RAHANDUSMINISTEERIUM

ASUTUSESISESEKS KASUTAMISEKS
Märge tehtud: 11.01.2016
Kehtib kuni: 11.01.2081
Alus: AvTS § 95 lg 1 p 19, HKMS § 89
Teabevaldaja: Rahandusministeerium

Eesnimi Perekonnanimi
Asutuse nimi
E-posti aadress

Teie: 19.11.2015 nr 3-3-8-1-385-15
(*haldusasi nr 3-3-1-75-15*)

Meie: kuupäev digitaalallkirjas
nr 1.1-12 /<DataType_26023703_3_1
/>

Arvamuse andmine kohtuasjas nr 3-3-1-75-15

Austatud riigikohtunikud

Riigikohtu halduskolleegium kaasas oma 19.11.2015 määrusega Rahandusministeeriumi haldusasjas nr 3-3-1-75-15 arvamuse andmiseks. Enne määruses toodud küsimustele vastamist soovime märkida järgmist.

Rahandusvaldkond on üks tugevamate avalik-õiguslike piirangutega ettevõtlusvaldkond, mille korraldamine on üks riigi tuumikfunktsioonidest. Selles valdkonnas tegutsemiseks on vajalikud spetsiifilised teadmised ja finantsasutuste juhtidele on kehtestatud kõrgendatud nõuded hariduse, kogemuste, reputatsiooni jt sobivusnõuete osas. Rahapesu ja terrorismi rahastamise tõkestamine on üks osa riigi finantspoliitikast ja see on vahetult seotud kõigi finantsvaldkonnas tegutsevate ettevõtjate igapäevase tegevusega, sest lisaks kriminaalõigusel põhinevale lähenemisele saab rahapesu tulemuslikult vältida tõhusa rahandussüsteemi abil.[1] Rahapesu ja terrorismi rahastamisega seotud riskid mõjutavad otseselt krediidi- ja finantseerimisasutuste kapitali hinda ja kõikide laenusaajate jaoks laenuressursi hinda.

Rahapesu ja terrorismi rahastamise tõkestamise alaste õigusnormide rakendamisel ja tõlgendamisel tuleb arvestada rahapesuvastase töökonna (ingl k *Financial Action Task Force*,[2] edaspidi: FATF) soovitustega. 2007. aastal, kui võeti vastu rahapesu ja terrorismi rahastamise tõkestamise seadus (edaspidi: RahaPTS), kehtisid FATF-i 40 soovitust rahapesu tõkestamise kohta ja 9 erisoovitust terrorismi rahastamise vastu. Käesoleval ajal kehtivad 2012. aasta veebruaris kinnitatud FATFi soovitused.[3]

Kuigi FATF annab välja n-ö soovitusliku iseloomuga soovitusi ja juhiseid, rõhutab rahandussüsteemi rahapesu ja terrorismi rahastamise eesmärgil kasutamise vältimise kohta antud direktiivi 2005/60/EÜ põhjenduspunkt 5, et EL tegevus peaks arvestama eelkõige juhtivaima rahvusvahelise rahapesu ja terrorismi rahastamisega võitleva organi, kelleks on

[1] Direktiivi 2005/60/EÜ põhjenduspunkt 1.
[2] Kasutatakse ka prantsusekeelset nimetust Group d´Action Financiere sur le Blanchment de Capitaux – lüh. GAFI. Asutatud 1989. a. G7 valitsusjuhtide initsiatiivil. Tänapäeval on FATF valitsustevaheline organ, kes kehtestab norme, töötab välja ja edendab rahapesu ja terrorikuritegude rahastamise vastase võitluse poliitikat.
[3] Kättesaadav: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

FATF, soovitusi. Eesti on teatavasti ka Euroopa Nõukogu liige ning osaleb MONEYVAL-i[4] vastastikuse hindamise voorudes, mille raames kontrollitakse FATF-i soovituste täitmist. Samuti on FATF soovituste ja standardite järgimise vajadust kinnitatud Euroopa Liidu institutsioonid[5] ning ÜRO Julgeolekunõukogu[6]. Pealegi on eelnimetatud soovitused osaks stabiilse finantskeskkonna põhistandarditest.[7] Lisaks eeltoodule reguleerib ka Rahvusvahelise organiseeritud kuritegevuse vastu võitlemise Ühinenud Rahvaste Organisatsiooni konventsiooni rahapesu tõkestamise meetmed.[8]

Tuleb arvestada, et rahandusvaldkonnas rakendatakse riiklikus järelevalves riskipõhist lähenemist juba alates 1999. aastast. Rahapesu ja terrorismi rahastamise tõkestamise abinõude eemärk on ennetada ja tõkestada õigusrikkumisi, mitte tegeleda üksnes tagajärgede kõrvaldamisega. Samas on Eesti olnud 1990ndatest alates finantsvaldkonna, eelkõige makseteenuste valdkonnas väga innovaatiline. Muu hulgas on arendatud suundanäitavalt antud valdkonna õiguskeskkonda, arvestades uute tehnoloogiate rakendamisega kaasnevaid riske. Uute maksevahendite õigusliku regulatsiooni kehtestamisel on peamine küsimus, kuidas saavutada mõistlik tasakaal ühelt poolt finantsinnovatsiooni ja sellest tulenevate positiivsete majanduslike mõjude ning teiselt poolt julgeolekuriskide, sh uute makseviiside kuritegelikel ja muudel ebaseaduslikel eesmärkidel kasutamise ohtude vahel. Elektrooniliste maksete regulatsioonide väljatöötamisel kohaldatav tehnoloogilise neutraalsuse põhimõte[9] ei välista ega vähenda avaliku võimu õigust takistada elektroonilises keskkonnas õigusrikkumiste toimepanemist, näiteks terrorismi rahastamist.

RahaPTS eelnõu väljatöötamisele eelnenud analüüs näitas, et peamisteks riskifaktoriteks kahtlaste tehingute teatiste põhjal on interneti-kuritegevusest saadud tulu siirdamine Eestisse või läbi Eesti finantssüsteemi, kontode müük, variisikute kasutamine, mittetraditsiooniliste makseteenuste kasutamine ja mitteresidentidega seotud rahavood.[10] Eelnõu koostamise käigus koostasid rahapesu andmebüroo ja Finantsinspektsioon elektrooniliste maksete, sh alternatiivsete maksevahendite teenuste riskianalüüsi. Selle analüüsi tulemused kinnitasid, et infotehnoloogia kõrge tase ja infotehnoloogiliste vahendite laialdane kasutamine tekitab Eesti praktikas täiendavaid rahapesu ja terrorismi rahastamise riske. Alternatiivsete maksevahendite teenustest tulenevate rahapesu ja terrorismi rahastamise riskide aktuaalsus Eestis ja maailmas tervikuna ei ole ajas vähenenud, vaid pigem vastupidi. Pariisis 13. novembril 2015 toimunud terrorirünnakud näitasid taas, et Euroopa peab terrorismile ühiselt ja tulemuslikumalt

[4] MONEYVAL on Euroopa Nõukogu rahapesuvastase võitlusega tegelev ekspertkomitee, mis teostab liikmesriikides vastastikuseid hindamisi rahapesu ja terrorismi rahastamise vastase võitluse meetmete rahvusvahelistele standarditele vastavuse osas. Vt Internetist: http://www.coe.int/t/dghl/monitoring/moneyval/

[5] 16. – 17.10.2001. a toimunud Euroopa Liidu rahandus-, majandus- ja justiits- ning siseasjade ministrite kohtumisel vastuvõetud otsuse alusel rakendada FATF-i standardeid täielikult nii EL liikmesriikides kui ka kandidaatriikides. 11. märtsil 2004. a Madridis toimunud terrorirünnakute järgselt kokku tulnud Euroopa Ülemkogu rõhutas vajadust tagada, et ühenduse loodud terrorismivastase võitluse ja õigusalase koostöö parandamise raamistikku kohandataks vastavalt FATF-i vastu võetud üheksale erisoovitusele terrorismi rahastamise vastu.

[6] ÜRO Julgeolekunõukogu resolutsioon nr 1617 (2005).

[7] Vt Finantsstabiilsuse Nõukogu (Financial Stability Board) kodulehekülg, Key Standards for Sound Financial Systems: http://www.fsb.org/what-we-do/about-the-compendium-of-standards/key_standards/

[8] Eesti Vabariik ratifitseeris rahvusvahelise organiseeritud kuritegevuse vastu võitlemise Ühinenud Rahvaste Organisatsiooni konventsiooni 29. septembril 2003. Selle konventsiooni artikliga 7 võttis Eesti muu hulgas kohustuse rakendada rahapesuilmingute vältimiseks ja nende kindlakstegemiseks pankade ja teiste finantsasutuste ning vajaduse järgi ka muude asutuste tegevuse reguleerimise ja tegevuse üle teostatava järelevalve korra ning kohaldab seda asutustele, mida võidakse kasutada rahapesuks; korras nähakse ette kliendi isikusamasuse tuvastamise, arvepidamise ning kahtlasest tehingust teatamise nõue.

[9] Tehnoloogilise neutraalsuse tagamine regulatsioonis tähendab seda, et regulatsioon ei saa põhineda ühelgi konkreetsel tehnoloogial vaid peab jääma piisavalt üldisele tasemele ja mitte jalgu jääma ajas kiiresti muutuvale tehnoloogiale.

[10] Seletuskiri RahaPTS eelnõu (137 SE) juurde lk 3, kättesaadav: http://www.riigikogu.ee/tegevus/eelnoud/eelnou/046802d9-335d-415b-c4a1-650aa487eb33/Rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20seadus/

reageerima ning võtma terrorismi võitlemiseks konkreetseid meetmeid. Selleks tegeleb Euroopa Komisjon aktiivselt seoses terrorismi rahastamise vältimise teemaga ka virtuaalvaluutadega. Majandus- ja rahandusküsimuste nõukogu (ECOFIN) kohtumisel 15. jaanuaril 2016 arutatakse Prantsusmaa ettepanekute paketti terrorismi rahastamise tõkestamiseks.

RahaPTS-iga otsustas Eesti 2008. aastal rangemalt reguleerida alternatiivseid maksevahenduse teenuse pakkujaid, kuna praktikas osutus juba 2006. a probleemiks Venemaa päritoluga alternatiivne maksevahend (WebMoney), mille teenust hakati aktiivselt kasutama, et kurjategijad *phishing*'u teel saadud rahasid kätte saaksid (nt 2015. aasta detsembris ulatus WebMoney tehingute arv päevas ca 400 000 tehinguni[11]).

Eesti on infotehnoloogia arengute valdkonnas üks edukamaid riike. Võrreldes enamuse riikidega on meie infotehnoloogiline tase oluliselt kõrgem ja seega ka vastava valdkonnaga seonduvad riskid on oluliselt suuremad. Eesti väga kõrge infotehnoloogia tase toob lisaks hüvedele paratamatult kaasa ka suuremaid riske rahapesu ja terrorismi rahastamise osas. Seetõttu tuleb mistahes olulisi uuendusi infotehnoloogia valdkonnas põhjalikult analüüsida, et regulatsioonid oleks sellised, mille abil õnnestuks maandada potentsiaalseid riske.[12]

Järgnevalt vastame Riigikohtu halduskolleegiumi poolt kaasatud haldusorganitele esitatud küsimustele.

1. Kas *bitcoin*'ide vahetamisteenuse tasu eest pakkuja, olenemata sellest, kas teenuse pakkuja vahendab ostjat ja müüjat või on ise *bitcoin*'ide ostjaks või müüjaks, on käsitatav rahapesu ja terrorismi rahastamise tõkestamise seaduse (RahaPTS) § 6 lõikes 4 sätestatud alternatiivsete maksevahendite teenuse pakkujana? Kas nimetatud norm laiendab rahapesuvastast järelevalvet ka krüpto-rahade (antud juhul *bitcoin*) müügitehinguid vahendavate isikute tegevusele olukorras, kus õigusakti väljatöötamise ja vastuvõtmise hetkel ei olnud *bitcoin*'e veel loodud?

RahaPTS § 6 lg 4 sätestab, et alternatiivsete maksevahendite teenuse pakkuja on isik, kes oma majandus- või kutsetegevuse käigus ostab, müüb või vahendab side-, ülekande- või kliiringsüsteemi kaudu rahalist väärtust omavaid vahendeid, mille abil on võimalik täita rahalisi kohustusi või mida saab vahetada kehtiva vääringu vastu, kuid kes ei ole sama paragrahvi lõikes 1 nimetatud isik ega finantseerimisasutus krediidiasutuste seaduse tähenduses.

Isik, kes vastab alternatiivse maksevahendite teenuse pakkuja tunnustele, on tulenevalt RahaPTS § 3 lg 1 punktist 2, § 6 lg 2 punktist 4 ning §-st 10 kõnealuse seaduse tähenduses finantseerimisasutus ning seega kohustatud isik, kes peab täitma RahaPTS 2. peatükis sätestatud hoolsuskohustusi ning rahapesu ja terrorismi rahastamise kahtluse korral sama seaduse 3. peatükis sätestatud kohustusi. Kohustatud isikute poolt RahaPTS ja selle alusel antud õigusaktide nõuete täitmise üle teostatakse riiklikku järelevalvet vastavalt RahaPTS 5. peatükile.

[11] Kättesaadav: http://www.webmoney.ru/rus/information/statistic/index.shtml.

[12] Aina enam tehinguid (sh finantstehinguid) tehakse virtuaalse keskkonna vahendusel, samuti on levinud kelmused, sh arvutikelmused ja identiteedivargused (teiste isikute ID kaartidega tehingute tegemine jne). Vt Kuritegevus Eestis 2013, kättesaadav: http://www.kriminaalpoliitika.ee/sites/www.kriminaalpoliitika.ee/files/elfinder/dokumendid/18._kuritegevus_eestis_2013.pdf.

Oleme seisukohal, et kohustatud isikuks kvalifitseerumine ei saa sõltuda sellest, kas vaadeldava isiku poolt pakutav teenus ning tema kasutatavad tehnoloogilised lahendused olid RahaPTS jõustumise hetkel olemas. Esiteks saab tehnoloogiliste arengutega arvestamiseks tõlgendada õigusakte dünaamiliselt, lähtudes nende eesmärgist ning kaitstavatest õigushüvedest. Nagu ülalpool selgitatud, on rahapesu ja terrorismi rahastamise tõkestamise valdkonnas seaduste tõlgendamise aluseks lisaks Euroopa Liidu õigusele ka FATF soovitused ja muud suunised, mis ajas samuti täiustuvad. Teiseks on RahaPTS § 6 lõikes 4 nimetatud alternatiivse maksevahendite teenuse pakkuja tunnuste sätestamisel arvestatud järjepideva tehnoloogia arenguga.

Alternatiivsete maksevahendite teenuse mõiste sätestamisel on eeskujuks võetud Rahvusvahelise Valuutafondi ja Ühinenud Rahvaste Organisatsiooni mudelseadus[13] ning (2003. a. redaktsioonis) FATF-i soovitused, sh erisoovitus VI (praeguses FATF soovituste redaktsioonis soovitus nr 14).

RahaPTS sätestatud kohustatud isikute ring tugineb FATF-i soovitustes toodud mõistete selgitustele. FATF-i soovituste tähenduses on finantsasutuseks kõik füüsilised või juriidilised isikud, kes teevad kliendi eest või nimel ettevõtluse korras ühte või mitut järgmistest tegevustest või operatsioonidest:

„[…] 4. raha või väärtuse ülekandmine.“

Punktile 4 lisatud joonealuses märkuses öeldakse, et see kohaldub nii formaalsele kui informaalsele finantstegevusele, sh alternatiivsetele ülekande tegevustele. Lisaks tuleb vaadata erisoovituste VI ja VII rakendusmärkusi.[14]

FATF erisoovitus VI (alternatiivsete maksevahendite teenus) defineerib *raha või väärtuse ülekandeteenusena* finantsteenust, mis võtab vastu sularaha, tšekke, teisi rahalisi maksevahendeid või **muud väärtusekandjaid** ühes kohas ja maksab vastava summa sularahas või muul kujul makse saajale teises kohas kas kommunikatsiooni, sõnumi, ülekande või sellise kliiringarvestuste võrgu kaudu, kuhu raha/väärtuse ülekandeteenus kuulub. Selliste teenuste kaudu sooritatud tehingutes võivad osaleda vahendajad ja nendega võib kaasneda kolmanda isiku lõppmakse.[15]

---

[13] Model legislation on money laundering and financing of terrorism. Kättesaadav: http://www.imolin.org/pdf/imolin/ModelLaw-February2007.pdf

[14] Financial Action Task Force on Money Laundering. The Forty Recommendations. 20 June 2003. Lk 13. Kättesaadav: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf
(“Financial institutions” means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer: *4. The transfer of money or value*
This applies to financial activity in both the formal or informal sector e.g. ***alternative remittance activity.*** *See the Interpretative Note to Special Recommendation VI. It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretative Note to Special Recommendation VII*).

[15] FATF IX Special Recommendations. Kättesaadav: http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf *(ingl.k.* VI.Alternative Remittance
„Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions)

VI erisoovitus koosneb kolmest põhielemendist:
1. Riigid peaksid nõudma selliste (füüsiliste või juriidiliste) isikute litsentseerimist või registreerimist, kes osutavad raha/väärtuse ülekandeteenuseid, sh mitteformaalsete süsteemide või võrgustike kaudu.
2. Riigid peaksid tagama, et raha/väärtuse ülekandeteenustele, kohaldatakse nagu pankadele või mittepankadest finantsasutustele FATFi neljakümmet soovitust (eelkõige soovitusi 4—16 ja 21—25) ning üheksat erisoovitust (eelkõige VII erisoovitust).
3. Riigid peaksid olema suutelised määrama karistusi sellistele raha/väärtuse ülekandeteenuste (kaasa arvatud alternatiivsete maksevahendite teenuse) pakkujatele, kes tegutsevad tegevusloata või registreerimata ega järgi asjakohaseid FATFi soovitusi.

Sama mõiste on määratletud eelnimetatud mudelseaduses 1. detsembrist 2005. Joonealuse märkusena on mainitud, et seda kohaldatakse nii formaalsele kui ka mitteformaalsele finantstegevusele, st alternatiivsele makseteenuse pakkuja tegevusele. Mudelseadus toob välja ka raha või väärtuse ülekandeteenuse sama mõiste.

Alternatiivse maksevahendite teenusepakkuja mõiste kasutuselevõtu kohta öeldakse RahaPTS eelnõu seletuskirjas järgmist: „Alternatiivsete maksevahendite teenuste pakkuja mõiste on sätestatud seetõttu, et tänapäeval kasutatakse järjest enam ka Eestis rahaliste kohustuste täitmise kõikvõimalikke viise, mis ei ole käsitletavad traditsiooniliste makseviisidena. Maailmas kasutatakse järjest enam mittetraditsioonilisi rahalist väärtust omavate vahendite ülekande ja edastamise viise, samuti alternatiivseid maksevahendeid, mida kasutatakse rahapesu ja terrorikuritegude rahastamise skeemides. FATF on analüüsinud erinevates maailma riikides kasutatavaid mittetraditsioonilisi makseviise ja toonud välja negatiivsed kasvutrendid selliste vahendite kasutamisel rahapesu skeemides. Uute täiendavate riskidena tuuakse välja Interneti […] edastuskanalite kasutamist, ärisuhte loomist vahetu kontaktita. […] Alternatiivsete süsteemide sarnaseks jooneks on see, et nad võimaldavad tehinguosalistel rahalist väärtust üle kanda koheselt, mugavalt, turvaliselt ja, mis kõige märkimisväärsem, anonüümselt. Kasutatakse nn elektroonilisi rahakotte (ingl. k. *elektronic purse*) ja digitaalse väärismetalli-põhiseid maksesüsteeme (e-kuld, e-hõbe). “[16]

Seega on RahaPTS eelnõu koostamisel lähtutud arusaamast, et alternatiivsed maksevahendite teenused kujutavad endast nn uusi maksete meetodeid, mida pakutakse väljaspool traditsioonilist reguleeritud finantssüsteemi. Ka FATF-i raportid jm dokumendid on alates 2006. aastast kuni käesoleva ajani lähtunud selgelt arusaamast, et lepingulisel alusel kasutatakse järjest enam elektroonilises/digitaalses vormis vahetusväärtust, mis on teatud määral rahale sarnaste omadustega ja mille ülekandmine toimub mittetraditsioonilisi finantsasutuste süsteeme, võrgustikke või kanaleid kasutades, millega kaasnevad kõrgendatud rahapesu ja terrorismi rahastamise riskid.[17] Muu hulgas on selgitatud, et FATF-i soovitus nr 14

[16] VT RahaPTS eelnõu seleltuskiri (137SE), lk 12.
[17] 2006.a. oktoobris avaldas FATF raporti „Report on New Payment Methods“, milles muuhulgas kirjeldatakse sarnaselt RahaPTS seletuskirjaga digitaalse väärismetalli-põhiseid maksesüsteeme (nn e-kul, e-gold) (lk 9, 16, 22, 26) ja elektroonilisi rahakotte (electronic purse (lk 14, 20), eeltooduga seotud riske ja regulatsioone (kättesaadav: http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf).
2010.a. oktoobris avaldatud FATF raport „Money Laundering using New Payment Methods“ käsitleb virtuaalse vääringuna nii väärismetallide põhiseid väärtusi kui lihtsalt digitaalset väärtust (Vt täpsemalt „Money Laundering using New Payment Methods“ FATF 2010, lk 17. Kättesaadav: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf).
2015. a juuni FATFi juhend riskipõhise lähenemise kohta virtuaalvaluutale toob tsentraliseeritud virtuaalvaluuta näitena E-kulla, Liberty Reserve, WebMoney detsentraliseeritud virtuaalvaluuta (krüptovaluuta) näitena Bitcoini, Litecoini ja Rippl (Kättesaadav: http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf). Nimetatud juhendis on täpsemalt selgitatud riskipõhise lähenemise põhimõtet ning ka FATF-i soovitust nr 15 (vana soovitus nr 8), mis käsitleb uute tehnoloogiatega (nt virtuaalvaluutadega) seonduvate riskide maandamise vajadust. Siinkohal on oluline tähele panna, et asjakohase soovituse sisu oli

(endine erisoovitus VI), mis käsitleb raha või alternatiivse maksevahendi ülekandeteenused, kohaldub ka virtuaalraha vahetuse teenuse pakkujatele.[18] Samadest arusaamadest on lähtutud ka Eesti õigusaktide väljatöötamisel.

Eeltoodust nähtub, et RahaPTS § 6 lg 4 käsitleb alternatiivsete maksevahendite teenust sarnaselt FATF-i erisoovituses VI tooduga laialt kolme üldise tunnuse alusel:

1. rahalist väärtust omavate vahendite ost, müük või vahendus;
2. side-, ülekande- või kliiringsüsteemi kasutamine (sh informaalse ülekandesüsteemi või vastava võrgustiku kaudu);
3. teenuse pakkumine majandus- või kutsetegevuse käigus.

Oleme seisukohal, et (majandus- või kutsetegevuse käigus) *bitcoin*'ide vahetamisteenust tasu eest pakkuja on käsitatav RahaPTS § 6 lõikes 4 sätestatud alternatiivsete maksevahendite teenuse pakkujana.

Seejuures ei oma tähtsust asjaolu, kas teenuse pakkuja vahendab ostjat ja müüjat või on ise *bitcoin*'ide ostjaks või müüjaks, kuna RahaPTS § 6 lg 4 kohaselt hõlmab alternatiivse makseteenuse pakkumine nii rahalist väärtust omavate vahendite müüki ja ostu kui ka vahendamist.

Bitcoin'ide vahetamisteenust tasu eest pakkuja RahaPTS § 6 lõikes 4 sätestatud tunnustele vastavuse hindamisel on peamine küsimus, kas *bitcoin*'id on rahalist väärtust omavad vahendid, mille abil on võimalik täita rahalisi kohustusi või mida saab vahetada kehtiva vääringu vastu. Sellele küsimusele tuleb vastata jaatavalt, mida kinnitavad nt Euroopa Kohtu 22.10.2015 otsusega asjas C-264/14 tuvastatud asjaolud. Nimelt toob kohtuotsuse p 52 toob välja, et on selge, et virtuaalsel valuutal *bitcoin* ei ole muud mõtet, kui olla kasutatav maksevahendina, ning et osa ettevõtjaid aktsepteerivad seda antud eesmärgil (st võimaldavad *bitcoin*'dega rahalisi kohustusi õiendada).

Lisaks märgime, et virtuaal- või krüptorahad ei ole oma olemuselt esimesed alternatiivsed vahetusväärtuse meediumid. Enne virtuaal- või krüptoraha loomist on maailmapraktikas pikka aega kasutatud väärtusekandja omadustega kuponge, tšekke, marke, vautšereid ja muid nn „paralleelvääringuid", mis on väljaspool õiguslikku arusaama rahast.[19] Seega ei oma määravat tähtsust ka tehnoloogia arengust tingitud sõnakasutuse erinevused, vaid elektroonilises keskkonnas eksisteerivate vahetusväärtuse meediumite tsiviilkäibes kasutamise võimalikkus (st kas neid on võimalik osta, müüa või vahetada) ja selliste väärtuste informaalse ülekandmise süsteemide olemuslik sarnasus. Eesti ei ole ka ainus riik, kelle juba olemasolev regulatsioon hõlmab virtuaalvaluutasid. Näiteks on Šveits ametlikult avaldanud seisukoha, et nende olemasolev rahapesu ja terrorismi rahastamise tõkestamise seadus katab ka virtuaalvaluutade professionaalse vahenduse ja müügi.[20]

---

sama FATF-i standardite vanemas versioonis ja kehtis seega ka RahaPTS väljatöötamise hetkel, mistõttu ei ole tegemist uue standardiga.

Euroopa Pangandusjärelevalve Asutuse (EBA) arvamuse (kättesaadav: https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf) kohaselt on virtuaalraha eksisteerinud pikka aega enne hiljutist virtuaalvaluuta detsentraliseerimise vajadust. Varasemad näiteid tsentraliseeritud virtuaalvaluutast, mis ei olnud konverteeritav - World of Warcraft Gold või Frequent Flyer Miles, ühesuunalise konverteeritavusega oli endine Facebook krediit, Linden dollarid, mitmesuunalise konverteeritavusega E-gold ja Liberty Reserve. Soov selliste valuutade järele sai alguse videomängude kogukondade liikmeilt, kes otsisid mugavat viisi, kuidas kasutajaid premeerida või nendega finantstehinguid sõlmida.

[18] 2015. a juuni FATFi juhend riskipõhise lähenemise kohta virtuaalvaluutale (viide 17), punkt 33.

[19] Vt. täpsemalt F.A.Mann „The Legal Aspect of Money" 5th ed. Oxford: Clarendon Press, 1992, lk 25.

[20] 2015. a juuni FATFi juhend riskipõhise lähenemise kohta virtuaalvaluutale (viide 17), punkt 81.

2. Kas Euroopa Parlamendi ja Nõukogu direktiivi 2005/60/EÜ regulatsioon on kohaldatav *bitcoin*'ide vahetamisteenusele? Kui jah, siis millises ulatuses?

Direktiivi 2005/60/EÜ artikkel 2 lg 1 nimetab asutused või isikud, kelle suhtes kõnealust direktiivi kohaldatakse. Sama direktiivi art 4 lõikest 1 nähtub aga üheselt, et see loetelu ei ole ammendav, kuna liikmesriigid peavad kandma hoolt selle eest, et direktiivi sätteid laiendatakse täies ulatuses või osaliselt elukutsetele ja ettevõtjate kategooriatele, mis ei ole küll artikli 2 lõikes 1 osutatud asutused ja isikud, kuid tegutsevad alal, mida võidakse eriti tõenäoliselt kasutada rahapesu ja terrorismi rahastamise eesmärkidel.

Nii FATF kui ka Euroopa Pangandusjärelevalve Asutus (edaspidi: EBA) on kinnitanud virtuaalvaluutadega (sh *bitcoin*'idega) kaasnevat rahapesuriski.[21] Seetõttu oleme seisukohal, et liikmesriigid võivad direktiivi sätteid täies ulatuses laiendada ka *bitcoin*'i vahetusteenuse pakkujale.

3. Kas RahaPTS § 6 lg 4 on vastavuses Euroopa Parlamendi ja Nõukogu direktiivi 2005/60/EÜ mõtte ja eesmärgiga (eelkõige artiklitega 4 ja 5) ning FATF soovitustega? Kas esineb vajadus eelotsuse küsimiseks Euroopa Kohtult?

Oleme seisukohal, et RahaPTS § 6 lg 4 on kooskõlas direktiiviga 2005/60/EÜ, ning leiame, et puudub vajadus eelotsuse küsimiseks Euroopa Kohtult, kuna asjakohased direktiivi normid on piisavalt selged. Ühtlasi oleme seisukohal, et RahaPTS § 6 lg 4 on kooskõlas FATF soovitustega.

Direktiivi mõte ja eesmärk on rahandussüsteemi rahapesu ja terrorismi rahastamise eesmärgil kasutamise vältimine. Seda muu hulgas põhjusel, et kurjategijate ja nende kaasaaitajate püüded varjata kuritegelikul teel saadud tulu päritolu või suunata seaduslikku või ebaseaduslikku raha terroristlikesse eesmärkidesse, võivad tõsiselt ohustada krediidi- ja finantseerimisasutuste usaldusväärsust, terviklikkust ja stabiilsust ning kõigutada usaldust rahandussüsteemi suhtes üldiselt (direktiivi 2005/60/EÜ põhjenduspunkt nr 2).

Direktiivi artikli 5 kohaselt võib liikmesriik kehtestada direktiivi sätetest rangemaid sätteid, mis tähendab, et direktiivis on toodud rahapesu tõkestamise alased miinimumstandardid. Direktiivi artikkel 4 lg 1 paneb liikmesriigile kohustuse direktiivi sätteid rakendada ka nendele ettevõtjatele, kelle tegevusalal võib eeldada tõenäolist rahapesu riski. Seega võis Eesti seadusandja laiendada direktiivis toodud kohustatud isikute nimekirja ning lisada sinna RahaPTS § 6 lõikes 4 toodud tunnustele vastavad isikud ehk alternatiivsete maksevahendite teenuse pakkujad. RahaPTS eelnõu väljatöötamisel lähtuti mitte ainult direktiivi sätetest, vaid ka FATF soovitustest. Rangema regulatsiooni kehtestamise vajadus tulenes praktikas väljakujunenud negatiivsetest trendidest, sh julgeolupoliitilistest riskidest ja eelnõu koostamise käigus tehtud Eesti praktika riskianalüüsist.

Euroopa Liidu Toimimise Lepingu artikli 267 lõike 3 kohaselt peab iga liikmesriigi kohus, mille otsuste peale ei saa riigisisese õiguse järgi edasi kaevata, taotlema Euroopa Liidu aluslepingute tõlgendamise või Euroopa Liidu institutsioonide, organite või asutuste õigusaktide kehtivuse ja tõlgendamise küsimuse üleskerkimisel Euroopa Kohtult eelotsust. Euroopa Kohtu praktika kohaselt esineb kaks erandit, millal liikmesriigi kõrgeim kohus ei ole kohustatud vastavalt Euroopa Liidu õiguse tõlgenduses Euroopa Kohtult eelotsust küsima. Need juhtumid on *acte éclairé* (Euroopa Kohus on varasemas kohtupraktikas õigusnormi juba selgitanud) ja *acte clair* (õigusnorm on üheselt mõistetav ja piisavalt selge).[22]

[21] EBA arvamus (viide 17) lk 32 jj; 2015. a juuni FATFi juhend riskipõhise lähenemise kohta (viide 17) virtuaalvaluutale http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

[22] Vt Euroopa Kohtu 06.10.1982 otsus kohtuasjas 283/81.

Leiame, et EL õiguse normid, mida tuleb rakendada lahendades küsimust, kas RahaPTS § 6 lg 4 on kooskõlas direktiiviga, on üheselt mõistetavad ja piisavalt selged. Nimelt ei saa direktiivi artiklitele 4 ja 5 omistada eesmärki piirata liikmesriikide võimalusi rahapesuvastaste abinõude kehtestamisel. Nagu märgitud, annavad need liikmesriikidele hoopis õiguse kehtestada rangemaid rahapesuvastaseid abinõusid. Seda on Eesti RahaPTS § 6 lg 4 sätestamisega teinud. Seega on antud juhul tegemist *acte clair* olukorraga, mistõttu puudub vajadus küsida Euroopa Kohtult eelotsust.

Vastates Riigikohtu halduskolleegiumi 1. küsimusele, märkisime, et RahaPTS § 6 lg 4 põhinebki suures osas FATF-i soovitustel, mistõttu ei korda me siinkohal ülaltoodud selgitusi. Täiendavalt märgime, et Eesti rahapesuvastaste õigusaktide vastavust nii FATF-i soovitustele kui ka direktiivile 2005/60/EÜ on kinnitanud korduvad rahvusvaheliste hindamiste tulemused.[23]

Nt MONEYVAL-i IV hindamisvooru raportis[24] nimetatakse alternatiivsete maksevahendite teenuse pakkujaid selgelt ja korduvalt, kuid kordagi ei ole mainitud või tõstatatud küsimust liiga laia kohustatud isikute ringi kohta. Vastupidi – tuuakse välja, et maksete valdkonnas, sh alternatiivsete maksevahendite teenuste pakkujatega seotud riskid on kõrged ja et alternatiivsete maksevahendite teenuste pakkujatel on hoolsusmeetmete kohaldamise kohustus ja nad alluvad riiklikule järelevalvele. IV hindamisvooru raporti lk 106 punktis 409 on alternatiivsete maksevahendite hulgas *bitcoin*'id eraldi selgelt välja toodud.

4. Kui *bitcoin*'ide vahetamisteenuse pakkuja on käsitatav alternatiivsete maksevahendite teenuse pakkujana RahaPTS § 6 lg 4 mõttes ning seeläbi finantseerimisasutuseks, siis kas virtuaalsete valuutade vahetamisteenuse pakkuja tegevuse üle järelevalve teostamiseks on Eesti õiguslik regulatsioon teenusepakkuja ja järelevalveasutuste õiguste ja kohustuste sätestamisel kohane ja piisav ning põhiseaduse § 13 lõikes 2 sätestatud õigusselguse põhimõttega kooskõlas? Kas *bitcoin*'ide kui virtuaalse valuuta olemusest tulenevad eripärad eeldaksid õigusaktides (nt RahaPTS-s) järelevalve eriregulatsiooni kehtestamist?

Rahandusvaldkonnas tegutsemine nõuab alati spetsiifilisi teadmisi ja oskusi. Finantsvaldkonnas tegevuse alustamine nõuab asjakohaste õigusnormide ja juhendmaterjalide eelnevat põhjalikku tundmist ning nõuete kohaste teenuste pakkumiseks spetsiaalseid ettevalmistusi. Kehtiv õiguslik regulatsioon on virtuaalsete valuutade vahetamisteenuse pakkuja ja järelevalveasutuste õiguste ja kohustuste sätestamisel kohane ja piisav ning põhiseaduse § 13 lõikes 2 sätestatud õigusselguse põhimõttega kooskõlas.

Alternatiivse makseteenuse pakkuja mõiste on määratletud üldiste väga laiade tunnuste alusel, arvestades ka tehnoloogilise neutraalsuse põhimõtet. Normi õigusselguse kohta hinnangu andmisel tuleks silmas pidada, kas normi sõnastuses on tegemist nn tavakeeles kasutatava sõnavaraga, mida kasutatakse õigustekstis n-ö „loomulikus tähenduses" või õigusliku terminiga juriidilise keele tähenduses või valdkonna spetsiifilise terminoloogiaga.

RahaPTS § 6 lg 4 sõnastus „ostab, müüb või vahendab side-, ülekande- või kliiringsüsteemi

[23] Vt nt täpsemalt Moneyvali III vooru hindamise raport. Kättesaadav: https://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round3/MONEYVAL(2008)32Summ-EST3_en.pdf; Samuti ja III vooru hindamise raporti kokkuvõte. Kättesaadav: http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round3/MONEYVAL(2008)32Summ-EST3_en.pdf. Erisoovituse VI täitmine on hinnatud LC (*largely compliant* - suuresti vastavaks).

[24] Vt. täpsemalt Moneyvali IV vooru hindamise raporti p3, 19, 87, 373., 408, 409 jne. Kättesaadav: http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round4/MONEYVAL(2014)20_Estonia.pdf

kaudu rahalist väärtust omavaid vahendeid, mille abil on võimalik täita rahalisi kohustusi või mida saab vahetada kehtiva vääringu vastu“ kasutab nn tavakeeles tuntud sõnu, mis on keskmiste võimetega isikule piisava süvenemisega lugemisel arusaadavad, v.a. ehk sõna „kliiringsüsteem“. Sätte sõnastus ei anna alust väidetele, et tegemist võiks olla semantiliselt ebamäärase või semantiliselt mitmetähendusliku sõnakasutusega. Kvalitatiivseid ega kvantitatiivseid arutlusvõimalusi ei anna ka muud õigusnormi adressaadi käitumisvõimaluse kohta toodud tingimused, nagu nt: „[…] kuid kes ei ole lõikes 1 nimetatud isik ega finantseerimisasutus krediidiasutuste seaduse tähenduses“.

Arvestades virtuaalrahaga seotud riskide kasvu, on need olnud avaliku meedia kõrgendatud tähelepanu all ja ka Euroopa pädevad ametiasutused, sh Euroopa Pangandusjärelevalve Asutus (EBA) ja ka Finantsinspektsioon on avaldanud vastavaid hoiatusteateid ja muid asjakohaseid materjale.

EBA andis välja hoiatuse[25] 1.12.2013, mis on avaldatud Finantsinspektsiooni kodulehel[26] ja millega hoiatatakse tarbijaid virtuaalse raha eest. Viidatakse, et virtuaalses vääringus tehingute tegemise võimalust võidakse ära kasutada kuritegelikel eesmärkidel, sh rahapesuks. Selgelt hoiatatakse, et kuritegeliku ärakasutamise tulemuseks võib olla, et õiguskaitseorganid otsustavad valuutavahetuse platvormi sulgeda ja blokeerida juurdepääsu platvormidel hoitavale rahale ja selle kasutamisele.

Seadus ega Finantsinspektsiooni soovituslik juhend „Rahapesu ja terrorismi rahastamise tõkestamise meetmed krediidi- ja finantseerimisasutuses“[27] ei sisalda eraldi viidet krüptoraha või virtuaalvaluuta teenuse pakkujale, vaid nimetatud juhendis viidatakse alternatiivsete maksevahenditega seotud riskifaktoritele, mis tulenevad kliendi majandustegevusest ja konkreetse toote või teenuse avatusest võimalikele rahapesuriskidele (vt. p 4.6.4.2).

Õigusselguse põhimõte tuleneb nõudest, et isikul peab olema mõistlik võimalus ette näha õiguslikke tagajärgi, mida tema tegevus võib kaasa tuua - isikul peab olema õigusnormidele tuginedes võimalik prognoosida avaliku võimu käitumist. Alternatiivse makseteenuse pakkujal (ka *bitcoin*'ide vahetamisteenuse pakkujal) on võimalik ette näha, millised tagajärjed tema tegevusega kaasnevad, ning oma riske maandada asjakohaste siseprotseduuride kohaldamise teel ja prognoosida järelevalvemenetluse käiku.

Bitcoin'id võimaldavad teatavasti rahalist väärtust kiirelt ning anonüümselt edasi kanda. Võrreldes sularahaga on piiriülese liikumise kiirus märgatavalt suurem. *Bitcoin'ide* vahetamisteenuse pakkumisel peab teenuse osutaja mõistma, et tegemist on finantsteenusega, kuna *bitcoin*'i kasutatakse kui väärtusekandjat ja ülekandesüsteemi. Täpsemalt võimaldab teenus väärtuse ülekandmist, vormida ülekantud väärtus mõneks käibevaluutaks (nt müüa *bitcoin*'id eurode vastu) või osta *bitcoin*'e investeerimise või muul eesmärgil. Selliste võimaluste tõttu peavad teenusepakkujad kindlasti välja selgitama teenuse pakkumisega kaasnevad riskid, samuti välja selgitama enne tegevuse alustamist, millised õigusaktid teenust reguleerivad. Finantsteenuste rahapesuvastane regulatsioon ning sellekohane järelevalve on sätestatud RahaPTS-is. Oleme seisukohal, et rahapesu tõkestamise valdkonnas ei eelda *bitcoin*'ide eripära õigusaktides (sh RahaPTS-s) järelevalve eriregulatsiooni kehtestamist.

5. Kas tulenevalt *bitcoin*'idega tehtavate tehingute vormistamise võimalikest eripäradest (nt *bitcoin* protokollist ja reeglitest tulenev tehingupoolte anonüümsus) on *bitcoin*'ide vahetamisteenuse pakkujal, arvesse võtmata seda, kas teenuse pakkuja vahendab *bitcoin*'ide ostjat ja müüjat või on ise *bitcoin*'ide ostjaks või müüjaks, õiguslik kohustus ja

[25] Kättesaadav: https://www.fi.ee/public/EBA_virtuaalne_vaaring.pdf.
[26] Kättesaadav: https://www.fi.ee/?id=3444.
[27] Kättesaadav: http://www.fi.ee/failid/Soovituslik_juhend_Rahapesu_tokestamine.pdf.

ka võimalus klientide andmeid talletada ja hoolsuskohustust järgida (nt klientide isikusamasust kontrollida)? Kui jah, siis millisel õiguslikul alusel ja millisel tehnilisel viisil, et oleks tagatud *bitcoin*'ide andmebaasis tehtavate tehingute anonüümsus?

Riigikohtu küsimused keskenduvad „*bitcoin*'ide vahetamisteenuse tasu eest pakkujale", seega isikule, kes müüb, ostab või vahendab *bitcoin'*e, saades selle eest vastutasuks eurosid. Sellise tegevuse juures on võimalik eristada kahte toimingut: esiteks eurode üleandmine (kliendilt vahetusteenuse pakkujale või vastupidi) ning teiseks *bitcoin*'i omandiõiguse ülemineku registreerimine.

Bitcoin'idega arveldamiseks on vaja vastavat rahakotti, mis võib olla arvutisse installeeritud tarkvara, mobiilirakendus või veebipõhine lahendus. Igal rahakotil on olemas avalik võti (võrreldav kontonumbriga) ning privaatne võti (rahakoti kasutamiseks turvakood, mis on teada ainult rahakoti omanikule ja mis on võrreldav PIN-koodide ja kasutajatunnustega).

Bitcoin'i omandiõiguse üleminek algatatakse *bitcoin*'i ostja avaliku võtme saatmisega *bitcoin*'i müüjale, kes kinnitab tehingu personaalse võtmega ja sisestab koodi *bitcoin*'i süsteemi, kus kogu tehingu info saab avalikuks. *Bitcoin*'i süsteemi aluseks on avalik raamatupidamisregister ehk *block chain*. Põhimõtteliselt on tegemist koodiga, kus kajastuvad alates selle loomisest tehingublokkide kaupa kõik ringluses olevad *Bitcoin'*id ja nendega tehtud tehingud. Selles koodis sisaldubki *bitcoini*'de omandiõiguse üleminek, kuhu salvestub info nii, et ainult uus omanik saab neid kasutada. Omandiõigus läheb lõplikult üle siis, kui *bitcoin*'i süsteemis kaevandajad sinna sisestatud koodi üle kontrollivad ja selle kinnitavad.

Kehtiva vääringu vahetamine *bitcoin*'i vastu saab toimuda kas sularahas või rahaülekandena. Selle poolest ei erine *bitcoin*'i vahetamisteenus nt traditsioonilisest valuutavahetusteenusest. Seetõttu pole põhjust arvata, et *bitcoin*'i vahetamisteenuse pakkujal pole tehniliselt võimalik rakendada hoolsuskohustust ja teisi RahaPTS-is sätestatud kohustusi (nt tuvastada vastavalt RahaPTS § 13 lg 1 punktile 1 kliendi isikusamasuse, kes soovib sularaha eest *bitcoin*'e osta).

Õiguslik alus *bitcoin*'i vahetusteenuse pakkuja suhtes RahaPTS kohaldamiseks tuleneb selle seaduse § 3 lg 1 p 2, § 6 lg 2 p 4 ja lg 4 ning § 10 koostoimest, nagu selgitasime ülalpool. Seejuures näeb RahaPTS ette erisused hoolsusmeetme kohaldamisel alternatiivsete makseteenuste pakkujate poolt. RahaPTS § 15 lg 8 kohaselt on alternatiivsete maksevahendite teenuse pakkuja kohustatud tuvastama iga kliendi isikusamasuse ärisuhte loomisel ja tehingu tegemisel kliendiga samas kohas viibides, kui selle kliendi tehingute väärtus kalendrikuus ületab 1000 eurot või võrdväärse summa muus vääringus. Mitme kliendi vahelise tehingu vahendamisel peab ta tuvastama iga tehingus osaleva isiku isikusamasuse ja esitatud teavet kontrollima.

Lisaks märgime, et kohustatud isikul on RahaPTS § 13 lg 4 järgi sama seaduse § 13 lõike 1 punktides 1–3 nimetatud hoolsusmeetmete[28] kohaldamisel õigus tugineda teabele, mille ta on kirjalikku taasesitamist võimaldavas vormis saanud Eestis äriregistrisse kantud krediidiasutuselt või välisriigi krediidiasutuse filiaalilt või krediidiasutuselt, kes on registreeritud või kelle tegevuskoht on Euroopa Majanduspiirkonna lepinguriigis või kolmandas riigis, kus kehtivad käesolevas seaduses sätestatuga võrdväärsed nõuded. Samas peab kohustatud isik hankima teavet ärisuhte olemasolu ja tehingu eesmärgi ning olemuse

[28] Vastavalt RahaPTS § 13 lõikele 1 kohaldab kohustatud isik §-s 12 nimetatud kohustuse täitmiseks majandus-, kutse- või ametitegevuses järgmisi hoolsusmeetmeid:
1) kliendi või tehingus osaleva isiku isikusamasuse tuvastamine tema esitatud dokumentide ja andmete alusel ning esitatud teabe kontrollimine usaldusväärsest ja sõltumatust allikast hangitud teabe põhjal;
2) füüsilise või juriidilise isiku esindaja isikusamasuse ja esindusõiguse tuvastamine ning kontrollimine;
3) tegeliku kasusaaja tuvastamine, sealhulgas juriidilise isiku, usaldusfondi, seltsingu või muu sellise lepingulise õigusliku üksuse omandi- ja

kohta, samuti ärisuhet pidevalt jälgima (RahaPTS § 13 lg 1 punktid 4 ja 5). Ärisuhte ja tehingu eesmärgi kohta teabe hindamisel tuleb arvestada nn. „tunne oma klienti" põhimõtet. "Tunne oma klienti" põhimõte on kõige olulisem vahend kliendi või tehingu teise poole isiku ja tema tegevusega kaasnevate ohtude ärahoidmiseks ja kohustatud isiku enda tegevusriskide hindamiseks. Kohustatud isik peab teadma, kellega ta teeb tehingu või kes osaleb ametitoimingus või kes on tema kliendiks ja milline on selle isiku tavapärane tegevus. Kohustatud isik peab jälgima, et tehingud, mida klient teeb ja tema poolt kasutatavad rahalised vahendid oleksid kooskõlas kliendi majandustegevuse laadi ja ulatusega.

6. Kuidas toimub *bitcoin*'ide ostu-müügitehingu puhul virtuaalse valuuta omandiõiguse üleminek ja selle registreerimine *bitcoin*'ide andmebaasis? Kui üldse, siis milliseid andmeid näeb ja saab kontrollida vahetamisteenuse pakkuja? Kas vahetusteenuse pakkuja näeb, millise isiku arvelduskontolt on laekunud raha *bitcoin*'iga tehtud tehingult?

Bitcoin'i omandiõiguse üleminekut selgitasime vastuses eelmisele küsimusele. *Bitcoin*'i omandiõiguse üleminekuks on vaja teada vaid teise tehingupartneri rahakoti avalikku võtit. Kui aga vahetusteenuse pakkuja arveldab kliendiga eurodes, siis on tal nii tehniline võimalus kui ka õiguslik kohustus koguda ja kontrollida kõiki RahaPTS sätestatud kohustuste täitmiseks vajalikke andmeid nagu selgitasime eespool.

7. Kas *bitcoin*'ide müügitehingule omase anonüümsuse põhimõtte vähendamist eeldava järelevalvemenetluse rakendamine oleks kooskõlas *bitcoin*'ide protokolli ja reeglitega?

Kõigepealt leiame, et mõne õigushüve või avaliku huvi kaitsmiseks vajalik riikliku järelevalve ulatus ei saa sõltuda reeglitest, mida tehingupooled või turuosalised on omavahel kokku leppinud. Kui müügitehingute anonüümsust vähendav järelevalvemenetlus on proportsionaalne abinõu rahapesu tõkestamiseks, siis tuleb seda ka rakendada. Antud juhul pole seda probleemi aga meie hinnangul vaja lahendada. RahaPTS sätestatud kohustused ei nõua *bitcoin*'i vahetusteenuse pakkujalt, et ta sisestaks *block chain*'i mingeid täiendavaid andmeid vms. Hoolsuskohustust jt rahapesu tõkestamisega seotud kohustusi on vahetusteenuse pakkujal võimalik täita siis, kui ta arveldab klientidega seoses *bitcoin*'i ostu, müügi või vahendamisega eurodes (või muus kehtivas vääringus).

8. Kui RahaPTS-s finantseerimisasutusele ettenähtud hoolsusmeetmed kohalduvad *bitcoin*'ide vahetamisteenuse pakkujale ja eeldusel, et nende täitmine ei ole *bitcoin*'idega müügitehingute olemusest tulenevalt seaduses ettenähtud ulatuses võimalik, siis kas ettekirjutusega sellises ulatuses andmete nõudmine on proportsionaalne?

Kuna leiame, et *bitcoin*'i vahetamisteenuse pakkujal on võimalik täita RahaPTS-s sätestatud kohustusi, siis pole meie hinnangul ka alust kahelda PPA andmepesubüroo ettekirjutuse proportsionaalsuses. Andmete nõudmiseks on olemas seaduslik alus ning need on vajalikud riikliku järelevalve teostamiseks.

Lugupidamisega

(*allkirjastatud digitaalselt*)
Kaarel Eller
Rahandusministeeriumi õigusosakonna nõunik
Volitus toimiks