskohustus, kui ja sel määral mil „isikuandmed peavad jääma salajaseks liidu või liikmesriigi õigusega reguleeritava ametisaladuse hoidmise kohustuse, sealhulgas põhikirjajärgse saladuse hoidmise kohustuse tõttu“ (IKÜM art 14 lg 5 p d). KAS § 88 lõike 4 järgi on mh krediidiasutuse aktsionäridel, juhtidel, töötajatel tähtajatu pangasaladuse hoidmise kohustus. Teatud juhtudel (nt KAS § 88 lg 4^1-5^1) on pangasaladuse avaldamine siiski lubatud ning seda ei käsitata seaduse või lepinguga pandud konfidentsiaalsusnõude rikkumisena. Näiteks KAS § 5^1 lõiked 3 ja 4 võimaldavad krediidiasutustel avaldada pangasaladuse kolmandatele isikutele RahaPTS § 16 sätestatud alustel ja korras ning RahaPTS § 51 rakendamiseks vajalikus ulatuses. Samuti võimaldab üldmäärus piirata õigusaktiga andmesubjekti õigusi (sh andmetöötlusest teavitamist), et tagada süütegude tõkestamine, uurimine, avastamine jms, mis on asjakohane rahapesumeetmete korral (IKÜM art

[134] Arvamus 06/2014 õigustatud huvide mõiste kohta (viide 102), lk 43.
[135] AKI. Isikuandmete töötleja üldjuhend (viide 86), lk 8.

23, IKÜM pp 19). Seega puudub krediidiasutustel pangasaladuse ja andmekaitse regulatsioonist tulenevalt kohustus teavitada andmesubjekti, kui krediidiasutusel on õigustatud huvi isikuandmete töötlemiseks rahapesu tõkestamise eesmärgil ning ta sel eesmärgil edastab teavet teistele krediidiasutustele.

3 KREDIIDIASUTUSTE OMAVAHELINE INFOVAHETUS KURITEOKAHTLUSEGA TEHINGUTE JA KÕRGE RISKIGA KLIENTIDE OSAS

3.1 Krediidiasutuste infovahetus kuriteokahtlusega tehingute osas

3.1.1 Kuriteokahtlusega tehingu mõiste määratlemine

Rahapesu tõkestamise protsess on kahetasandiline, kus ühelt poolt püütakse ennetavate meetmetega rahapesu ära hoida ning teiselt poolt rahapesu kui kuritegu kriminaliseerida. Rahapesu ennetavate meetmete kohaldamise roll on avalik-õigusliku kohustusena pandud suuresti erasektorile (sh kohustatud isikutele RahaPTS § 2 lg 1 mõistes). Riigi roll on ennekõike kuriteo toimepanijaid koosseisu täitumisel kriminaalõiguslikult vastutusele võtta ja teo käigus saadud vahendid konfiskeerida.[136] Rahapesu tõkestamise valdkond on ilmekas näide sellest, millised pöördelised muutused on toimunud panganduses viimasel kümnendi jooksul ning kuidas on tänapäeva kiiresti muutuv maailm toonud kaasa nii uusi väärtusi kui ka seniste väärtuste ümberhindamist. Näiteks on eraõiguslikel isikutel lasuvad rahapesu ennetavad meetmed (sh oma kliendi tundmise nõuded) kehtinud sarnaste põhimõtetega juba aastakümneid, mistõttu pole küsimus normide või kohustuste puudumises, kuid aastate jooksu on muutunud pankadelt oodatav hoolsus, selle ulatus ja tähendus. M. Mäekeri ja A. Nõmme arvates on tulemuseks see, et avalikkus vaatab kunagisi tehinguid liigselt tänastele teadmistele tuginedes, mis tekitab mõnevõrra segadust juhtumite, väärtuste maailma ja nende käsitlemise ajateljel. Pankade hoolsust ei hinnata enam pelgalt skaalal, kas suudeti tõkestada rahapesu ja terrorismi rahastamist, vaid kas suudetakse ära hoida kahtlane tehing ja tegevus, mis võib viidata ükskõik millisele kuriteole. See on tõstnud pankadelt oodatava hoolsuse taseme rahapesu riskide tuvastamisel väga kõrgeks ning teinud pangad väga ettevaatlikuks, kuna avalikkuse ees võidakse sattuda hätta ka tehingutega, mida ei kvalifitseerita niivõrd seaduslikkuse järgi, vaid eetilistest tõekspidamistest lähtudes. Varasemalt *tavapärane* tuleb täna kvalifitseerida kui *kahtlane*.[137]

Rahapesu ja terrorismi rahastamise tõkestamise rahvusvahelised standardid, mis on kodifitseeritud FATF poolt ning rahvusvahelisse ja siseriiklikku õigusesse üle võetud, kohustavad krediidiasutusi

[136] Mäeker /Nõmm (2020) (viide 14), lk 662.
[137] Mäeker/Nõmm (2020) (viide 14), lk 661.

ja teisi kohustatud isikuid teatama pädevatele asutustele (nt rahapesu andmebüroodele) oma klientide kahtlastest tehingutest. Sel põhjusel kohaldatakse pangateenuseid kasutavate klientide suhtes hoolsusmeetmeid, mis peaks vähendama rahaliste ressursside väärkasutust ning suurendama isikute ligipääsu finantsteenustele. Broekhoven jt arvates on see praktikas viinud teistsugustele tulemustele ehk riskide maandamise asemel on hakatud neid vältima (ingl *de-risking*), mis on piiranud teatud kliendigruppide (nt mittetulundusühingute) ligipääsu finantsteenustele.[138] Täiendav analüüs vastava nähtuse kohta on esitatud alapunktis 3.2.3.

RahaPTS § 49 sätestab krediidiasutuste teatamiskohustuse rahapesu kahtluse korral. Nimetatud sätte kohaselt on krediidiasutused kohustatud teavitama Rahapesu Andmebürood tegevusest ja asjaoludest, mille tunnused viitavad kuritegevusest saadud tulu kasutamisele või mille puhul on tekkinud kahtlus, et tegemist on rahapesu või sellega seotud kuritegude toimepanemisega. Lisaks annab RahaPTS § 51 lõige 5 krediidi- ja finantseerimisasutustele õiguse vahetada omavahel teavet kõrge riskiga klientide ja kuriteokahtlusega tehingute kohta rahapesu tõkestamise eesmärgil. Järgnevalt on käsitletud *rahapesu* mõistet juriidilises tähenduses, rahapesu eelkuritegusid ning kahtlaste tehingute tunnuseid, et seeläbi sisustada *kuriteokahtlusega tehingu* mõiste ning määratleda krediidiasutuste infovahetuse ulatus kuriteokahtlusega tehingute osas vastavalt RahaPTS § 51 lõikele 5.

FATF-i uuendatud 40 soovituse[139] kohaselt peaksid riigid Viini konventsiooni[140] ja Palermo konventsiooni[141] alusel rahapesu kriminaliseerima ning kohaldama rahapesu kuritegu kõigi oluliste kuritegude suhtes, et hõlmata võimalikult suurt hulka eelkuritegusid. I. Ulsti arvates on väga oluline riigisiseselt kindlaks määrata, mida lugeda rahapesuks (st mida kriminaliseerida). Teisisõnu peab iga riik kindlaks määrama, milliseid raskeid kuritegusid käsitletakse tavapäraselt

[138] Broekhoven, L. van, Goswami, S. Can Stakeholder Dialogues Help Solve Financial Access Restrictions Faced by Non-Profit Organizations That Stem from Countering Terrorism Financing Standards and International Sanctions? – International Review of the Red Cross 2022/103 (917), lk 724.

[139] FATF Recommendations (2012-2022) (viide 32), soovitus nr 3 (lk 12) ja selle kommentaar (lk 38).

[140] Narkootiliste ja psühhotroopsete ainete ebaseadusliku ringluse vastane Ühinenud Rahvaste Organisatsiooni konventsioon (Viini konventsioon). – RT II 2000, 15, 92. United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention). Koostatud 20.12.1988 Viinis, jõustunud 11.11.1990. Eesti suhtes jõustunud 10.10.2000.

[141] Rahvusvahelise organiseeritud kuritegevuse vastu võitlemise Ühinenud Rahvaste Organisatsiooni konventsioon (Palermo konventsioon). – RT II 2003, 1, 1. United Nations Convention against Transnational Organized Crime (Palermo Convention). Koostatud 15.11.2000 New Yorgis, avatud allakirjutamiseks 12.12.2000 Palermos, jõustunud 29.09.2003. Eesti suhtes jõustunud 29.09.2003.

rahapesule eelnevate kuritegudena.[142] RahaPTS § 4 lõike 1 kohaselt on rahapesu „kuritegelikust tegevusest saadud vara või selle asemel saadud vara:

1) muundamine või üleandmine eesmärgiga varjata vara ebaseaduslikku päritolu või abistada kuritegelikus tegevuses osalenud isikut, et ta saaks hoiduda oma tegude õiguslikest tagajärgedest;
2) omandamine, valdamine või kasutamine, kui selle saamisel on teada, et see on saadud kuritegelikust tegevusest või selles osalemisest;
3) tõelise olemuse, päritolu, asukoha, käsutamisviisi, ümberpaigutamise või omandiõiguse varjamine või varaga seotud muude õiguste varjamine."

Rahapesu definitsiooni aluseks olev rahvusvaheline õigus (sh AMLD4 ja AMLD6) tugineb sisulises tähenduses Viini konventsioonile ehk narkokonventsioonile (art 3 lg 1 p-d b.i, b.ii ja c.i), mis defineerib erinevat tüüpi rahapesu vormid.[143] Samuti peegeldub rahapesu definitsioon Palermo konventsioonis ehk organiseeritud kuritegevuse vastases konventsioonis (art 6 lg 2 p a), mille järgi peaksid osalisriigid mh kohaldama rahapesu kuritegu võimalikult paljude ohtlike kuritegude suhtes. Rahapesu definitsioon võib küll tunduda selgepiiriline ning rahapesu tõkestamise eesmärk arusaadav, kuid reaalses rahapesu tõkestamises on toimunud paradigma muutus. M. Mäeker ja A. Nõmm leiavad, et rahvusvahelisi rahapesu tõkestamise eesmärke silmas pidades võiks arvata, et eraõiguslikele isikutele (st kohustatud isikutele) kohustusi pannes on silmas peetud tegevusi rahapesu tõkestamiseks selle juriidilises tähenduses (st aktiivset võitlust ning hoolsust eeldatakse rahapesu kuriteo koosseisu ja selle kvalifitseerimise piirides). Tegelikkuses on ootused rahapesu tõkestamisele muutunud, mistõttu on juba standardiseadja (FATF) kirjutanud rahapesu tõkestamise ülesandesse sisse võitluse eelkuritegude vastu.[144]

Samas leiab M. Kairjak, et „majanduskaristusõiguses ei saa olla ebamääraseid koosseise, mis võimaldavad karistusõigust kasutada kui instrumenti majanduselus avalikult halvaks pandava suhtes".[145] Nimelt on rahapesu oma olemuselt derivatiivne kuritegu, mille toimumise eelduseks on ühe või mitme muu kuriteo – eelkuriteo – toimepanemine (RahaPTS kasutab terminit *kuritegelik tegevus*). Lühidalt öeldes on rahapesu kuritegeliku päritoluga vara (ehk eelkuriteost

[142] Ulst, I. (viide 94), lk 504.
[143] KarS Komm (2021)/Tibar, I. (viide 49), § 394 komm. 4, lk 1116.
[144] Mäeker/Nõmm (2020) (viide 14), lk 664 ja lk 666.
[145] Kairjak, M. Majanduskaristusõigus karistusõiguse revisjoni raames. – Juridica 2014/VIII, lk 634.

pärit vara) ning selle allikaks olnud kuriteo vahelise seose näiline kaotamine erinevate manipulatsioonidega (nt varjamine, peitmine, vahetamine, üleandmine jms) ning selle vara suunamine majanduskäibesse.[146] Rahapesu objektiks olev vara peab seega pärinema vastavast eelkuriteost, kuigi eelkuriteod ei ole rahapesu koosseisu tunnused, vaid moodustavad rahapesuga süütegude kogumi (KarS § 63).[147] Samas ilma eelkuriteota pole võimalik rääkida rahapesust KarS § 394 lõike 1 mõttes[148] ehk rahapesu koosseisu täidab üksnes kuritegeliku tegevuse tulemusel saadud vara *pesemine*.[149] Eesti seadusandja pole piiranud eelkuritegude ringi, mille tulemusena saadud vara võib olla rahapesu objektiks.[150] Felddmanise jt arvates aitab see tagada, et kriminaliseeritud oleks võimalikult lai tegude ring, millega ebaseadusliku raha suunatakse legaalsesse käibesse.[151] Seega on kuritegeliku tegevuse (st eelkuriteo) all mõeldud iga kuritegu, millest on saadud rahapesu objekt.[152] Kui panna eelnev krediidiasutuste omavahelise infovahetuse konteksti, siis võib järeldada, et väga lai eelkuritegude ring muudab krediidiasutuste jaoks keerulisemaks nii rahapesu kahtluse tuvastamise kui ka teatamiskohustuse täitmise Rahapesu Andmebüroo ees, samuti on keerulisem määratleda krediidiasutuste omavahelise infovahetuse ulatust kuriteokahtlusega tehingute osas.

Lisaks raskendab rahapesu koosseisu (KarS § 394) määratlemist see, et rahapesu mõiste ei hõlma üksnes isikute varaliste õiguste sfääri puudutavaid tegusid, vaid majanduse normaalse toimimise kahjustamist. RKKK otsuse nr 3-1-1-68-10 p 16 järgi tuleb rahapesuna KarS § 394 lõike 1 tähenduses mõista niisuguseid RahaPTS § 4 lõikes 1 kirjeldatud tegusid, millega suunatakse legaalsesse majandus- või rahakäibesse kuritegelikke vahendeid sellises mahus ja sellisel viisil, mis käivet kahjustab.[153] Väikesemahulised tehingud üldiselt majandussüsteemi ei kahjusta, mistõttu võib tulla kohaldamisele KarS § 202 (s.o süüteo toimepanemise tulemusena saadud vara omandamine, hoidmine ja turustamine). Samas võivad majandussüsteemi usaldusväärsust

[146] Tibar, I. (koost.). KarS § 394 komm. 2, lk 944. – Sootak, J., Pikamäe, P. (toim) jt. Karistusseadustik. Kommenteeritud väljaanne. 4., täiend. ja ümbertööt. vlj. Tallinn: Juura 2015; vt KarS Komm (2021)/Tibar, I. (viide 49), § 394 komm. 5, lk 1116; vt ka Mäeker/Nõmm (2020) (viide 14), lk 664.
[147] KarS Komm (2021)/Tibar, I. (viide 49), § 394 komm. 9.1., lk 1116.
[148] RKKKo 22.06.2015, 3-1-1-94-14, p 170.
[149] RKKKm 24.05.2017, 3-1-1-24-17, p 11.
[150] RKKKo 27.06.2005, 3-1-1-34-05, p 21.
[151] Feldmanis, L., Ploom, T. Rahapesu kriminaliseerimine: kelle suhtes ja millise põhjendusega? – Juridica 2007/3, lk 187.
[152] Täpsustavalt tuleb mainida, et tänane kohtupraktika seostab rahapesu vaid kriminaaltulu tootvate kuritegudega, mitte rahapesule eelneva kriminaaltulu mittetootva tegevusega (nt dokumendi võltsimine teadmata päritoluga vara õigustamiseks). Vt KarS Komm (2021)/Tibar, I. (viide 49), § 394 komm. 9.2., lk 1117.
[153] RKKKo 13.12.2010, 3-1-1-68-10, p 16.

mõjutada ka pidevad väikestes summades tehtud tehingud (nt investeerimiskelmused, krediitkaardipettused, arvutikuriteod jms). Karistusseadustiku kommentaaride kohaselt ei sätesta seadus ega kohtupraktika ühest rahaliselt väljendatud lävendit, millest alates saab kõnelda potentsiaalist kahjustada majandussüsteemi. Samas on seadusandja näinud teatud kõrgema riskiga tehingute puhul ette hoolsusmeetmete kohaldamise kohustuse vastavalt RahaPTS §-le 19, kuna need võivad seada ohtu majandussüsteemi normaalse toimimise (nt tasumine sularahas üle 10 000 euro; ärisuhte väliselt tehingute juhuti tegemisel või vahendamisel, kui tehingu väärtus on üle 15 000 euro jne).[154]

3.1.2 Kuriteokahtlusega tehingu kohta teabe avaldamise ulatus

Vastavalt FATF 20. soovitusele[155], kui finantsasutusel on kahtlus või põhjendatud alus kahtlustada, et vara on saadud kuritegelikust tegevusest või on seotud terrorismi rahastamisega, peab ta viivitamata oma kahtlustest teatama rahapesu andmebüroole. Järgnevalt on kuriteokahtlusega tehingu mõistet sisustatud vastavalt Rahapesu Andmebüroo juhendile „Juhend kahtlaste tehingute tunnuste kohta“ (edaspidi *RAB juhend*), et seeläbi määratleda krediidiasutuste omavahelise infovahetuse ulatust kuriteokahtlusega tehingute osas. RAB juhend annab krediidiasutustele juhised RahaPTS §-s 49 sätestatud teatamiskohustuse täitmiseks. Teatamiskohustuse alusel tuleb RAB-ile esitada teateid rahapesu ja terrorismi rahastamise kahtluse, ebaharilike tehingute ja tegevuste kohta ning rahvusvaheliste finantssanktsioonide kahtluse või rakendatud meetmete kohta.[156] RAB-ile esitatavate teadete liigid on järgmised:

- rahapesu kahtlus;
- ebaharilik tehing;
- ebaharilik tegevus;
- kohustuslik sularahateade;
- kahtlus või teadmine rahvusvahelise finantssanktsiooni rakendamise vajadusest;
- terrorismi rahastamise kahtlus.

Lähtudes käesoleva magistritöö teemast üldiselt (st krediidiasutuste infovahetus rahapesu tõkestamise eesmärgil) ning käesoleva alapeatüki teemast (st krediidiasutuste infovahetus kuriteokahtlusega tehingute osas), käsitleme alljärgnevalt üksnes kolme esimest RAB teate liiki.

[154] KarS Komm (2021)/Tibar, I. (viide 49), § 394 komm. 3, lk 1115.
[155] FATF Recommendations (2012-2022) (viide 32), soovitus nr 20, lk 19.
[156] RAB juhend (viide 60), p 1, lk 1.

RAB juhendi järgi peab krediidiasutus esitama RAB-ile *rahapesu või rahapesuga seotud muu kuriteo kahtlusega teate* (edaspidi *rahapesukahtlusega teade,* ingl *Suspicious Transaction Report (STR)*)[157], kui on tekkinud põhjendatud kahtlus, et tehingus kasutatavad vahendid on või võivad olla kuritegelikku päritolu või suunatud kuritegelikule eesmärgile, olenemata sellest, kas kahtlus tekkis ainult selle tehingu põhjal, eelnenud või seotud tehingutest või asjaolude koosmõjust. Põhjendatud kahtluse korral tuleb kohaldada tugevdatud hoolsusmeetmeid, et kõrvaldada rahapesu kahtlus, ning hoida seejuures isiku eest saladuses asjaolu, et krediidiasutus on esitanud või plaanib esitada RAB-ile rahapesukahtlusega teate (STR). Kui rahapesu kahtlust ei suudeta kõrvaldada, ei tohi tehingut teha ega ärisuhet luua.[158] RAB juhendi järgi võivad rahapesukahtlusega teate (STR) indikaatoriteks olla mh isiku suhtes varasemalt teadaolev rahapesukahtlus, kahtlus esitatud andmete tõele vastavuse osas, hoolsusmeetmete täitmise võimatus, rahapesukahtlus sularahatehingu või juhuti tehtava tehingu korral, rahapesukahtlus tehingu asjaolude hindamise tulemusel jne.[159]

Krediidiasutus peab RAB-ile esitama *ebahariliku tehingu teate* (ingl *Unusual Transaction Report (UTR)*), kui majanduslikult ebahariliku või ebaloogilise tehingu või teha soovitud tehingu kohta antud selgitused ei ole eluliselt usutavad ning viitavad võimalikule seosele rahapesuga või ebaseaduslikule tulu varjamisele. Ebahariliku tehingu tuvastamisel kohaldab krediidiasutus kõrgendatud hoolsusmeetmeid, mille eesmärk on isikult selgituste saamine tehingu põhjendatuse kohta. Kui isikult saadud selgitustega ei suudeta tehingu ebaharilikkust ära põhjendada, peab krediidiasutus RAB-i teavitama, kuid võib tehingut jätkata.[160] RAB juhendi järgi võivad ebahariliku tehingu teate (UTR) indikaatoriteks olla mh hoolsusmeetmete kohaldamisel tuvastatud kahtlus isiku usaldusväärsuses (nt variisiku kahtlus vms), isiku ebaharilik käitumine; ebaharilik dokumentide esitamine, teenuste tellimine või lepingutingimused; ebaharilik tehing sularahaga, kontol, virtuaalvääringuga või väärtpaberitega; ebaharilik tehing kinnisvaraga jms.[161]

Krediidiasutus peab RAB-ile esitama *ebahariliku tegevuse teate* (ingl *Unusual Activity Report (UAR)*), kui krediidiasutus tuvastab temaga ärisuhtes oleva isiku või tema äripartneri korduvad või jätkuvad ebaharilikud tehingud või tegevuse. Ebahariliku tegevuse tuvastamisel kohaldab

[157] RAB juhend (viide 60), lk 6.
[158] *Ibid*, p 16, lk 3-4.
[159] *Ibid*, lk 6-9.
[160] *Ibid*, p 17, lk 4.
[161] *Ibid*, p 17, lk 10-15.

krediidiasutus samuti kõrgendatud hoolsusmeetmeid, mille eesmärk on isikult põhjenduste saamine ebahariliku tegevuse kohta. Kui majanduslike või eluliselt usutavate selgitustega ei suudeta tegevuse ebaharilikkust ära põhjendada, peab krediidiasutus RAB-i teavitama, kuid võib tehingut jätkata.[162] RAB juhendi järgi võivad ebahariliku tegevuse teate (UTR) indikaatoriteks olla mh isiku ebaharilik käitumine; ebaharilikud sularahatehingud, tehingud virtuaalvääringutega, väärtpaberitega, valuuta vahetamisel; ebaharilik tegevus hasartmängude mängimisel jms.[163]

Vastavalt RAB juhendile peavad krediidiasutused kohaldama kõrgendatud hoolsusmeetmeid nii rahapesu kahtluse, ebahariliku tehingu kui ka ebahariliku tegevuse tuvastamisel, et kõrvaldada rahapesu kahtlus või põhjendada ebaharilikku tehingut või tegevust. Eelnevast võiks järeldada, et kuriteokahtlusega tehingu mõiste RahaPTS § 51 lõike 5 mõttes hõlmab põhjendatud rahapesu kahtlusega tehinguid RAB juhendi järgi, kuna nende tehingute puhul pole kõrgendatud hoolsusmeetmetega suudetud rahapesu kahtlust kõrvaldada, mistõttu tuleb RAB-ile esitada rahapesukahtlusega teade (STR). Samas on üsna suur tõenäosus, et krediidiasutused ei suuda ka kõrgendatud hoolsusmeetmete kohaldamise käigus koguda piisavalt teavet ning veenduda selles, et toime on pandud rahapesu kuritegu selle juriidilise tähenduses või tehinguga seotud varad on kuritegelikku päritolu. Vastavat tendentsi peegeldab ka Euroopa Liidu rahapesu andmebüroodele esitatud teadete statistika, mille järgi esitasid eraõiguslikud isikud 12 suurimale Euroopa Liidu rahapesu andmebüroole 2010. a umbes 560 000 teadet, 2017. a 1,1 miljonit teadet ja 2018. a 1,6 miljonit teadet.

M. Mäekeri ja A. Nõmme arvates oleme jõudnud ajas selleni, kus eraõiguslikud isikud (sh krediidiasutused) peavad teatama juba kahtlasest tehingust või tegevusest, neid tehinguid ära hoidma ning tõkestama sisuliselt igasugust kuritegevust, mis isegi ei pruugi olla jõudnud rahapesu staadiumisse. Seetõttu kutsutakse rahapesu andmebüroole esitatavaid teateid rahvusvaheliselt pigem *kahtlase tehingu* ja *kahtlase tegevuse teadeteks,* kuna reaalsuses on kaugenetud rahapesu ja terrorismi rahastamise kahtlusest või eelkuriteost teavitamisest.[164] I. Ulst on seisukohal, et kui edastatava informatsiooni kriteeriumid on liiga laialt piiritletud, võivad finantsasutused otsustada oma riskide piiramiseks edastada kõike, mis jääb ettenähtud piiridesse, ning koormata seeläbi

[162] RAB juhend (viide 60), p 18, lk 4.
[163] *Ibid*, p 17, lk 15-18.
[164] Mäeker/Nõmm (2020) (viide 14), lk 666.

järelevalveasutusi üleliigse teabega (nö tekitada info ülekülluse olukorra).[165] Algne probleem tuleneb L. de Kokeri arvates juba sellest, et rahapesu risk pole selgelt defineeritud, mida peegeldavad ka erinevad rahapesu regulatsioonid.[166] Pellegrina jt leiavad, et rahapesu riski erinev defineerimine on lõppkokkuvõttes viinud kasutu rahapesu tõkestamise alase teabe *ületootmiseni*.[167] Takatsi arvates on selge, et kui pangad trahvi kartuses teavitavad järelevalveasutusi kõigest kahtlasest, siis ei teata nad tegelikult mitte midagi, muutes raportitega edastatud informatsiooni väärtusetuks.[168]

Käesoleva magistritöö autori arvates on krediidiasutuses tehtavate tehingute arvu, mahtu, kiirust, tehingutega edastatavat teavet ning piiratud aja- ja tööjõuressurssi arvestades ebarealistlik eeldada, et krediidiasutused suudavad tõkestada rahapesu selle juriidilises tähenduses ehk tuvastada kahtlusepõhiselt ning piisavatele tõenditele tuginedes majandussüsteemi kahjustavaid tehinguid ja neid ennetavalt ära hoida. M. Levi arvates näib ebatõenäoline, et kogutud andmed mitmesuguste kuritegude ja rahapesuskeemide kohta saavad üldse kunagi olema piisavalt head, et vastata karmidele tõenduspõhiseid lahendusi nõudvatele standarditele. Tema arvates pole taolised metoodilised „kullastandardid" sobivad ega realistlikud sedavõrd oluliste ühiskonna sotsiaalsete probleemide lahendamiseks, mistõttu võiksid standardid olla paindlikumad.[169] Terrorismi rahastamist puudutavas juhendis on ka FATF möönnud, et suure tõenäosusega pole finantsasutused võimelised tuvastama terrorismi rahastamise juhtumeid, kuid suudavad tuvastada kahtlaseid tehinguid, millest on kohustatud teavitama pädevaid järelevalveasutusi, kes teevad kindlaks kuritegeliku või terroristliku tegevuse ning otsustavad edasise tegevuse. Sel põhjusel ei pea finantsasutused tingimata kindlaks määrama rahaliste vahendite allikat või sihtkohta, vaid tegema kindlaks selle, kas tehingud on ebatavalised, kahtlased või viitavad muul viisil kuritegelikule või terroristlikule tegevusele.[170]

---

[165] Ulst, I. (viide 94), lk 506.

[166] de Koker, L. Identifying and Managing Low Money Laundering Risk: Perspectives on FATF's Risk-Based Guidance. – Journal of Financial Crime 2009/16 (4), lk 334.

[167] Pellegrina, L. D., Masciandaro, D. The Risk Based Approach In The New European Anti-Money Laundering Legislation: A Law And Economics View. – Review of Law and Economics 2009/5 (2), lk 932.

[168] Dr E. Takáts viitab seejuures nähtusele „*Theory of Crying Wolf*", mis käsitleb üleraporteerimist ja selle tagajärgi rahapesu tuvastamisele. Vt Takats, E. A Theory of Crying Wolf: The Economics of Money Laundering Enforcement. Journal of Law, Economics, & Organization 2011/27 (1), lk 34-35; vt ka Tibar, I. Tähelepanekuid uue rahapesu ja terrorismi rahastamise tõkestamise seaduse jõustumisega seoses. – Juridica 2018/1, lk 42.

[169] Levi, M. (viide 12), lk 317.

[170] FATF. Guidance for Financial Institutions in Detecting Terrorist Financing. 24 April 2002, lk 3. - https://www.fatf-

Autor nõustub selles mõttes I. Tibariga, kelle arvates tuleks pöörata tähelepanu RahaPTS eesmärgile ja fookuse seadmisele, kuivõrd seaduse tõlgendusest sõltub ka teatamiskohustuse sisu. Laiema tõlgenduse kohaselt võib see hõlmata praktiliselt kogu kuritegevust, mille tulemusel hajub tõkestamistegevuse fookus liigselt, mis koormab võrdselt kohustatud isikuid ja avalikku sektorit.[171] Selge fookuse puudumine üksnes võimendab käitumist, mida nimetatakse *igaks juhuks teatamiseks* ehk eksimise ja võimaliku karistuse hirmus saadetakse rahapesu kahtluse korral teade *igaks juhuks*, mille tulemusel ei erista asjaomased institutsioonid suure hulga informatsiooni hulgast enam viiteid ja vihjeid, mis päris rahapesu tuvastada aitaksid. Tsiteerides I. Tibarit: „Tegeledes kõigega ei saada pahatihti ühtegi asja õigesti tehtud. Mõistetavalt tekib ka juhul, kui jaatada kohustust teatada rahapesu andmebüroole igast kuriteo kahtlusest, meetme proportsionaalsuse küsimus.“[172] Sisuliselt devalveerib liigne raporteerimine rahapesu tõkestamise süsteemi ennast. RahaPTS § 49 lõikes 1 sätestatud teatamiskohustuse sisu tõlgendus on käesoleva magistritöö mõttes oluline, kuna see võib otseselt mõjutada RahaPTS § 51 lõikes 5 kehtestatud krediidiasutuste omavahelise infovahetuse ulatust kuriteokahtlusega tehingute ja kõrgema riskiga klientide osas.

Eelnevast lähtudes leiab autor, et kuriteokahtlusega tehingu mõiste on regulatsioonides ja juhistes liiga laialt määratletud, mis muudab keeruliseks krediidiasutuste omavahelise infovahetuse ulatuse piiritlemise kuriteokahtlusega tehingute osas, et vältida seeläbi isikuandmete õigustamatut töötlemist. Autori arvates peaks rahapesu tõkestamise regulatsioonid ja juhised andma selgemaid juhtnööre, kas krediidiasutuste omavaheline infovahetus kuriteokahtlusega tehingute osas peaks piirduma üksnes olukorraga, kui krediidiasutus on tuvastanud põhjendatud rahapesu kahtluse ning teavitanud sellest RAB-i (st esitanud STR teate). Kui krediidiasutuste omavaheline infovahetus kuriteokahtlusega tehingute osas hõlmab lisaks kahtlaseid või ebaharilikke tehinguid ja tegevusi, võiks juhistes täpsustada, kas infovahetusele peab eelnema või järgnema RAB teate esitamine (st UTR või UAR teadete esitamine) või millistel juhtudel pole kahtlasest tehingust või tegevusest vajalik RAB-i teavitada. Seejuures tuleb rõhutada, et RahaPTS § 51 lõike 1 kohaselt on krediidiasutusel keelatud teavitada teisi krediidiasutusi omavahelise infovahetuse käigus RAB teate esitamisest, v.a RahaPTS § 51 lõigetes 2 ja 3 sätestatud juhtudel (nt teabe esitamisel samasse

gafi.org/media/fatf/documents/Guidance%20for%20financial%20institutions%20in%20detecting%20terrorist%20financing.pdf (21.03.2022).

[171] Tibar, I. (2018) (viide 168), lk 46.

[172] Tibar, I. (2018) (viide 168), lk 42.

kontserni kuuluvatele krediidiasutustele või tehinguga seotud krediidiasutustele). Regulatsioonide ja juhiste täiendamine nii teavitamiskohustuse kui ka krediidiasutuste omavahelise infovahetuse osas peegeldaks adekvaatsemalt krediidiasutuste reaalseid tegevusi rahapesu tõkestamisel (sh RAB-ile teabe edastamist kahtlaste ning ebaharilike tehingute ja tegevuse kohta, mitte üksnes põhjendatud ja tõendatud rahapesu kahtluse või muude eelkuritegude kohta).

3.2 Krediidiasutuste infovahetus kõrge riskiga klientide osas

3.2.1 Kõrge riskiga kliendi mõiste määratlemine

Riskipõhine lähenemine, mis on sätestatud neljandas rahapesuvastases direktiivis (AMLD4 pp 22-23), hõlmab tõenduspõhist rahapesu riskide hindamist ning riske maandavate tegevuste suunamist (sh kõrgema riskiga kliendikategooriate tähistamist ja nendega piisavat tegelemist).[173] Riskipõhise lähenemise puhul pole probleem üksnes selles, et rahapesu valdkonnas on mitmeid piisavalt määratlemata õigusmõisteid nagu kõrge riskiga klient ja kuriteokahtlusega tehing, vaid lisaks selles, et rahapesu riski on juba olemuslikult keeruline sisustada. Nimelt leiab de Koker, et riskipõhise lähenemise rakendamiseks on FATF välja andnud põhjalikud juhised, kuid pole seejuures „rahapesu riski" mõistet piisavalt defineerinud, mis muudab keeruliseks madala, keskmise ja kõrge riskiga teenusepakkujate määratlemise.[174] Sama võiks järeldada klientide riskiastmete määramise kohta. Bello jt arvates ilmneb rahapesu regulatsioonidest ja mitmetest suunistest, et rahapesu riski käsitletakse kui „ohus olemist" või „avatust riskile" (ingl *being in risk*), mitte kui „riski võtmist" (ingl *taking risks*). Erinevus seisneb selles, et *riski võtmine* tähendab tegutsemist võimaluste otsimisel ning arvestamist võimalike ohtude realiseerumisega, kuid *avatus riskile* tähendab ohtusid, mis tulenevad väliste jõudude poolt.[175] Pellegrina ja Masciandaro arvates on rahapesu riski erinev defineerimine viinud olukorrani, kus pankadel pole võimalik kasutada rahapesu riski mõõtmiseks tavapäraseid riskihindamise tehnikaid, mille tulemuseks on pankade võimetus eristada tegelikult kuritegelikku ning kasutu rahapesuga seotud teabe üleküllus.[176]

[173] Sesterikova, K. Euroopa Parlamendi ja Nõukogu 20.05.2015 direktiivist (EL) 2015/849 tuleneva riskipõhise lähenemise ja Eesti kohtupraktikas väljatöötatud majandusliku põhjendatuse kriteerium. Magistritöö. Tartu: TÜ õigusteaduskond 2016, lk 22.
[174] de Koker, L. (viide 166), lk 334 ja 340.
[175] Bello, A. U., Harvey, J. From a Risk-Based to an Uncertainty-Based Approach to Anti-Money Laundering Compliance. – Security Journal 2016/30 (1), lk 26.
[176] Pellegrina, L. D., Masciandaro, D. (viide 167), lk 932.

Rahapesu tõkestamiseks peavad krediidiasutused kohaldama oma klientide suhtes ennetavaid meetmeid ehk hoolsusmeetmeid, mille eesmärk on tunne-oma-klienti-põhimõtte (ingl *Know Your Customer* ehk *KYC*) täitmine.[177] Hoolsusmeetmeid peavad krediidiasutused kohaldama nii ärisuhte loomisel kui ka ärisuhte pideval jälgimisel (ehk seirel), sh RahaPTS hoolsusmeetmete loetelu sätestab miinimumkriteeriumid ja on imperatiivse sisuga.[178] Kõrgema riskiga olukordades (nt kui klient on poliitilise taustaga isik) peavad krediidiasutused lisaks tavapärastele hoolsusmeetmetele rakendama kliendi suhtes kõrgendatud hoolsusmeetmeid.[179] Seega peab kõrgema riskiga kliendi puhul kohustatud isik võtma rohkem meetmeid, et kliendist ja tema riskiprofiilist aru saada ning selle põhjal määrata ärisuhte edasise seire režiim. Seejuures valib hoolsusmeetmete ulatuse ja viisi iga kohustatud isik ise.[180] Kokkuvõttes peaksid krediidiasutused riskipõhise lähenemisviisi rakendamisel suutma tagada, et rahapesu tõkestavad või leevendavad meetmed on vastavuses tuvastatud riskidega, ning peaksid olema võimelised tegema otsuseid, kuidas oma ressursse kõige tõhusamal viisil jaotada.[181]

Finantsinspektsiooni juhendi järgi peab krediidiasutusel „[…] hoolsusmeetmete kohaldamisel tekkima teadmine, arusaam ja veendumus, et kogutud on piisavalt andmeid kliendi, kliendi tegevuse, ärisuhte eesmärgi ning samuti ärisuhte raames tehtavate tehingute eesmärgi ja rahaliste vahendite päritolu jms kohta, mistõttu ta mõistab klienti ja tema (äri)tegevust, võttes seejuures arvesse kliendi riskiastet ning ärisuhtega kaasnevat riski ja olemust (ehk ärisuhte riskiprofiili). Selline veendumuse tase peab võimaldama tuvastada keerukaid, suure väärtusega ja ebatavalisi tehinguid ning tehingumustreid, millel ei ole mõistlikku või nähtavat majanduslikku või õiguspärast eesmärki või mis ei ole konkreetse ärispetsiifika jaoks iseloomulik […].“[182] Kliendi riskiaste tuleb määrata vähemalt skaalal madalam (madal), keskmine ja keskmisest kõrgem (kõrge).[183]

RahaPTS § 51 lg 5 võimaldab krediidi- ja finantseerimisasutustel vahetada omavahel teavet kuriteokahtlusega tehingute ja kõrgema riskiga klientide kohta rahapesu tõkestamise eesmärgil. Siinkohal tuleb rõhutada, et kliendi tavapärasest kõrgem riskitase ei tähenda seda, et klient peseks

[177] Finantsinspektsiooni soovituslik juhend (viide 44), p 4.1.1. ja p 4.1.4.2., lk 23-24.
[178] Finantsinspektsiooni soovituslik juhend (viide 44), p 4.1.3., lk 23.
[179] EBA riskitegurite suunised (viide 40), p 4.45, lk 35.
[180] RahaPTS seletuskiri 459 SE (viide 11), lk 39.
[181] FATF Recommendations (2012-2022) (viide 32), soovitus nr 1, lk 31.
[182] Finantsinspektsiooni soovituslik juhend (viide 44), p 4.1.1.-4.1.2., lk 23.
[183] Finantsinspektsiooni soovituslik juhend (viide 44), p 4.2.2., lk 26.

raha või rahastaks terrorismi, vaid seda, et asjaolusid kogumise arvestades tuleb kliendi tegevusele ja temaga seotud asjaoludele rohkem tähelepanu pöörata. Samuti ei tähenda kliendi madalam riskitase, et klienti ei saaks rahapesu või terrorismi rahastamisega seostada.[184] Kliendi riskitaseme määramine on lõppkokkuvõttes ikkagi krediidiasutuse diskretsiooniotsus, isegi kui selle kujundamisel tuleb arvesse võtta erinevaid riskifaktoreid, mida on kirjeldatud nii rahvusvahelistes suunistes kui ka siseriikliku järelevalveasutuse soovituslikes juhendites.[185] Isikuandmete töötlemise õigusliku aluse ja ulatuse määramine võib osutuda keeruliseks, eriti nendel juhtudel, kui teabevahetus ei puuduta sama isikut ja sama tehingut, milles osaleb kaks või enam krediidiasutust (RahaPTS § 49 lg 3).

Rahapesu tõkestamise seisukohalt võivad kõrgema riskiga füüsilisest isikust kliendile viidata mh järgmised riskifaktorid: a) klient on kõrgema riskiga riikliku taustaga isik, tema pereliige või tema lähedane kaastöötaja; b) kliendi rikkuse allikat ja/või päritolu on keeruline tuvastada; c) klient on mitteresident; d) kliendi käitumine on ebatavaline (nt ei soovi esitada hoolsusmeetmete teavet, väldib vahetut kohtumist, esitab ebastandardses vormis tõendid isiku kohta vms); e) kliendi tehingud on seotud keerukate, suure väärtusega ja ebatavaliste tehingutega ja tehingumustritega, millel ei ole mõistlikku või nähtavat majanduslikku või õiguspärast eesmärki või mis ei ole konkreetse kliendikategooria puhul iseloomulik jne.[186] Muudes kõrge riskiga olukordades peaksid krediidiasutused otsustama teabe põhjal tugevdatud hoolsusmeetmete asjakohase liigi (sh soovitud lisateabe ja suurendatud seire ulatuse), mis muuhulgas sõltub põhjusest, miks kliendiga loodud ärisuhe on liigitatud suure riskiga suhteks.[187] Siinkohal tuleb rõhutada, et riskipõhise lähenemisviisi rakendamine ei tähenda seda, et krediidiasutus peaks vältima ärisuhete loomist teatud kliendikategooriatega, mida nad seostavad suurema rahapesu riskiga, või need ärisuhted lõpetama, kuna individuaalsete ärisuhetega seotud risk võib varieeruda isegi samas kliendikategoorias.[188]

Tõenäoliselt pole võimalik luua ammendavat loetelu indikaatoritest, mille järgi määrata erineva tasemega rahapesu riski, kuna rahapesu riski mõjutavad kokkuvõttes väga paljud tegurid, mida

[184] Finantsinspektsiooni soovituslik juhend (viide 44), p 4.2.3., lk 26.
[185] Eelkõige EBA riskitegurite suunised (viide 40) ja Finantsinspektsiooni soovituslik juhend (viide 44).
[186] Finantsinspektsiooni soovituslik juhend (viide 44), p 4.2.6., lk 27-28; vt ka EBA riskitegurite suunised (viide 40), lk 35 ja p 9.6., lk 57.
[187] EBA riskitegurite suunised (viide 40), p 4.62., lk 39.
[188] EBA riskitegurite suunised (viide 40), p 4.68., lk 41.

tuleb arvesse võtta ja hinnata (eelkõige kogumis). Isegi kui kliendile kõrgema riskiastme määramiseks on erinevates suunistes ette antud teatud kriteeriumid (nt isiku poliitiline taust vms), määrab krediidiasutus kliendi riskiastme suuresti teabe põhjal, mis on talle hoolsusmeetmete kohaldamise (sh ärisuhte seire) käigus teatavaks saanud. Seega on kliendi riskiastme määramine lõppkokkuvõttes iga krediidiasutuse diskretsiooniotsus, mis sõltub olulisel määral kliendi tausta ja tehingute kohta kogutud teabest, samuti kliendi riskiastme määramiseks kasutatavast riskihindamise metoodikast ning krediidiasutuse riskiisust jms. Järelikult pole võimalik *kõrgema riskiga kliendi* mõistet üheselt defineerida, mis muudab omakorda keeruliseks krediidiasutuste omavahelise infovahetuse perspektiivist isikuandmete töötlemise õigusliku aluse ja ulatuse määratlemise kõrgema riskiga klientide osas.

3.2.2 Kõrge riskiga kliendi kohta teabe avaldamise õiguslik alus ja ulatus

Tulenevalt raskustest kõrgema riskiga kliendi mõiste sisustamisel, pole sugugi lihtsam määrata krediidiasutuste omavahelise infovahetuse õiguslikku alust ja ulatust kõrgema riskiga klientide osas. KAS § 88 lõike 5^1 ja RahaPTS § 5 lõigete 2 ja 3 kohaselt võiks krediidiasutuste omavahelise infovahetuse kõrgema riskiga klientide osas jagada kolme suuremasse gruppi:

1) infovahetus samasse kontserni kuuluvate krediidiasutuse vahel;
2) infovahetus olukorras, kus see puudutab sama isikut ja sama tehingut, milles osaleb kaks või enam krediidiasutust (edaspidi *tehinguga seotud krediidiasutused*);
3) infovahetus krediidiasutuste vahel, kes pole tehinguga seotud ega kuulu samasse kontserni.

Kahel esimesel juhul on krediidiasutuste omavaheline infovahetus kõrgema riskiga klientide osas oluliselt vähem piiratud. Samasse kontserni kuuluvate krediidiasutuste puhul on oluliselt vähem piiranguid seoses pangasaladuse hoidmise kohustusega (KAS § 88 lg 5^1 p 3 ja KAS § 88 lg 7) ning RAB teate avaldamise keeluga (RahaPTS § 51 lg 2 p 2). Samuti on rakendata RAB teate avaldamise keeldu teabevahetusele olukorras, kus see puudutab sama isikut ja sama tehingut, milles osaleb kaks või enam kohustatud isikut, kes on mh krediidiasutused (RahaPTS § 51 lg 3).

Samasse kontserni kuuluvale ettevõtjale võib krediidiasutus vajadusel korral küll avaldada pangasaladuseks olevat teavet RahaPTS-is sätestatud hoolsusmeetmete kohaldamiseks (nö vajaduspõhine infovahetus KAS § 88 lg 5^1 p 3 alusel), kuid see ei tähenda teabe piiramatut edastamist kontserni kuuluvate ettevõtjate vahel, vaid eeldab mh kontsernisisese korra kehtestamist rahapesu tõkestamise alase teabe vahetamiseks ning sarnaste isikuandmete kaitse

reeglite kehtestamist RahaPTS § 15 lõike 1 alusel. Samuti eeldab pangasaladuse avaldamine ka kontsernisiseselt teabe avaldamist järelepärimise vastusena kirjalikus või kirjalikku taasesitamist võimaldavas vormis (KAS § 88 lg 5^1 alusel). Vastavad kohustused on suuresti seotud üldmääruses sätestatud vastutuse (ingl *accountability*) põhimõttega ehk kohustusega rakendada sisemisi kontrollimehhanisme ja protseduure, mis tagavad ja tõendavad andmekaitsereeglite järgimist. Need kohustused võivad muuhulgas väljenduda töötlustoimingute registri pidamises ja andmekaitse mõjuhinnangute tegemises, kui töötlemine võib tekitada suure riski füüsiliste isikute õigustele ja vabadustele. Vastav hindamine tuleb seejuures läbi viia enne kavandatud andmetöötlust ning seda tuleb ajakohastada kogu töötlemise elutsükli jooksul, et hinnata andmetöötlusega seotud riske ning vajadusel võtta kasutusele kaitsemeetmed nende riskide vähendamiseks ja juhtimiseks.[189] Igal juhul peavad krediidiasutused kehtestama piisavad kontrollimeetmed edastatud teabe konfidentsiaalsuse ja kasutamise kohta, samuti andmete lekkimise või vihjete andmise (ingl *tipping-off*) vältimiseks.[190]

RahaPTS rakendamisel kogutud isikuandmeid võib töödelda üksnes rahapesu tõkestamise eesmärgil, mida käsitletakse avaliku huvi küsimusena üldmääruse mõistes (RahaPTS § 48 lg 2). Üldmääruse põhjenduspunkti 50 kohaselt, kui isikuandmete töötlemine kaitseb eelkõige üldist avalikku huvi pakkuvaid olulisi eesmärke, peaks vastutaval töötlejal olema lubatud isikuandmeid edasi töödelda, olenemata eesmärkidele vastavusest. Hoolsusmeetmete kohaldamise käigus kogutud teabe vahetamine samasse kontserni kuuluvate ettevõtjate vahel (sh kõrgema riskiga klientide osas) täidab algse ja edasise andmetöötluse mõttes sama eesmärki kogu kontserni vaates, mistõttu toimub andmetöötlus üldjuhul avalikes huvides oleva ülesande täitmiseks (IKÜM art 6 lg 1 p e). Loomulikult võib esineda olukordi, kui kontsernisisese andmetöötluse õigusliku alusena oleks kohasem kasutada õigustatud huvi (IKÜM art 6 lg 1 p e), kuid vastavaid olukordi peavad krediidiasutused iseseisvalt hindama lähtudes mh kontserniülestest protseduurireeglitest ning vajadusel tuvastama õigustatud huvi olemasolu ja viima läbi huvide tasakaalustamise.

[189] Commission Nationale Informatique & Libertés (CNIL). When Trust Pay Off. Today's and tomorrow's means of payment facing the challenge of data protection. White Paper Collection - No 2, 23 February 2022, lk 55. - https://www.cnil.fr/sites/default/files/atoms/files/cnil-white-paper_when-trust-pays-off.pdf (03.03.2022).

[190] FATF. Consolidated FATF Standards on Information Sharing. Relevant excerpts from the FATF Recommendations and Interpretive Notes. Updated November 2017, lk 15. - https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Consolidated-FATF-Standards-information-sharing.pdf (21.02.2022).

Andmetöötluse õigusliku aluse ja ulatuse määratlemine võib osutuda keerulisemaks olukorras, kus infovahetus toimub tehinguga seotud krediidiasutuste vahel. RahaPS § 16 lõige 1 ning KAS § 88 lõige 5^1 punkt 4 võimaldavad kohustatud isikutel jagada omavahel pangasaladusega kaitstud teavet, kuid ei määratle edastatava teabe kriteeriume või teevad seda liiga laialt. Samavõrd üldsõnaline on ka KAS § 88 lõike 5^1 punkti 3, mis võimaldab krediidiasutusel kirjalikus või kirjalikku taasesitamist võimaldavas vormis esitatud järelepärimise vastusena avaldada pangasaladuse mh teisele isikule RahaPTS § 51 rakendamiseks vajalikus ulatuses. Kui lähtuda sellest, et RahaPTS § 16 lõige 1 on rahapesu tõkestamise eesmärgil toimuva infovahetuse mõttes üldnorm, siis erinormina täpsustavad krediidiasutuste omavahelist infovahetust kuriteokahtlusega tehingute ja kõrgema riskiga klientide osas RahaPTS § 51 lõige 5 ning isikusamasuse tuvastamise, poliitilise taustaga isikute ja tegelike kasusaajate osas Raha PTS § 16 lõige 2 koosmõju RahaPTS § 20 lõige 1 punktid 1, 3 ja 5. Õiguskirjanduses on välja toodud, et erinormi eesmärk on sätestada teatud erisused üldnormist ning üldnorm ise enam kohaldamisele ei tule.[191] Seega peaksid krediidiasutused kõrgema riskiga klientidega seotud infovahetuse puhul lähtuma RahaPTS § 51 lõikes 5 sätestatust.

Vastav erinorm on paigutatud RahaPTS 5. peatükki, mis käsitleb krediidiasutuse teavitamiskohustust rahapesu kahtluse korral, ning paragrahvi 51, mis reguleerib RAB-ile esitatava teate konfidentsiaalsust. Regulatsiooni loogikast lähtuvalt võiks järeldada, et krediidiasutuste omavaheline infovahetus kõrgema riskiga klientide osas on eelkõige õigustatud juhul, kui tehingus osalev krediidiasutus tuvastab põhjendatud rahapesu kahtluse või muud asjaolud, mis osutavad kuritegelikust tegevusest saadud tulu kasutamisele või muule kahtlasele või ebaharilikule tehingule või tegevusele. I. Ulsti arvates tugineb ebaharilikest tehingutest teatamine tegelikult kahele põhiprintsiibile – tunne oma klienti (ingl *Know Your Customer* ehk KYC) põhimõttele ning eeldusele, et finantsasutused on võimelised ebaharilikke tehinguid eristama.[192] Selle tagamiseks peab krediidiasutus kehtestama protseduurireeglid, mis mh sisaldavad metoodikat ja juhendit, kui krediidiasutusel tekib rahapesu kahtlus või on tegemist ebatavalise tehingu või asjaoluga, samuti RAB-i teavitamiskohustuse täitmise juhendit (RahaPTS § 14 lg 1 p 3). Seega kui krediidiasutuste omavaheline infovahetus puudutab suurema riskiga

[191] Agarmaa, M. Maksejõuetuse revisjon. Pankrotiavalduse esitamine, pankrotimenetluse raugemine, pankroti välja kuulutamine ja tagajärjed, pankrotivara moodustamine, pankrotivara valitsemine. 2018, lk 96. - https://www.just.ee/sites/www.just.ee/files/mari_agarmaa_analuus-kontseptsioon.pdf (09.04.2022).
[192] Ulst, I. (viide 94), lk 506.

kliente, kelle puhul on tuvastatud kahtlane või ebatavaline tehing või asjaolud, toimub andmetöötlus avalikes huvides oleva ülesande täitmiseks (IKÜM art 6 lg 1 p e). Vastavat seisukohta toetab ka I. Ulsti arvamus, mille järgi võib konfidentsiaalse info väljastamist krediidiasutuste poolt lugeda väiksemaks üleastumiseks kui terrorismi rahastamist ja rahapesu.[193] Sellest hoolimata peab pangasaladusega seotud teabe edastamine kolmandale isikule toimuma regulatsioonidega lubatud piirides ning lähtuma põhjendatud vajadusest. Samuti tuleks regulatsioonides või juhendites täpsustada edastatava teabe ulatust kõrgema riskiga klientide osas, kuna informatsiooni kriteeriumite täpsem defineerimine tagab andmete kogumise ja edastamise protsessi efektiivsuse. Juhised võiksid täpsustada ka RAB teatamiskohustust kõrgema riskiga kliente puudutava infovahetuse puhul (st kas, millise juhul ja millisel hetkel tuleb RAB teade esitada).

Kõigil ülejäänud juhtudel, kui infovahetus toimub krediidiasutuste vahel, kes pole tehinguga seotud ega kuulu samasse kontserni, peaks kõrgema riskiga klientidega seotud andmetöötlus olema vajalik krediidiasutuse või kolmanda isiku õigustatud huvi korral (IKÜM art 6 lg 1 p f), mis muuhulgas eeldab õigustatud huvi olemasolu tuvastamist ning erinevate huvide tasakaalustamist. Kaalukausile tuleb ühelt poolt panna riigi huvi finantsandmetele juurdepääsu ja kahtlaste tehingute avaldamise vastu, finantsasutuste huvi olla vabad koormavatest lisakohustustest ning klientide huvi säilitada piisaval määral ja ulatuses finantsprivaatsus.[194] Krediidiasutuste peamine eesmärk on kasumi teenimine finantsvahenduse kaudu ning suurema hulga rahaliste vahendite kaasamine oma äritegevuse arendamiseks ja kasvatamiseks. Ühelt poolt võib krediidiasutuste omavahelist infovahetust kõrgema riskiga isikute osas takistada see, et infovahetuse puhul on tegemist krediidiasutustele antud võimalusega, mitte seaduses määratud kohustusega. Teisalt on kliendi riskiastme määramine krediidiasutuste diskretsiooniotsus, mistõttu ei tasu eeldada krediidiasutuste aktiivsust kõrgema riskiga klientide kohta info avaldamisel teistele krediidiasutustele, kui selleks puudub põhjendatud vajadus (nt kahtlane või ebaharilik tehing, põhjendatud rahapesu kahtlus vms). Kokkuvõttes peavad krediidiasutused looma ja rakendama toimivad protseduurireeglid, mis võimaldavad kahtlaseid ja ebaharilikke tehinguid tuvastada ning kuritegelikke juhtumeid

[193] Ulst, I. (viide 94), lk 506.
[194] Myers, J. M. International Strategies to Combat Money Laundering. Financial Crimes Enforcement Network U.S. Department of the Treasury for the International Symposium on the Prevention and Control of Financial Fraud. Beijing, 19-22 October 1998, lk 4. - https://icclr.org/wp-content/uploads/2019/06/myer_pap.pdf?x94276 (21.01.2022); vt ka Ulst, I. (viide 94), lk 506.

tõkestada. Enne kõrgema riskiga kliendist või temaga seotud tehingust teatamist peab krediidiasutus sisuliselt hindama, millal kaalub kliendi privaatautonoomia ülesse teiste krediidiasutuste õigustatud huvi vastava teabe saamise osas. See tähendab krediidiasutusele olulist halduskoormust infomatsiooni kriteeriumite defineerimisel, õigustatud huvi hindamisel ja huvide tasakaalustamisel, et tagada andmete kogumise ja edastamise protsessi efektiivsus. Kahjuks pole krediidiasutuste omavahelise infovahetuse õiguslikud alused ja ulatus, samuti infovahetusega seotud mõisted ja infomatsiooni kriteeriumid regulatsioonides ega muudes juhistes määratletud piisavalt üksikasjalikult ja üheselt mõistetavalt, et kaitsta füüsilisi isikuid isikuandmete õigustamatu töötlemise eest. Kokkuvõttes nõustub autor I. Ulsti järeldusega, mille kohaselt sõltub finantsasutuste ja finantssüsteemi kaitse suurel määral finantsasutustest endist, nende kompetentsusest ning koostöövalmidusest.[195] See puudutab ka füüsiliste isikute kaitset isikuandmete töötlemisel, mis toimub krediidiasutuste omavahelise infovahetuse käigus rahapesu tõkestamise eesmärgil.

3.2.3 Kõrgema riskiga klientide ligipääs finantsteenustele

Rahapesuvastaste algatuste ja tehnoloogilise innovatsiooni kõrval on valdkonna arenguga kaasnenud ka negatiivseid tagajärgi. Karmid rahapesu regulatsioonid, ebaproportsionaalsed hoolsusmeetmete kohaldamise kulud, järelevalvega seotud halduskoormus ning võimalikud karistused on soovimatu tagajärjena vähendanud teatud kliendigruppide ligipääsu finantsteenustele (ingl *financial inclusion*). Vastavat nähtust tähistatakse õiguskirjanduses mõistega *de-risking* (nö riskide vältimine maandamise asemel), mis sisuliselt tähendab kontode sulgemist ja ärisuhte lõpetamist klientidega, kelle riskitase on hinnatud kõrgeks.[196] Näiteks võivad krediidiasutustel loobuda ärisuhete loomisest või jätkamisest klientidega, kelle tausta kontrollimine või rahaliste vahendite päritolu tõendamine kujuneb liialt kulukaks, keeruliseks või riskantseks seoses pankade vastutuse ja võimalike karistusõiguslike sanktsioonide tõttu.[197] T. Durner ja L. Shetret leiavad, et riskide maandamise asemel on krediidiasutustel lihtsam oma riske

[195] Ulst, I. (viide 94), lk 507.
[196] Durner, T., Shetret, L. Understanding Bank De-Risking and Its Effects on Financial Inclusion. An exploratory study. OXFAM International, Global Center on Cooperative Security, Research Report, 18 November 2015, lk 3. - https://www.oxfam.org/en/research/understanding-bank-de-risking-and-its-effects-financial-inclusion (15.02.2022).
[197] Jäärats, E. (viide 43), lk 4.

minimeerida ning kõrge riskiga klientidest loobuda, jättes nad „pangata“ (ingl *bank-less*) ehk ilma ligipääsust tavapärastele finantsteenustele.[198]

MONEYVAL on *de-risking* nähtust käsitlevas raportis jõudnud järeldusele, et krediidiasutused on muutunud ärisuhete loomisel üha valivamaks ja ettevaatlikumaks, eriti kõrge riskiga klientide ja jurisdiktsioonide osas. Peamiste *de-risking* meetoditena on MONEYVAL välja toonud finantstoodete ja -teenuste keelamise või piiramise teatud riikides ja kliendisektorites ning kliendisuhete lõpetamise olemasolevate klientidega ja korrespondentpankadega, samuti ülemäärased aruandlusnõuded (ingl *defensive reporting*).[199] Sarnast seisukohta on väljendanud FATF, kelle hinnangul võib liiga ettevaatlik lähenemine rahapesu tõkestamise kaitsemeetmetele (sh riskipõhise lähenemise mitte rakendamine) põhjustada olukorra, kus krediidiasutused hakkavad piirama tarbijate ja äriühingute ligipääsu reguleeritud finantssüsteemile.[200] Krediidiasutuste omavaheline infovahetus rahapesu tõkestamise eesmärgil võib kõrgema riskiga klientide olukorda veelgi halvendada, kuna tekib oht sattuda kõrgema riskiga klientide hulka või lausa *musta nimekirja* (ingl *blacklist*) ka krediidiasutuste juures, kellega ärisuhe puudub või kes on kliendi riskitaseme hinnanud madalamaks. Kokkuvõttes võib rahapesu tõkestamise eesmärgil toimuv krediidiasutuste omavaheline infovahetus vähendada füüsiliste isikute ligipääsu finantsteenustele, kuna edastatud teabe põhjal suureneb oht, et kõrgema riskiga klientidega lõpetatakse ärisuhted ning suletakse nende pangakontod.

Õiguskantsler Ü. Madise on rahandusministrile saadetud kirjas „Märgukiri põhimakseteenuste tagamise kohta“[201] suunanud tähelepanu sarnastele probleemidele, mis puudutavad pangakontode ilma põhjendusteta sulgemisi, pangakonto uuesti avamise raskusi ning pangakonto kaudu juurdepääsu tagamist põhimakseteenustele (vt VÕS[202] § 709 lg 15[1]). Hädaolukorra seaduse[203] §

[198] Durner, T., Shetret, L. (viide 196), lk 3.
[199] MONEYVAL. Report. “De-Risking” Within MONEYVAL States and Territories. Council of Europe, Strasbourg, 15 April 2015, p 10 ja 13, lk 6. https://rm.coe.int/report-de-risking-within-moneyval-states-and-territories/168071510a (20.11.2021).
[200] FATF. Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion – With a Supplement on Customer Due Diligence. Paris, 2013-2017, lk 2 ja lk 31. - www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html (02.10.2021).
[201] Õiguskantsler. Märgukiri põhimakseteenuste tagamise kohta. Õiguskantsler Ülle Madise märgukiri rahandusminister Martin Helmele, nr 6-1/191286/2001261, 10.03.2020. - https://www.oiguskantsler.ee/sites/default/files/field_document2/M%C3%A4rgukiri%20p%C3%B5himakseteenuste%20tagamise%20kohta.pdf (20.11.2021).
[202] Võlaõigusseadus. – RT I, 15.03.2022, 14.
[203] Hädaolukorra seadus. – RT I, 17.11.2021, 9.

36 lg 3 järgi on makseteenused elutähtsad teenused, mille toimepidevust korraldab Eesti Pank. 2022. aasta märtsi seisuga on elutähtsa teenuse osutajad AS SEB Pank, Swedbank AS, Luminor Bank AS ja AS LHV Pank.[204] Õiguskantsler on märgukirjas välja toonud, et põhimaksekonto on tänapäeva ühiskonna majanduselus ja ühiskondlikus elus osalemisel hädavajalikuks eeltingimuseks, mistõttu tähendab põhimakseteenuste piiramine (sh pangakonto sulgemine) isiku juurdepääsu piiramist elutähtsale teenusele ehk isiku nende põhiõiguste olulist piiramist, mille teostamiseks on vajalik pangakonto olemasolu.[205] Seejuures viitab õiguskantsler FATF-i suunistele, mis eeldavad rahapesu riskide kontrollimisel tervikliku riskipõhise lähenemise rakendamist (ingl *risk-based approach*)[206] ning kliendisuhte lõpetamist üksnes põhjendatud juhul, kui rahapesu riske ei saa vähendada.[207] See tähendab, et pangad peavad riskide vältimise asemel tegelema riskide juhtimisega, sh kohaldama potentsiaalselt kõrge riskiga klientide suhtes tugevdatud hoolsusmeetmeid, mitte lõpetama nendega kliendisuhet.[208] Õiguskantsler on seisukohal, et füüsiliste isikutega kliendisuhete lõpetamine peaks tervikliku riskipõhise käsitlemise korral olema äärmuslik lahendus või sootuks välistatud.[209]

Lisaks on MONEYVAL oma raportis rõhutanud, et pankade riskide vähendamisega ja finantsteenustele ligipääsu piiramisega võib kaasneda uusi riske ja läbipaistmatust ülemaailmses finantssüsteemis, kuna see sunnib ettevõtteid ja füüsilisi isikuid kasutama vähem reguleeritud või reguleerimata kanaleid. MONEYVAL hinnangul teeb raha liikumine reguleeritud ja jälgitavate kanalite kaudu rahapesu tõkestamise hõlpsamaks ning aitab suurendada finantsteenuste kättesaadavust.[210] Krediidiasutuste omavaheline infovahetus kuriteokahtlusega tehingute osas ei tohiks üldjuhul vähendada kõrgema riskiga klientidele ligipääsu põhimakseteenustele (sh viia pangakonto sulgemiseni), kui rahapesu kahtlus või muud kuritegelikule tegevusele viitavad asjaolud ei leia kinnitamist järelevalveasutuse (st RAB) poolt. RAB või FI täiendavad juhised krediidiasutuste omavahelise infovahetuse kohta võiksid mh anda suuniseid olukordadeks, kui kuriteokahtlusega tehingu või kõrgema riskiga klientide kohta edastatud teave ja hinnangud

[204] Makseteenuse ja sularaharingluse kirjeldus ja toimepidevuse nõuded. RMm 13.07.2018 nr 7. – RT I, 05.03.2019, 21.
[205] Õiguskantsler. Märgukiri põhimakseteenuste tagamise kohta (viide 201), p 1 ja 2, lk 1-2.
[206] FATF Recommendations (2012-2022) (viide 32), lk 31.
[207] Õiguskantsler. Märgukiri põhimakseteenuste tagamise kohta (viide 201), p 21, lk 4.
[208] *Ibid*, p 21, lk 4.
[209] *Ibid*, p 31, lk 6.
[210] MONEYVAL. Report on "De-Risking" (viide 199), p 5.1 ja 5.2, lk 5.

osutuvad põhjendamatuks ning krediidiasutused peaksid võtma meetmeid kas infovahetusele eelnenud olukorra taastamiseks või selle mõjude vähendamiseks.

Kahjuks on andmesubjekti õigused tutvuda andmetega piiratud, kui isikuandmeid töödeldakse rahapesu tõkestamise eesmärgil (nt saada teavet krediidiasutuste omavahelise infovahetuse käigus edastatud andmete kohta või pangakonto sulgemise põhjuste kohta). Üldjuhul reguleerib andmesubjekti õigust tutvuda andmetega üldmääruse artikkel 15 ning selle õiguse piiramisel kohaldatakse üldmääruse artiklit 23. Üldmääruse artikli 15 lõike 1 kohaselt on andmesubjektil õigus saada vastutavalt töötlejalt kinnitust selle kohta, kas teda käsitlevaid isikuandmeid töödeldakse, ning sellisel juhul tutvuda isikuandmetega, nende töötlemise eesmärgiga, isikuandmete liikidega jms. Samas võib üldmääruse artikli 23 lõike 1 punkti d järgi piirata seadusandliku meetmega andmesubjektide õigusi (sh õigust tutvuda andmetega), et tagada süütegude tõkestamine, uurimine, avastamine või nende eest vastutusele võtmine või kriminaalkaristuste täitmisele pööramine, sh avalikku julgeolekut ähvardavate ohtude eest kaitsmine ja nende ennetamine. Seejuures peab sätte kohaldamine andmesubjekti õiguste piiramiseks olema vajalik ja proportsionaalne, arvestades üldmääruse artiklist 15 andmesubjektile võrreldes teiste isikutega tulenevaid õigusi.[211] Siseriiklikus õiguses on vastav piirang kehtestatud KAS § 89^3 lõike 1 punktis 1, mille järgi ei kohaldata krediidiasutuse suhtes üldmääruse artiklites 15 ja 17–21 sätestatud kohustusi selliste isikuandmete (sh asukohaandmete) suhtes ning sellises ulatuses, mida krediidiasutus töötleb monitooringu ärisuhte seire teostamisel rahapesu ja terrorismi rahastamise tõkestamise eesmärgil. Järelikult on andmesubjektide võimalused tutvuda krediidiasutuste omavahelise infovahetuse käigus edastatud andmete, antud hinnangute ja tehtud otsustega piiratud, mistõttu suureneb krediidiasutuste vastutus isikuandmete kaitse ning (põhi)makseteenuste kättesaadavuse tagamisel (sh kõrgema riskiga klientidele) ning järelevalve olulisus vastava tegevuse üle kontrolli teostamisel.

Suletud pangakontode probleemi ning andmesubjekti piiratud võimalusi tutvuda rahapesu tõkestamise eesmärgil kogutud andmetega on Riigikohus käsitlenud oma 24. märtsi 2022. aasta lahendis 3-20-332/39. Lahendi kohaselt suleti 2015. ja 2016. aastal kaebaja pangakontod Ameerika Ühendriikides. Kaebaja soovis RAB-ilt saada teavet, kas tema kohta on esitatud Eesti või välisriigi krediidiasutustele või välisriigi ametiasutustele teavet, milles on viidatud rahapesu

[211] RKHKo 24.03.2022, 3-20-332/39, p 11.

kahtlusele[212], mille esitamisest RAB keeldus. RAB-i vastuse kohaselt ei saa nad väljastada oma ülesannete täitmisel kogutud andmeid ega teavet selliste andmete olemasolu või võimaliku andmevahetuse kohta, viidates RahaPTS § 60 lõikele 1 ja AvTS[213] § 23 lõike 1 punktile 1. Riigikohus rahuldas kaebaja kassatsioonkaebuse materiaalõiguse normi ebaõige kohaldamise tõttu. Riigikohus järeldas, et „RahaPTS § 60 lõike 1 teine lause ei piira andmesubjekti õigusi vahetult seaduse alusel, vaid annab selleks RAB-i juhile kaalutlusõiguse“[214] ehk võimaldab RAB juhil kehtestada teabele juurdepääsupiirangu.[215] Vastavat otsust polnud RAB juht teinud. Riigikohtu hinnangul, kui RAB juht pole andmesubjekti juurdepääsuõigust piiranud, ei saa ta keelduda andmesubjekti andmete väljastamisest, mistõttu oli teabe väljastamisest keeldumine õigusvastane.[216] Riigikohus leidis, et kui esinevad põhjused andmesubjekti õiguste piiramiseks kooskõlas üldmääruse artikliga 23, saab RAB juht piirangute üle otsustada enne kaebaja taotluste üle uue otsuse tegemist. Kokkuvõttes ei võtnud Riigikohus lõplikku seisukohta RahaPTS § 60 lõike 1 kooskõla kohta üldmääruse artikliga 23, kuna otsust andmesubjekti õiguste piiramise kohta polnud veel tehtud.[217]

Vastav Riigikohtu lahend on ilmekas näide sellest, et andmesubjektide pangakontosid võidakse sulgeda põhjendusi esitamata[218], kuid andmesubjekti võimalused pääseda ligi rahapesu tõkestamise eesmärgil kogutud teabele ning kaitsta oma õigusi on taolistel juhtudel üsna piiratud. Andmesubjekti ligipääs krediidiasutuste omavahelise infovahetuse käigus edastatud teabele on samaväärselt piiratud, mistõttu ei paranda see andmesubjekti võimalusi oma õiguste kaitsmisel (nt isikuandmete õigustamatu töötlemise või pangakontode põhjendamatu sulgemise korral). Seega peaks suurenema järelevalve krediidiasutuste omavahelise infovahetuse üle, mis toimub rahapesu tõkestamise eesmärgil, et veenduda tõhusate kaitsemeetmete rakendamises, mis peaks tagama isikuandmete kaitse vastava andmetöötluse puhul.

[212] RKHKo 24.03.2022, 3-20-332/39, p 1.
[213] Avaliku teabe seadus. – RT I, 10.03.2022, 4.
[214] RKHKo 24.03.2022, 3-20-332/39, p 13.
[215] RKHKo 24.03.2022, 3-20-332/39, p 11.
[216] RKHKo 24.03.2022, 3-20-332/39, p 13.
[217] RKHKo 24.03.2022, 3-20-332/39, p 14.
[218] RKHKo 24.03.2022, 3-20-332/39, p 2.

KOKKUVÕTE

Käesoleva töö eesmärgiks oli analüüsida kehtivat rahapesu tõkestamise ja andmekaitse õigusraamistikku, et selgitada välja, kas rahapesu tõkestamise eesmärgil toimuva krediidiasutuste omavahelise infovahetuse õiguslikud alused ja ulatus on regulatsioonides ja neid täiendavates juhistes piisavalt selgelt määratletud ning üheselt mõistetavad, et kaitsta füüsilisi isikuid isikuandmete õigustamatu töötlemise ja selle võimalike negatiivsete tagajärgede eest. Töös püstitati järgmised uurimisküsimused:

(1) Millisel õiguslikul alusel ja millises ulatuses on lubatud isikuandmete töötlemine krediidiasutuste omavahelise infovahetuse käigus rahapesu tõkestamise eesmärgil?
(2) Milliste põhimõtete ja piirangutega peavad krediidiasutused arvestama isikuandmete töötlemisel krediidiasutuste omavahelise infovahetuse käigus rahapesu tõkestamise eesmärgil?

Töö esialgsed hüpoteesid sõnastati järgmiselt:

(1) Rahapesu tõkestamise eesmärgil toimuva krediidiasutuste omavahelise infovahetuse õiguslikud alused ja ulatus pole regulatsioonides ja neid selgitavates juhistes piisavalt üksikasjalikult ja üheselt mõistetavalt määratletud, et kaitsta füüsilisi isikuid isikuandmete õigustamatu töötlemise ja selle võimalike negatiivsete tagajärgede eest.
(2) Rahapesu tõkestamise eesmärgil toimuv krediidiasutuste omavaheline infovahetus võib vähendada füüsiliste isikute ligipääsu finantsteenustele, kuna edastatud teabe põhjal suureneb oht, et krediidiasutused hakkavad vältima riske nende maandamise asemel (ingl *de-risking*) ning sulgevad pangakontod ja lõpetavad ärisuhted kõrgema riskiga klientidega.

Mõlemale uurimisküsimusele vastamiseks analüüsiti esmalt rahapesu tõkestamise õigusraamistikku ning krediidiasutuste omavahelise infovahetuse õiguslikke aluseid ja sellele kohalduvaid piiranguid liidu ja riigisiseses õiguses, et tuvastada võimalikke probleemikohti. Seejärel uuriti isikuandmete kaitse õiguslikku raamistikku ning isikuandmete töötlemisele kohalduvat regulatsiooni seoses krediidiasutuste omavahelise infovahetusega rahapesu tõkestamise eesmärgil, et määratleda kõige asjakohasemad isikuandmete töötlemise õiguslikud alused ning andmetöötluse ulatust mõjutavad tegurid. Eraldi peatükis käsitleti krediidiasutuste omavahelist infovahetust kuriteokahtlusega tehingute ning kõrgema riskiga klientide osas, kuna

tegemist on piisalt määratlemata õigusmõistetega, mis muudavad isikuandmete töötlemise õigusliku aluse ja ulatuse määratlemise keerulisemaks.

Krediidiasutused peavad oma klientide suhtes kohaldama hoolsusmeetmeid (sh tunne-oma-klienti põhimõtet) nii ärisuhte loomisel kui ka selle käigus. Ühelt poolt küsivad pangad kui eraõiguslikud juriidilised isikud ning kasumile orienteeritud ettevõtjad oma klientidelt teavet nende vajadustele vastavate pangateenuste pakkumiseks. Teisalt koguvad pangad kui sotsiaalselt vastutustundlikud ettevõtjad klientide kohta teavet rahvusvaheliste ja siseriiklike regulatsioonide täitmiseks, et mh tõkestada rahapesu, terrorismi rahastamist, korruptsiooni ja muid majanduskuritegusid. Krediidiasutused peavad rahapesu tõkestamise eesmärgil kogutud isikuandmeid töötlema kooskõlas kohaldatavate andmekaitsenormidega, mis muuhulgas tähendab seda, et isikuandmete töötlemiseks peab alati olema seaduslik alus ning järgida tuleb isikuandmete töötlemise põhimõtteid ja nendest tulenevaid piiranguid (sh eesmärgi piirang, võimalikult väheste andmete kogumine jms). Krediidiasutuste koostöö ja infovahetuse mõttes on isikuandmete töötlemise aluste, eesmärgi ja ulatuse piiritlemine oluline, et vältida isikuandmete põhjendamatut töötlemist ning tagada, et pangasaladusega kaitstud teavet avaldatakse kolmandatele isikutele (sh teistele krediidiasutustele) üksnes seadusega sätestatud alustel ja ulatuses.

Igasugune isikuandmete töötlemine peab olema seaduslik ja õiglane, et vältida sekkumist andmesubjekti õigusesse eraelu puutumatuse ja isikuandmete kaitsele. Samas pole vastavad õigused absoluutsed, kuna ühe isiku õigus eraelu austamisele ja isikuandmete kaitsele võib põrkuda teise isiku sõna- ja teabevabadusega, eneseteostusvabaduse ja ettevõtlusvabadusega jms, mistõttu tuleb põhiõigusi konkreetses olukorras tasakaalustada ja kooskõlastada muude õigustatud huvide ja õigustega, sh teiste inimeste huvidega (erahuvid) või kogu ühiskonna huvidega (avalikud huvid). Süütegude tõkestamine, uurimine ja avastamine on avaliku huvi eesmärgid, mille puhul peetakse üksikisikute õiguste piiramist õiguspäraseks, kui selline piirang arvestab põhiõiguste ja -vabaduste olemust ning on vajalik ja proportsionaalne. Rahapesu tõkestamine lähtub avaliku huvi eesmärgist (s.o süütegude avastamine ja tõkestamine), mistõttu võib sekkumist üksikisiku põhiõigustesse pidada üldjuhul õiguspäraseks, kui krediidiasutused töötlevad isikuandmeid rahapesu tõkestamise eesmärgil. Järelikult on avalikes huvides ka see, kui isikud, kes rahapesu tõkestamise eesmärgil kohaldavad klientide suhtes hoolsusmeetmeid, saavad omavahel vahetada selleks vajalikku teavet.

Krediidiasutuste omavahelist infovahetust rahapesu tõkestamise eesmärgil reguleerivad siseriiklikus õiguses peamiselt järgmised sätted – KAS § 88 ning RahaPTS § 16 lõige 1 ja § 51 lõige 5. RahaPTS § 16 lõige 1 võimaldab kõigil kohustatud isikutel teha rahapesu tõkestamise eesmärgil koostööd (sh edastada ja vahetada teavet ning vastata päringutele), järgides õigusaktidest tulenevaid kohustusi ja piiranguid. Samas võivad RahaPTS § 51 lõike 5 kohaselt üksnes krediidi- ja finantseerimisasutustel vahetada omavahel teavet kõrge riskiga klientide ja kuriteokahtlusega tehingute kohta rahapesu tõkestamise eesmärgil. Pangasaladuse tähtajatu hoidmise kohustus, isikuandmete kaitse nõuded ning rahapesukahtlusega teate konfidentsiaalsus on peamised piirangud, millega krediidiasutused omavahelise infovahetuse puhul peavad arvestama. Lisaks andmetöötluse seaduslikkuse põhimõttele mõjutavad krediidiasutuste omavahelist infovahetust rahapesu tõkestamise eesmärgil kõige enam *eesmärgikohasuse põhimõte* (IKÜM art 5 lg 1 p b) ning *võimalikult väheste andmete kogumise põhimõte* (IKÜM art 5 lg 1 p c). Eesmärgikohasuse põhimõtte järgi võivad krediidiasutused koguda isikuandmeid täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel (nt hoolsusmeetmete kohaldamiseks) ning ei või neid isikuandmeid hiljem töödelda viisil, mis on nende eesmärkidega vastuolus (nt turunduslikel eesmärkidel). Võimalikult väheste andmete kogumise põhimõtte järgi peavad isikuandmed olema asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt.

Krediidiasutuse kohustuseks on mistahes andmetöötlustoimingu algatamisel (sh infovahetuseks teiste krediidiasutustega) välja selgitada asjakohane isikuandmete töötlemise õiguslik alus. Võrdväärse kaitstuse taseme tagamiseks kõigis liikmesriikides näeb üldmääruse artikkel 6 ette ammendava ja piirava loetelu juhtudest, millal isikuandmete töötlemist võib pidada seaduslikuks. Rahapesu tõkestamise eesmärgil toimuva krediidiasutuste omavahelise infovahetuse korral on kõige asjakohasemad isikuandmete töötlemise õiguslikud alused töötlemine avalikes huvides oleva ülesande täitmiseks (IKÜM art 6 lg 1 p e) ning töötlemine õigustatud huvi korral (IKÜM art 6 lg 1 p f). Vastavat järeldust toetab asjaolu, et tegemist on krediidiasutustele antud õigusega vahetada omavahel pangasaladusega kaitstud teavet rahapesu tõkestamise eesmärgil, mitte õigusaktist tuleneva vastavasisulise kohustusega, milleks on koostöö tegemine järelevalve- ja korrakaitseasustustega.

Üldjuhul toimub krediidiasutuste omavahelise infovahetuse käigus isikuandmete töötlemine avalikes huvides oleva ülesande täitmiseks (IKÜM art 6 lg 1 p e). Vastavat järeldust toetab üldmääruse põhjenduspunkt 19, mille kohaselt toimub isikuandmete töötlemine rahapesuvastaste

meetmete rakendamiseks krediidiasutuste kui eraõiguslike asutuste poolt avalikes huvides oleva ülesande täitmiseks. Siseriiklikult rõhutab vastavat isikuandmete töötlemise õiguslikku alust ja eesmärki RahaPTS § 48 lõige 2, mille järgi võivad krediidiasutused RahaPTS rakendamisel kogutud isikuandmeid töödelda üksnes rahapesu ja terrorismi rahastamise tõkestamise eesmärgil, mida käsitatakse avaliku huvi küsimusena üldmääruse mõistes. Samas võib isikuandmete töötlemine rahapesu tõkestamise eesmärgil toimuda ka õigustatud huvi korral (IKÜM art 6 lg 1 p f). Artikli 29 andmekaitse töörühma arvamuse järgi võib üheks õigustatud huvi näiteks olla pettuse, teenuste kuritarvitamise või rahapesu takistamine. Seega annab üldmäärus krediidiasutusele võimaluse avaldada pangasaladusega kaitstud teavet kolmandatele isikutele, kellel on olemas õiguspärane huvi, mida krediidiasutus peab iga kord andmetöötluse algatamisel hindama.

Isikuandmete töötlemine õigustatud huvi alusel on seaduslik juhul, kui täidetud on kolm kumulatiivset tingimust: 1) andmete avaldamine peab olema vajalik kolmanda isiku õigustatud huvide teostamiseks; 2) isikuandmete töötlemine peab toimuma õigustatud huvide teostamiseks; 3) andmesubjekti põhiõigused ja -vabadused ei tohi olla vastutava töötleja või kolmandate isikute õigustatud huvide suhtes ülimuslikud. Vastanduvate õiguste ja huvide kaalumisel peab krediidiasutus lähtuma iga üksikjuhtumi konkreetsetest asjaoludest ning võtma arvesse andmesubjekti mõistlikke ootusi, andmesubjekti õiguste rikkumise raskust ning teatud juhtudel ka tema vanust. Andmesubjekti mõistlike ootuste puhul tuleb arvestada seda, kas andmesubjekt võis andmete kogumise ajal ja kontekstis mõistlikkuse piires eeldada, et isikuandmeid võidakse teatud otstarbel töödelda. Autori arvates ei saa andmesubjektil olla mõistlikku ootust, et algselt rahapesu tõkestamise eesmärgil hoolsusmeetmete kohaldamiseks kogutud isikuandmeid samal eesmärgil täiendavalt ei töödelda. Pigem on küsimus selles, kas andmesubjekti huvid ja põhiõigused kaaluvad teatud andmetöötluse olukorras ülesse krediidiasutuste huvid töödelda isikuandmeid rahapesu tõkestamise eesmärgil (nt huvi edastada teavet kahtlaste tehingute ja kõrgema riskiga klientide kohta teistele krediidiasutustele). Hea tava kohaselt tuleb õigsustatud huvi hindamine dokumenteerida piisavalt üksikasjalikult ja läbipaistvalt, et asjakohased sidusrühmad, sh andmesubjektid ja andmekaitseasutused ning lõppkokkuvõttes kohtud saaksid vajaduse korral kontrollida, et tehtud on terviklik ja nõuetekohane hindamine. Seega peaksid krediidiasutused õigustamatu andmetöötluse vältimiseks ning andmesubjekti kaitsva meetmena omavahelise infovahetuse käigus piisava põhjalikkusega dokumenteerima nii õigustatud huvi olemasolu kui ka erinevate huvide tasakaalustamise tulemused.

Seadusandja pole üldisetl pidanud vajalikuks detailselt reguleerida isikuandmete töötlemise ulatust krediidiasutuste omavahelise infovahetuse puhul. Üsna üldsõnaliselt reguleerib infovahetuse ulatust kuriteokahtlusega tehingute ja kõrgema riskiga klientide osas RahaPTS § 51 lõige 5 ning isikusamasuse tuvastamise, poliitilise taustaga isikute ja tegelike kasusaajate osas Raha PTS § 16 lõige 2 koosmõju RahaPTS § 20 lõige 1 punktid 1, 3 ja 5. Seejuures tuleb tähele panna, et tegelikke kasusaajaid ja isikute riiklikku tausta puudutav teave on oma iseloomult avalik, mistõttu ei saa selle suhtes esineda ootust privaatsusele. Seega on krediidiasutustele jäetud suhteliselt suur otsustusõigus ja tegevusvabadus rahapesu tõkestamise eesmärgil toimuva infovahetuse viisi ja ulatuse määramisel, mis muudab keerulisemaks ühtlase andmekaitse taseme saavutamise ning füüsiliste isikute kaitsmise isikuandmete õigustamatu töötlemise ja selle tagajärgede eest.

RahaPTS § 51 lõige 5 on krediidiasutuste omavahelise infovahetuse mõttes võtmetähtsusega säte siseriiklikus õiguses, mille sisustamise ja tõlgendamise osas vajaksid krediidiasutused täpsemaid juhiseid kas Rahapesu Andmebüroolt või Andmekaitse Inspektsioonilt. Küsimusi tekitab nii sätte asukoht (RahaPTS 5. peatükk), infovahetuse üldnormi (RahaPTS § 16 lg 1) ja erinormi (RahaPTS § 51 lg 5) vahekord kui ka sättes sisalduvad piisavalt määratlemata õigusmõisted (sh kõrge riskiga klient ja kuriteokahtlusega tehing). Nimelt on vastav säte paigutatud RahaPTS 5. peatükki, mis sätestab RAB teatamiskohustuse rahapesu kahtluse korral, ning RahaPTS paragrahvi 51, mis reguleerib RAB teate konfidentsiaalsust. Kahjuks ei täpsusta regulatsioonid ega neid selgitavad juhised, kas infovahetus kuriteokahtlusega tehingute ja kõrgema riskiga klientide osas eeldab põhjendatud rahapesu kahtluse tuvastamist ning RAB-ile teate esitamist, kas RAB teade tuleb esitada enne teiste krediidiasutuste teavitamist või tohib seda teha ka viivitamata pärast krediidiasutuste omavahelist infovahetust ning kas ebaharilike tehingute ja tegevuste puhul toimub krediidiasutuste omavaheline infovahetus samal õiguslikul alusel ja ulatuses, kui kuriteokahtlusega tehingute puhul.

Samuti on RahaPTS § 51 lõikes 5 kasutatavad mõisted (st kuriteokahtlusega tehing ja kõrgema riskiga klient) raskesti tõlgendatavad või piisavalt määratlemata. Näiteks on kuriteokahtlusega tehingu mõiste sisustamine keeruline seetõttu, et rahapesu kuriteo toimumise eelduseks on muu kuriteo ehk eelkuriteo toimepanemine. Eelkuriteoks võib samas olla iga karistusseadustiku eriosas sätestatud kuritegu, millest on saadud rahapesu objekt ehk kuritegeliku tegevuse tulemusel saadud vara. Väga lai eelkuritegude ring muudab keerulisemaks nii rahapesu kahtluse tuvastamise, RAB teatamiskohustuse täitmise kui ka krediidiasutuste omavahelise infovahetuse ulatuse määratlemise

kuriteokahtlusega tehingute osas. Kõrgema riskiga kliendi mõiste sisustamine on keeruline aga seetõttu, et kliendi riskiastme määramine on lõppkokkuvõttes iga krediidiasutuse diskretsiooniotsus, mis sõltub olulisel määral kliendi tausta ja tehingute kohta kogutud teabest, kasutatavast riskihindamise metoodikast, krediidiasutuse riskiisust jms. Seega pole võimalik kõrgema riskiga kliendi mõistet üheselt defineerida, mis muudab keeruliseks krediidiasutuste omavahelise infovahetuse õigusliku aluse ja ulatuse määratlemise kõrgema riskiga klientide osas. Kokkuvõttes võib järeldada, et ebaselgete või raskesti sisustatavate õigusmõistete korral tuleks isikuandmete töötlemise õiguslikke aluseid ja ulatust regulatsioonides või neid selgitavates juhendites täpsustada, et vältida isikuandmete põhjendamata töötlemist ja selle tagajärgi.

Lisaks leiab autor, et krediidiasutuses tehtavate tehingute arvu, mahtu, kiirust, tehingutega edastatavat teavet ning piiratud aja- ja tööjõuressurssi arvesse võttes, on ebarealistlik eeldada, et krediidiasutused suudavad tõkestada rahapesu selle juriidilises tähenduses ehk tuvastada kahtlusepõhiselt ning piisavatele tõenditele tuginedes majandussüsteemi kahjustavaid tehinguid ja neid ennetavalt ära hoida. M. Mäekeri jt hinnangul oleme jõudnud ajas selleni, kus eraõiguslikud isikud (sh krediidiasutused) peavad teatama juba kahtlasest tehingust või tegevusest, neid tehinguid ära hoidma ning tõkestama sisuliselt igasugust kuritegevust, mis isegi ei pruugi olla jõudnud rahapesu staadiumisse. Autori arvates peaks rahapesu tõkestamise regulatsioonid või neid täiendavad juhised andma selgemaid juhtnööre krediidiasutuste omavahelise infovahetuse osas, mis puudutab kuriteokahtlusega tehinguid ning muid kahtlaseid või ebaharilikke tehinguid ja tegevusi, sh kas või millise juhul peab infovahetusele eelnema või järgnema RAB teate esitamine.

Kokkuvõttes on rahapesu tõkestamise valdkonnas toimunud üldine paradigma muutus. Rahapesu ennetavad meetmed on sarnaste põhimõtetega kehtinud juba aastakümneid, mistõttu pole küsimus normide või kohustuste puudumises, kuid aastate jooksu on muutunud pankadelt oodatav hoolsus, selle ulatus ja tähendus. M. Mäekeri ja A. Nõmme arvates vaadatakse kunagisi tehinguid liigselt tänastele teadmistele tuginedes ning pankade hoolsust ei hinnata enam pelgalt skaalal, kas suudeti tõkestada rahapesu ja terrorismi rahastamist, vaid kas suudetakse ära hoida kahtlane tehing ja tegevus, mis võib viidata ükskõik millisele kuriteole. See on tõstnud pankadelt oodatava hoolsuse taseme rahapesu riskide tuvastamisel väga kõrgeks ning teinud pangad väga ettevaatlikuks, kuna avalikkuse ees võidakse sattuda hätta ka tehingutega, mida ei kvalifitseerita niivõrd seaduslikkuse järgi, vaid eetilistest tõekspidamistest lähtudes. Varasemalt tavapärane tuleb täna kvalifitseerida kui kahtlane. Sarnane paradigma muutus võib toimuda aastate pärast ka andmekaitse valdkonnas,

mille tulemusel täna krediidiasutuste omavahelises infovahetuses asjakohaseks, oluliseks, vajalikuks peetav isikuandmete töötlemine võib tulevikus valdkonna regulatsioonide, juhiste, kohtupraktika ja üldise suhtumise muutudes osutuda ebaproportsionaalseks või lausa lubamatuks. Seega täna õiguspäraseks ja proportsionaalseks peetavat andmetöötlust võidakse tulevikus hinnata kui õigustamatut ja ebaproportsionaalset. Krediidiasutuste omavahelise infovahetuse piisavalt üksikasjalikud juhised peaksid aitama taolisi olukordi ennetada ja vältida.

RAB hinnangul, mida automatiseeritumalt ja ühtlustatumalt toimib teadete ja spontaanse info vahetamise süsteem Euroopa Liidu liikmesriikide vahel, seda suurem on kasu rahapesu tõkestamise süsteemile. Krediidiasutuste omavahelise infovahetuse ühtlustamine ja automatiseerimise suunas on Eesti suuremad krediidiasutused juba samme astunud. Nimelt ühinesid neli suuremat Eesti krediidiasutust (sh LHV, Swedbank, SEB ja Luminor) 2020. aastal pilootprojektiga AML Bridge, mida arendab Eesti finantstehnoloogia ettevõte Salv Technologies OÜ. Tegemist on teabe- ja andmevahetusplatvormiga, mis võimaldab krediidiasutuste omavahelist infovahetust rahapesu tõkestamise eesmärgil kooskõlas kehtivate rahapesu, pangasaladuse ja andmekaitse normidega. Käesoleva töö autor pooldab infotehnoloogiliste lahenduste kasutuselevõtmist rahapesu tõkestamise valdkonnas, kuid tänane õigusraamistik ei pruugi tagada isikuandmete seaduslikku ja õiglast töötlemist krediidiasutuste omavahelise infovahetuse käigus rahapesu tõkestamise eesmärgil, kuna infovahetuse õiguslikud alused ja ulatus pole regulatsioonides ja neid selgitavates juhistes piisavalt üksikasjalikult ja üheselt mõistetalt määratletud, et tagada rahapesuvastaste meetmete ja andmekaitse põhimõtete ühetaoline rakendamine ning vähendada isikuandmete õigustamatu töötlemise juhtumeid (sh *AML Bridge* lahendust kasutades) ja nende võimalikke negatiivseid tagajärgi. Salv Technologies OÜ arvates on pilootprojekti suurimaks väljakutseks samuti kliendiandmete kasutamise ulatuse määratlemine, mistõttu aitaks valdkonnaülesed suunised muuta infovahetuse õigusraamistiku selgemaks. Loodetavasti toetab lähiaastatel vastu võetav uus rahapesu tõkestamise pakett (st otsekohalduv määrus) läbi ühtlustatud põhimõtete ja regulatsioonide ka kohustatud isikute vahelist infovahetust.

Kokkuvõttes peaks krediidiasutuste omavaheline infovahetus rahapesu tõkestamise eesmärgil lihtsustama hoolsusmeetmete kohaldamiseks vajaliku teabe kogumist, kõrgema riskiga klientide ja kuriteokahtlusega tehingute tuvastamist ning süütegude avastamist ja tõkestamist, kuid sellega võivad kaasneda ka negatiivsed tagajärjed. Mainekahju ja võimalikud regulatiivsed sanktsioonid on muutnud krediidiasutused ärisuhete loomisel ja jätkamisel üha valivamaks ja ettevaatlikumaks

ning vähendanud krediidiasutuste riskiisu kõrgema riskiga klientide ja jurisdiktsioonide osas, mis teatud juhtude on kaasa toonud ärisuhete lõpetamise ja arvelduskontode sulgemise ning vähendanud finantsteenuste kättesaadavust kliendigruppidele, kelle riskitase on hinnatud tavapärasest kõrgemaks. Rahapesu tõkestamise eesmärgil toimuv krediidiasutuste omavaheline infovahetus võib vähendada füüsiliste isikute ligipääsu finantsteenustele, kuna edastatud teabe põhjal suureneb oht, et krediidiasutused hakkavad vältima riske nende maandamise asemel (ingl de-risking) ning sulgevad pangakontod ja lõpetavad ärisuhted kõrgema riskiga klientidega. Kuna andmesubjektide võimalused tutvuda krediidiasutuste omavahelise infovahetuse käigus edastatud teabega, antud hinnangute ja tehtud otsustega on piiratud, suureneb krediidiasutuste vastutus isikuandmete kaitse ning (põhi)makseteenuste kättesaadavuse tagamisel (sh kõrgema riskiga klientidele) ning järelevalveasutuste olulisus vastava tegevuse üle kontrolli teostamisel.

Exchange of Information Between Credit Institutions for the Purpose of Preventing Money Laundering from the Perspective of Personal Data Protection. Summary

The European Union (EU) is committed to fighting against money laundering and terrorist financing, both within the EU and worldwide. The EU has developed a strong legal framework to combat money laundering, which is supported by the case law of the European Court of Justice. Today, in addition to public institutions, companies (incl. large corporations with a global reach) are increasingly processing personal data, which means that data subjects may not perceive in the light of these developments what and to what extent their personal data are processed and how and to what extent their rights can be effectively protected.

The activities of credit institutions in preventing money laundering and terrorist financing, maintaining banking secrecy, protecting personal data and providing basic payment services are quite complex in a rapidly changing technological and regulatory environment, as they require a thorough knowledge of private law, public law and criminal law; compliance with the principles enshrined in the Treaties and (directly applicable) EU regulations; orientation in international, EU and national regulations, standards and other guidelines; and dealing with conflicts of fundamental rights (e.g., freedom of establishment vs. data protection).

In 2020, four major Estonian credit institutions (including LHV, Swedbank, SEB and Luminor), whose combined market shares account for almost 90% of the Estonian banking market, merged with the *AML Bridge* pilot project, which is being developed by the Estonian financial technology company Salv Technologies OÜ. AML Bridge is an information and data exchange platform that enables credit institutions to exchange anti-money laundering information quickly, securely and reliably through a technical solution that complies with applicable money laundering, banking secrecy and data protection standards. The author of this thesis is in favor of the introduction of new information technology solutions in the field of money laundering prevention. However, the current legal framework may not sufficiently support the data exchange between credit institutions for AML purposes, as the legal bases and scope of data exchange are not clear and unambiguous to ensure uniform treatment and implementation of AML measures and thereby reduce the possibilities for unjustified processing of personal data and its negative consequences.

The purpose of this thesis was to analyze the current anti-money laundering and data protection legal framework in order to determine whether the legal bases and scope of data exchange between credit institutions for AML purposes are sufficiently clear and unambiguous to protect individuals from unauthorized processing of personal data and possible negative consequences. The research questions posed in this thesis are as follows:

(1) On what legal basis and to what extent is the processing of personal data permitted in the data exchange between credit institutions for the AML purposes?
(2) What principles and restrictions must credit institutions take into account when processing personal data in the data exchange between credit institutions for the AML purposes?

The initial hypotheses of the work were formulated as follows:

(1) The legal bases and scope of the data exchange between credit institutions for the AML purposes are not defined in sufficient detail and unambiguously in the regulations and guidelines in order to protect natural persons against unjustified processing of personal data and possible negative consequences.
(2) The data exchange between credit institutions for AML purposes may reduce the access of natural persons to financial services, as the provided information may increases the risk that banks close accounts and terminate business relationships with high-risk customers due to *de-risking*.

In order to answer both questions, the AML and data protection legal frameworks and applicble provisions were analysed to identify possible problems and to determine the most appropriate legal bases for personal data processing and the factors affecting the data processing. A separate chapter was dedicated to the data exchange between credit institutions on suspicious transactions and higher-risk customers, as those are sufficiently undefined legal concepts, which make it difficult to define the legal basis and scope of the data processing.

Credit institutions shall apply due diligence measures (including *know-your-customer* principle) to their customers both when establishing and in the course of a business relationship. Banks gather customer data to provide banking services that meet their needs and to comply with international and national regulations to prevent money laundering, terrorist financing, corruption and other economic crimes. Credit institutions must process personal data collected for the AML purposes

in accordance with applicable data protection standards, which means that there must always be a legal basis for personal data processing and the principles and restrictions on data processing must be respected (including purpose limitation, data minimisation, etc.). In terms of cooperation and data exchange between credit institutions, it is important to define the legal bases, purpose and scope of personal data processing in order to prevent unjustified processing of personal data and ensure that information protected by banking secrecy is disclosed to third parties (including other credit institutions) only on the basis and to the extent provided by law.

Any processing of personal data must be lawful and fair in order to avoid interfering with the data subject's right to privacy and the protection of personal data. The prevention, investigation and detection of criminal offenses are objectives in the public interest for which a restriction on the rights of individuals is considered lawful if it respects the nature of fundamental rights and freedoms and is necessary and proportionate. The prevention of money laundering is based on a public interest objective (i.e. the detection and prevention of criminal offenses), which is why an interference with the fundamental rights of the individual can generally be considered legitimate if credit institutions process personal data for the AML purposes.

The data exchange between credit institutions for AML purposes is mainly regulated in national law by the following provisions – KAS § 88 and RahaPTS § 16 (1) and § 51 (5). RahaPTS § 16 (1) enables all obligated persons to cooperate for the purpose of preventing money laundering (incl. forwarding and exchanging information and answering inquiries), observing the obligations and restrictions arising from legislation. However, pursuant to RahaPTS § 51 (5), only credit and financial institutions may exchange information on higher-risk customers and suspicious transactions for the purpose of preventing money laundering. The obligation to maintain banking secrecy, the personal data protection requirements and the confidentiality of suspicious activity reporting are the main restrictions that credit institutions must take into account in the data processing. In addition to the principle of lawfulness, the pupose limitation (GDPR Art 5 (1) (b)) and the mimimisation principle (GDPR Art 5 (1) (c)) have the greatest impact on the data exchange between credit institutions.

The obligation of a credit institution is to determine an appropriate legal basis for data processing upon initiation of any data processing operation (incl. data exchange with other credit institutions). In order to ensure an equivalent level of protection in all Member States, Article 6 of the GDPR

provides an exhaustive and restrictive list of cases in which the processing of personal data may be considered lawful. For the purpose of preventing money laundering, the most appropriate legal bases for personal data processing is processing in the public interest (GDPR Art 6 (1) (e)) and processing for the purpose of legitimate interest (GDPR Art 6 (1) (f)). This conclusion is supported by the fact that cooperation for AML purposes is an opportunity (not an obligation) for obligated persons, but cooperation with supervisory and law enforcement authorities for the same purpose is an obligation (not an option) imposed on obligated persons by law. As a rule, personal data is processed in the public interest (GDPR Art 6 (1) (e)) in the data exchange between credit institutions for the AML purposes. This view is reflected in recital 19 of the GDPR and in RahaPTS § 48 (2).

Nevertheless, the personal data may also be processed for the purpose of legitimate interest (GDPR Art 6 (1) (f))). In the opinion of the Article 29 Data Protection Working Party, one of the legitimate interests may be, *inter alia*, the prevention of fraud, abuse of money or money laundering. The processing of personal data for the purpose of a legitimate interest is lawful if three cumulative conditions are met: 1) the disclosure of the data must be necessary for the exercise of the legitimate interests of a third party; 2) the processing of personal data must take place for the performance of legitimate interests; 3) the fundamental rights and freedoms of the data subject shall not take precedence over the legitimate interests of the controller or third parties. In all such cases the major question is whether the interests and fundamental rights of the data subject outweigh the interests of the credit institutions in processing certain personal data for the AML purposes (e.g., exchange data on suspicious transactions and high-risk customers). Good practice requires that the assessment of a legitimate interest is documented in sufficient detail to allow relevant stakeholders, including data subjects and data protection authorities, and ultimately the courts, to verify, where appropriate, that a complete and proper assessment of legitimate interest has been made. Therefore, in order to avoid unjustified data processing and as a measure to protect the data subject, credit institutions should document in sufficient detail in the data exchange both the existence of a legitimate interest and the results of the balancing of different interests.

The legislator has not considered it necessary to regulate in detail the scope of personal data processing in data exchange between credit institutions. Quite generally, the scope of information exchange is regulated by RahaPTS § 51 (5) for suspicious transactions and high-risk customers and by RahaPTS § 16 lg 2 for identifying natural persons, politically exposed persons and

beneficial owners. The data related to politically exposed persons and beneficial owners is public in nature, so there can be no expectation of privacy. Thus, credit institutions have a relatively large margin of discretion to determine the manner and extent of data exchange between credit instiurions, which makes it more difficult to achieve a uniform level of data protection and protect individuals from unauthorized processing of personal data and its possible negative consequences.

RahaPTS § 51 (5) is a key provision in national law in terms of the data exchange between credit institutions. The provision is placed in RahaPTS Chapter 5, which stipulates the obligation to notify FIU in case of money laundering suspicion. Unfortunately, the regulations and guidelines do not specify whether, in which cases and when a SAR has to be filed to FIU in relation to the data exchange between credit intitutions for the AML purposes, especially when data on unusual transactions and activities is processed. Besides, the terms used in RahaPTS § 51 (5) are not sufficiently defined and are difficult to interpret. For example, the transactions suspected of a criminal offence are difficult to define, as a money laundering crime is related to a predicate offense, but a predicate offense may be any criminal offense provided for in the Penal Code. The wide range of predicate offenses make it more difficult to identify suspicious transactions, to comply with reporting obligations to the FIU, as well as to determine the extent of the data exchange between credit institutions on suspicious transactions. The high-risk customer is difficult to define, as the risk level is the discretionary decision of each credit institution, which depends on the gathered data and client activities, the risk assessment methodology used, the risk appetite, etc. Thus, it is not possible to unambiguously define the concept of a high-risk customer, which makes it difficult to define the legal basis and scope of the data exchange between credit institutions for high-risk customers. In conclusion, in the case of unclear or insufficiently defined legal terms or concepts, the legal bases and scope of data processing should be specified in the regulations and guidelines to avoid unjustified processing of personal data and their possible negative effects.

In addition to the above, taking into account the number, volume and speed of transactions and the limited number of staff, it is unrealistic to assume that credit institutions are able to prevent money laundering in its legal sense, i.e., to identify suspicious transactions based on sufficient evidence and preventively. According to M. Mäeker *et al*, we have reached a point where obliged persons (incl. credit institutions) have to report a suspicious transaction or activity, prevent such transactions and prevent virtually any crime that have not even reached the stage of money laundering. All in all, there has been a general paradigm shift in AML. The AML measures have

been in place for decades with similar principles, but the diligence expected from banks, its scope and meaning have changed over the years. The level of due diligence expected of banks in identifying money laundering risks has made banks very cautious, as the public may also face transactions that do not qualify as legal but ethical. According to M. Mäeker *et al*, previous transactions are evaluated on the basis of current knowledge and qualified as suspicious today. A similar paradigm shift may take place years later in the field of data protection, as a result of which the processing of personal data considered relevant, important and necessary today may turn out to be disproportionate or even unacceptable in the future. Sufficiently detailed guidelines for the data exchange between credit institutions for the AML purposes should help to prevent and avoid such situations.

In conclusion, the data exchange between credit institutions for AML purposes should facilitate the collection of information necessary for the application of due diligence measures, the identification of high-risk customers and suspicious transactions, and the detection and prevention of criminal offenses, but may also have negative consequences. Reputation and possible regulatory sanctions have made credit institutions more selective and cautious in establishing and maintaining business relationships and have reduced their exposure to high-risk customers and jurisdictions, which in some cases has led to business closures and current account closures and reduced access to financial services. Thus, the data exchange between credit institutions for the AML purposes may reduce the access of natural persons to financial services, as the provided information may increases the risk that banks close accounts and terminate business relationships with high-risk customers due to *de risking*.

KASUTATUD LÜHENDID

AMLD4	20. mai 2015. aasta Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2015/849 (nn neljas rahapesuvastane direktiiv)
AMLD5	30. mai 2018. a Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2018/843 (nn viies rahapesuvastane direktiiv)
AMLD6	23. oktoobri 2018. aasta Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2018/1673 (nn kuues rahapesuvastane direktiiv)
FATF	Rahapesuvastane töökond (ingl *Financial Action Task Force*)
MONEYVAL	Euroopa Nõukogu rahapesu vastase võitlusega tegelev ekspertkomitee (ingl *Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism*)
STR	Rahapesu või rahapesuga seotud muu kuriteo kahtlusega teade ehk rahapesukahtlusega teade (ingl *Suspicious Transaction Report*)
UAR	Ebahariliku tegevuse teade (ingl *Unusual Activity Report*)
UTR	Ebahariliku tehingu teade (ingl *Unusual Transaction Report*)

KASUTATUD KIRJANDUS

1. Agarmaa, M. Maksejõuetuse revisjon. Pankrotiavalduse esitamine, pankrotimenetluse raugemine, pankroti välja kuulutamine ja tagajärjed, pankrotivara moodustamine, pankrotivara valitsemine. 2018. - https://www.just.ee/sites/www.just.ee/files/mari_agarmaa_analuus-kontseptsioon.pdf (09.04.2022).
2. Andmekaitse Inspektsioon. Isikuandmete töötleja üldjuhend. Kinnitatud 31.05.2018, muudetud 28.09.2018 ja 19.03.2019. - https://www.aki.ee/sites/default/files/dokumendid/isikuandmete_tootleja_uldjuhend.pdf (21.10.2021). Viidatud: AKI. Isikuandmete töötleja üldjuhend
3. Andmekaitse Inspektsioon (AKI). Pankade seire seoses isikuandmete töötlemisega nõusoleku alusel ja lepingu täitmiseks. Isikuandmete kaitse seaduse täitmise seire. Tallinn: Andmekaitse Inspektsioon 2013. - https://www.aki.ee/sites/default/files/seired/Pankade_seire2013.pdf (09.03.2022).
4. Artikli 29 alusel asutatud andmekaitse töörühm. Arvamus 06/2014 andmete vastutava töötleja õigustatud huvide mõiste kohta direktiivi 95/46/EÜ artikli 7 tähenduses. 844/14/ET, WP 217, 09.04.2014. Viidatud: Arvamus 06/2014 õigustatud huvide mõiste kohta
5. Artikli 29 alusel asutatud andmekaitse töörühm. Arvamus 15/2011 nõusoleku määratluse kohta. 01197/11/ET, WP187, 13.07.2011, lk 3. Viidatud: Arvamus 15/2011 nõusoleku määratluse kohta
6. Artikli 29 alusel asutatud andmekaitse töörühm. Suunised määruse (EL) 2016/679 kohase nõusoleku kohta. 17/ET, WP 259 rev. 01, 28.11.2017, muudetud 10.04.2018.
7. Bello, A. U., Harvey, J. From a Risk-Based to an Uncertainty-Based Approach to Anti-Money Laundering Compliance. – Security Journal 2016/30 (1).
8. Bilali, G. Know Your Customer - Or Not. - University of Toledo Law Review 2012/43.
9. Bogdanov, D., Siil, T. Infotehnoloogilised võimalused põhiõiguste kaitsel. – Juridica 2020/8.
10. Broekhoven, L. van, Goswami, S. Can Stakeholder Dialogues Help Solve Financial Access Restrictions Faced by Non-Profit Organizations That Stem from Countering

Terrorism Financing Standards and International Sanctions? – International Review of the Red Cross 2022/103 (917).

11. Böszörmenyi, J., Schweighofer, E. A Review of Tools to Comply with the Fourth EU Anti-Money Laundering Directive. International Review of Law, Computers & Technology 2015/ 29 (1).
12. Commission Nationale Informatique & Libertés (CNIL). When Trust Pay Off. Today's and tomorrow's means of payment facing the challenge of data protection. White Paper Collection - No 2, 23 February 2022. - https://www.cnil.fr/sites/default/files/atoms/files/cnil-white-paper_when-trust-pays-off.pdf (03.03.2022).
13. de Koker, L. Identifying and Managing Low Money Laundering Risk: Perspectives on FATF's Risk-Based Guidance. – Journal of Financial Crime 2009/16 (4).
14. Durner, T., Shetret, L. Understanding Bank De-Risking and Its Effects on Financial Inclusion. An exploratory study. OXFAM International, Global Center on Cooperative Security, Research Report, 18 November 2015. - https://www.oxfam.org/en/research/understanding-bank-de-risking-and-its-effects-financial-inclusion (15.02.2022).
15. Egmont Group. Organization and Structure. - https://egmontgroup.org/about/organization-and-structure/ (01.03.2022).
16. Euroopa andmekaitseõiguse käsiraamat. 2018. aasta väljaanne. Luxembourg: Euroopa Liidu Väljaannete Talitus 2020. - https://www.echr.coe.int/Documents/Handbook_data_protection_EST.pdf (15.01.2022). Viidatud: Euroopa andmekaitseõiguse käsiraamat
17. Euroopa Komisjon. Ettepanek: Euroopa Parlamendi ja Nõukogu Määrus, millega asutatakse rahapesu ja terrorismi rahastamise tõkestamise amet ning muudetakse määruseid (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010. COM(2021) 421 final, 2021/0240(COD). Brüssel, 20.7.2021. - https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52021PC0421&from=EN (01.04.2022).
18. Euroopa Komisjon. Komisjoni teatis Euroopa Parlamendile ja Nõukogule. Andmekaitse kodanike võimestajana ja ELi valmistumine digiüleminekuks – isikuandmete kaitse üldmääruse kohaldamise kaks esimest aastat. COM(2020) 264 final. Brüssel, 24.6.2020. -

https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52020DC0264&from=EN (15.02.2021).

19. Euroopa Komisjon. Komisjoni teatis tegevuskava kohta, mis käsitleb liidu terviklikku poliitikat rahapesu ja terrorismi rahastamise ärahoidmiseks. – ELT C 164, 13.05.2020, lk 21-33.
20. European Commission. Factsheet: Stronger EU Rules to Fight Financial Crime. July 2021. - https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/210720-anti-money-laundering-countering-financing-terrorism-factsheet_en.pdf (01.04.2022).
21. European Banking Authority (EBA). Suunised, mis on koostatud direktiivi (EL) 2015/849 artikli 17 ja artikli 18 lõike 4 alusel, milles käsitletakse kliendi suhtes rakendatavaid hoolsusmeetmeid ning tegureid, mida krediidi- ja finantseerimisasutused peaksid arvestama, kui hindavad üksikute ärisuhete ja juhutehingute rahapesu ja terrorismi rahastamise riski (edaspidi „rahapesu ja terrorismi rahastamise riskitegurite suunised“), millega tunnistatakse kehtetuks ja asendatakse suunised JC/2017/37. EBA/GL/2021/02, 1. märts 2021. - https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20ML-TF%20risk%20factors%20%28revised%29%202021-02/Translations/1016926/Guidelines%20ML%20TF%20Risk%20Factors_ET.pdf (14.09.2021). Viidatud: EBA riskitegurite suunised
22. European Supervisory Authorities (ESAs). Joint Guidelines on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis. The Risk-Based Supervision Guidelines. Joint Guidelines. ESAs 2016 72, 16 November 2016. - https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1663861/7159758d-8337-499e-8b12-e34911f9b4b6/Joint%20Guidelines%20on%20Risk-Based%20Supervision%20%28ESAS%202016%2072%29.pdf?retry=1 (14.09.2021).
23. Evestus, S.-H. Eelkuriteo sisustamine rahapesukuriteo puhul. Rahapesu mõiste Eesti karistusõiguses. – Juridica 2015/5.

24. FATF. Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion – With a Supplement on Customer Due Diligence. Paris, 2013-2017. – www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html (02.10.2021).
25. FATF. Consolidated FATF Standards on Information Sharing. Relevant excerpts from the FATF Recommendations and Interpretive Notes. Updated November 2017. - https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Consolidated-FATF-Standards-information-sharing.pdf (21.02.2022).
26. FATF. FATF IX Special Recommendations. October 2001 (incorporating all subsequent amendments until February 2008). Paris, 2008. - http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf (20.10.2021).
27. FATF. Guidance for a Risk-Based Approach. The Banking Sector. Paris, October 2014. – https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf (01.10.2021).
28. FATF. Guidance for Financial Institutions in Detecting Terrorist Financing. 24 April 2002. - https://www.fatf-gafi.org/media/fatf/documents/Guidance%20for%20financial%20institutions%20in%20detecting%20terrorist%20financing.pdf (21.03.2022).
29. FATF. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations. Updated March 2022. Paris, 2012-2022. - http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (01.04.2021). Viidatud: FATF Recommendations (2012-2022)
30. FATF. The Forty Recommendations of the Financial Action Task Force on Money Laundering. Paris, 1990. – http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf (20.10.2021).
31. Feldmanis, L., Ploom, T. Rahapesu kriminaliseerimine: kelle suhtes ja millise põhjendusega? – Juridica 2007/3.

32. Finantsinspektsioon. Finantsinspektsiooni soovituslik juhend „Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks“. Kehtestatud Finantsinspektsiooni juhatuse 26.11.2018. a otsusega nr 1.1-7/172. - https://www.fi.ee/sites/default/files/2018-11/FI_AML_Soovituslik_juhend.pdf (14.09.2021). Viidatud: Finantsinspektsiooni soovituslik juhend
33. Finantsinspektsiooni seaduse ja teiste seaduste muutmise seaduse eelnõu 326 SE seletuskiri. 08.02.2021, lk 11. - https://www.riigikogu.ee/tegevus/eelnoud/eelnou/adf3f17b-4142-451e-bed3-15ebc706458f/Finantsinspektsiooni%20seaduse%20ja%20teiste%20seaduste%20muutmise%20seadus (15.01.2022).
34. FinCen. History of Anti-Money Laundering Laws. U.S. Treasury, The Financial Crimes Enforcement Network. - https://www.fincen.gov/history-anti-money-laundering-laws#:~:text=The%20BSA%20was%20established%20in,tools%20to%20combat%20money%20laundering (08.03.2022).
35. Hartzog, W., Richards, N. Privacy's Constitutional Moment and the Limits of Data Protection. – Boston College Law Review 2020/61 (5).
36. Ilus, T. Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste Kohtu lahendite valguses. – Juridica 2005/VIII.
37. Ilus, T. Isikuandmete kaitse olemus ja arengusuunad. – Juridica 2002/VII.
38. Jäärats, E. Pankade diskretsiooniõigus tunne-oma-klienti põhimõtte täitmisel ning selle negatiivsed tagajärjed. Uurimistöö. Tallinn: TÜ õigusteaduskond 2019.
39. Kairjak, M. Majanduskaristusõigus karistusõiguse revisjoni raames. – Juridica 2014/VIII.
40. Kihuoja, T. Isikuandmete kaitse õiguse riived rahapesu ja terrorismi rahastamise tõkestamiseks kohaldatavate hoolsusmeetmete käigus ning õiguslikud alused isikuandmete töötlemiseks krediidiasutustel. Magistritöö. Tartu: TÜ õigusteaduskond 2021.
41. Levi, M. Evaluating the Control of Money Laundering and Its Underlying Offences: The Search for Meaningful Data. – Asian Journal of Criminology 2020/15.
42. Liivat, E. Pangasaladuse kontseptsiooni muutumine ajas. Bakalaureusetöö. Magistritöö. Tallinn: TÜ õigusteaduskond 2013.

43. Lowe, R. J. Anti-Money Laundering – the Need for Intelligence. – Journal of Financial 2017/24 (3).
44. Madise, Ü. (toim) jt. Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne. Komm vlj. Tallinn: Juura 2020. - https://pohiseadus.ee/ (01.10.2022).
45. MONEYVAL. Report. "De-Risking" Within MONEYVAL States and Territories. Council of Europe, Strasbourg, 15 April 2015. - https://rm.coe.int/report-de-risking-within-moneyval-states-and-territories/168071510a (20.11.2021). Viidatud: MONEYVAL. Report on "De-Risking"
46. Mäeker, M, Nõmm, A. The AML Compliance Book. 150 Golden Rules. Tallinn: Tallinna Raamatutrükikoja OÜ 2020.
47. Mäeker, M., Nõmm, A. Pangasaladuse hoidjast politseinikuks: valikud rahapesu tõkestamisel. – Juridica 2020/8. Viidatud: Mäeker/Nõmm (2020)
48. Myers, J. M. International Strategies to Combat Money Laundering. Financial Crimes Enforcement Network U.S. Department of the Treasury for the International Symposium on the Prevention and Control of Financial Fraud. Beijing, 19-22 October 1998, lk 4. - https://icclr.org/wp-content/uploads/2019/06/myer_pap.pdf?x94276 (21.01.2022)
49. Nguyenm, C. L. Preventing the Use of Financial Institutions for Money Laundering and the Implications for Financial Privacy. – Journal of Money Laundering Control 2018/21 (1).
50. Pellegrina, L. D., Masciandaro, D. The Risk Based Approach In The New European Anti-Money Laundering Legislation: A Law And Economics View. – Review of Law and Economics 2009/5 (2).
51. Pikknurm, K. Investeerimisühingu vastavuskontrolli teostaja ja juhatuse vastutus rahapesu tõkestamisel Eesti õigusruumis. – Tallinn: TÜ õigusteaduskond 2018.
52. Raa, R., Siibak, K. Pangasaladus. – Juridica 2002/3.
53. Rahapesu Andmebüroo. Aastaraamat 2020. Ülevaade Rahapesu Andmebüroo tegevusest 2020. aastal. RAB: Tallinn 2021. - https://fiu.ee/aastaraamatud-ja-uuringud/aastaraamatud#item-1 (01.03.2021). Viidatud: RAB aastaraamat 2020
54. Rahapesu Andmebüroo. Juhend kahtlaste tehingute tunnuste kohta. Kinnitatud Rahapesu Andmebüroo poolt 06.05.2019. -

https://www.politsei.ee/files/Rahapesu/juhendkahtlastetehingutetunnustekohta.pdf?222a84e8fa (20.01.2021). Viidatud: RAB juhend

55. Rahapesu ja terrorismi rahastamise tõkestamise seaduse eelnõu 459 SE seletuskiri. 04.05.2017. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/fb03e20e-caf7-463d-9b60-ddf6021742b2/Rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20seadus (14.09.2021).
56. Rahapesu ja terrorismi rahastamise tõkestamise seaduse ja teiste seaduste muutmise seaduse eelnõu 130 SE seletuskiri. 19.12.2019. - https://www.riigikogu.ee/tegevus/eelnoud/eelnou/69421167-7e69-4383-b2f8-b9f2912a13e6/Rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20seaduse%20ja%20teiste%20seaduste%20muutmise%20seadus (15.01.2022).
57. Rahapesu ja terrorismi rahastamise tõkestamise seaduse ja teiste seaduste muutmise seaduse eelnõu 507 SE seletuskiri. 10.01.2022. - https://www.riigikogu.ee/tegevus/eelnoud/eelnou/ffe848a6-7b78-43cf-b106-720915882205/Rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20seaduse%20ja%20teiste%20seaduste%20muutmise%20seadus (25.02.2022).
58. Rummi, P. Andmesubjekti kaitse profiilianalüüsil põhinevate automatiseeritud otsuste tegemise regulatsiooni rakendamisel krediidiasutuste tingimuste näitel. Magistritöö. Tallinn: TÜ õigusteaduskond 2020.
59. Salv. Towards a New Standard in AML/CTF. The case for FinCrime Intelligence Sharing – an In-Depth Look at the AML Bridge Estonia Pilot. April 2021. - https://salv.com/assets/files/AML%20Bridge%20Estonia%20whitepaper.pdf (26.11.2021). Viidatud: Salv AML Bridge
60. Sarapuu, T. Piiriülese investeerimisteenuse osutamine ja kliendi isikusamasuse tuvastamine. Magistritöö. Tallinn: TÜ õigusteaduskond 2015.
61. Sein, K., Mikiver, M., Tupay, P. K. Pilguheit andmesubjekti õiguskaitsevahenditele uues isikuandmete kaitse üldmääruses. – Juridica 2018/2.
62. Sesterikova, K. Euroopa Parlamendi ja Nõukogu 20.05.2015 direktiivist (EL) 2015/849 tuleneva riskipõhise lähenemise ja Eesti kohtupraktikas väljatöötatud majandusliku põhjendatuse kriteerium. Magistritöö. Tartu: TÜ õigusteaduskond 2016.

63. Siclari, D. The New Anti-Money Laundering Law. First Perspectives on the 4th European Union Directive. New York: Palgrave Pivot 2016.
64. Sootak, J., Pikamäe, P. (toim) jt. Karistusseadustik. Kommenteeritud väljaanne. 4., täiend. ja ümbertööt. vlj. Tallinn: Juura 2015.
65. Sootak, J., Pikamäe, P. (koost) jt. Karistusseadustik. Kommenteeritud väljaanne. 5., täiend. ja ümbertööt. vlj. Tallinn: Juura 2021. Viidatud: KarS Komm (2021)/Autor
66. Takats, E. A Theory of Crying Wolf: The Economics of Money Laundering Enforcement. Journal of Law, Economics, & Organization 2011/27 (1).
67. Tellisaar, L. Tegelike kasusaajate registri ülesanne rahapesu tõkestamisel. Magistritöö, Tallinn: TTÜ majandusteaduskond 2018.
68. Tibar, I. Rahapesu: kujunemislugu ja koosseis Eesti karistusõiguses. Magistritöö, Tartu Ülikooli õigusteaduskond 2007.
69. Tibar, I. Tähelepanekuid uue rahapesu ja terrorismi rahastamise tõkestamise seaduse jõustumisega seoses. – Juridica 2018/1. Viidatud: Tibar, I. (2018)
70. Tikk, E. Informatsioonilise enesemääratlemise rahvusvahelis-õiguslik raamistik, sisustamine Eesti õiguses ja selle praktilisest kohaldamisest veebikeskkonnas. Tartu: Tartu Ülikool 2004.
71. Ulst, I. Rahapesu ja terrorismi finantseerimine: regulatiivsed aspektid ja finantssüsteemi kaitsmine. – Juridica 2003/7.
72. Õiguskantsler. Märgukiri põhimakseteenuste tagamise kohta. Õiguskantsler Ülle Madise märgukiri rahandusminister Martin Helmele, nr 6-1/191286/2001261, 10.03.2020. - https://www.oiguskantsler.ee/sites/default/files/field_document2/M%C3%A4rgukiri%20p%C3%B5himakseteenuste%20tagamise%20kohta.pdf (20.11.2021). Viidatud: Õiguskantsler. Märgukiri põhimakseteenuste tagamise kohta

KASUTATUD ÕIGUSAKTID

73. 4. detsembri 2001. a Euroopa Parlamendi ja Nõukogu direktiiv 2001/97/EÜ, millega muudetakse Nõukogu direktiivi 91/308/EMÜ rahandussüsteemi rahapesu eesmärgil kasutamise vältimise kohta. – Euroopa Ühenduste Teataja L 344, lk 76-81. Direktiiv kaotas kehtivuse 14.12.2005.
74. 10. juuni 1991. aasta Euroopa Ühenduste Nõukogu direktiiv 91/308/EMÜ rahandussüsteemi rahapesu eesmärgil kasutamise vältimise kohta. – ELT 09/1. kd, 28.12.2001, lk 153-158. Direktiiv kaotas kehtivuse 14.12.2005.
75. 20. mai 2015. aasta Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2015/849, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist ning millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 648/2012 ja tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2005/60/EÜ ja komisjoni direktiiv 2006/70/EÜ (neljas rahapesuvastane direktiiv ehk AMLD4). – ELT L 141, 30.06.2021, lk 73-117.
76. 23. oktoobri 2018. aasta Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2018/1673 rahapesu vastu võitlemise kohta kriminaalõiguse abil (kuues rahapesuvastane direktiiv ehk AMLD6). ELT L 284, lk 22-30.
77. 23. oktoobri 2018. aasta Euroopa Parlamendi ja Nõukogu määrus (EL)2018/1725, mis käsitleb füüsiliste isikute kaitsetisikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ. – ELT L 295, 21.11.2018, lk 39-98.
78. 24. oktoobri 1995. aasta Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – EÜT L 281, 20.11.2003, lk 31-50. Direktiiv kaotas kehtivuse 24.05.2018.
79. 26. oktoobri 2005. aasta Euroopa Parlamendi ja Nõukogu direktiiv 2005/60/EÜ rahandussüsteemi rahapesu ja terrorismi rahastamise eesmärgil kasutamise vältimise kohta. – ELT L 309, 25.11.2005, lk 15-36. Direktiiv kaotas kehtivuse 25.06.2017.
80. 27. aprilli 2016. aasta Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119, 04.05.2016, lk 1–88.

81. 30. mai 2018. aasta Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2018/843, 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 (viies rahapesuvastane direktiiv ehk AMLD5). – ELT L 156, lk 43-74.
82. Avaliku teabe seadus. – RT I, 10.03.2022, 4.
83. Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.
84. Euroopa Liidu toimimise lepingu konsolideeritud versioon. – ELT C 202, 07.06.2016, lk 47-199.
85. Euroopa Liidu põhiõiguste harta. – ELT C 202, 07.06.2016, lk 389-405.
86. Finantsinspektsiooni seadus. – RT I, 29.03.2022, 8.
87. Hädaolukorra seadus. – RT I, 17.11.2021, 9.
88. Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2010, 14, 54.
89. Makseteenuse ja sularaharingluse kirjeldus ja toimepidevuse nõuded. RMm 13.07.2018 nr 7. – RT I, 05.03.2019, 21.
90. Narkootiliste ja psühhotroopsete ainete ebaseadusliku ringluse vastane Ühinenud Rahvaste Organisatsiooni konventsioon (Viini konventsioon). – RT II 2000, 15, 92. United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention). Koostatud 20.12.1988 Viinis, jõustunud 11.11.1990. Eesti suhtes jõustunud 10.10.2000.
91. Karistusseadustik. – RT I, 21.05.2021, 9.
92. Korruptsioonivastane seadus. – RT I, 13.04.2021, 4.
93. Krediidiasutuste seadus. – RT I, 29.03.2022, 5.
94. Rahapesu ja terrorismi rahastamise tõkestamise seadus. – RT I, 12.03.2022, 19.
95. Rahvusvahelise organiseeritud kuritegevuse vastu võitlemise Ühinenud Rahvaste Organisatsiooni konventsioon (Palermo konventsioon). – RT II 2003, 1, 1. United Nations Convention against Transnational Organized Crime (Palermo Convention). Koostatud 15.11.2000 New Yorgis, avatud allakirjutamiseks 12.12.2000 Palermos, jõustunud 29.09.2003. Eesti suhtes jõustunud 29.09.2003.
96. Võlaõigusseadus. – RT I, 15.03.2022, 14.
97. Äriseadustik. – RT I, 12.03.2022, 12.

KASUTATUD KOHTUPRAKTIKA

Riigikohtu lahendid

98. RKKKm 11.04.2011, 3-1-1-97-10.
99. RKKKm 24.05.2017, 3-1-1-24-17.
100. RKKKo 27.06.2005, 3-1-1-34-05.
101. RKKKo 13.12.2010, 3-1-1-68-10.
102. RKKKo 22.06.2015, 3-1-1-94-14.
103. RKHKo 10.06.2016, 3-3-1-84-15.
104. RKHKo 24.03.2022, 3-20-332/39.

Euroopa Kohtu lahendid

105. EKo C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde vs. Rīgas pašvaldības SIA „Rīgas satiksme“*, ECLI:EU:C:2017:336.
106. EKo C-190/17, *Lu Zheng versus Ministerio de Economía y Competitividad*, ECLI:EU:C:2018:357.
107. EKo C-212/11, *Jyske Bank Gibraltar Ltd versus Administración del Estado*, ECLI:EU:C:2013:270.
108. EKo C-524/06, *Heinz Huber vs. Bundesrepublik Deutschland* (suurkoda), ECLI:EU:C:2008:724.
109. Liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd (C-293/12) vs Minister for Communications, Marine and Natural Resources jtn ning Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl* jt, ECLI:EU:C:2014:238.
110. Liidetud kohtuasjad EKo C-92/09 ja C-93/09, *Volker und Markus Schenke GbR ja Hartmut Eifert vs. Land Hessen*, ECLI:EU:C:2010:662.
111. Liidetud kohtuasjad EKo C-468/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) vs. Administración del Estado*, ECLI:EU:C:2011:777.

Euroopa Inimõiguste Kohtu lahendid

112. Liidetud kohtuasjad EIKo 30562/04 ja 30566/04, *S. ja Marper vs. Ühendkuningriik*, 08.12.2008.