Infotehnoloogia arengute mõju rahapesu ja terrorismi rahastamise ohtudele finantssektoris

Käesoleva analüüsi on koostanud Rahandusministeerium ja selle eesmärk on hinnata infotehnoloogia arengute mõju rahapesu ja terrorismi rahastamise ohtudele.

Sissejuhatus:

Kogu senise inimajaloo vältel on usaldussuhte loomine ja kontroll selle üle toimunud inimese poolt ja finantsalase õigusliku regulatsiooni üldpõhimõtted põhinevad eelkõige antud eeldusel. Mida rohkem ühiskond moderniseerub ja infotehnoloogia areneb, seda vähem eelöeldu kehtib.

Finantsteenused kui usaldusteenused

Finantsteenused on teatavasti suurel määral usaldusteenused ja vastavate teenuselepingute sõlmimise teoreetiline kontseptsioon erineb näiteks müügilepingust (müügileping ei ole teatavasti oma olemuselt usaldussuhe).

Infotehnoloogia arengute mõju finantsteenustele

Viimastel aastakümnel on infotehnoloogilised arengud plahvatuslikult kasvanud. Nimetatud arengud on kahtlemata mõjutanud ka finantsteenuste osutamise viise. Enamus tehinguid toimuvad interneti keskkonna vahendusel ja lisaks kasutatakse tsiviilkäibes aina enam rahaliste kohustuste täitmisel lisaks traditsioonilistele makseviisidele ka alternatiivseid makseviise. Elektroonsed süsteemid on muutnud raha ülekandmise ühest riigist teise märksa lihtsamaks ja kiiremaks. Samas kätkevad nimetatud uued tehnoloogiad mitmeid riske, sh rahapesu ja terrorismi rahastamise riske.

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, mis oleksid võimelised maandama potentsiaalseid riske. Lisaks infotehnoloogilistele arengutele tuleb Eestil arvestada ka geopoliitiliste mõjudega, mis koosmõjus suurendavad Eesti rahapesu ja terrorismi rahastamise alaseid riske veelgi enam.

Eesti infotehnoloogia tase ja riskid

Eesti on infotehnoloogia arengute valdkonnas üks edukamaid riike. Meil on käivitatud arvukalt erinevaid registreid ja virtuaalteenuseid, olemas on nn e-valitsus ja elanikkond kasutab aktiivselt ID- kaarti ja selle abil ligipääsetavaid virtuaalteenused (nt X-tee Ettevõtteportaal jms), sh e-pangateenuseid. Võrreldes enamiku riikidega on meie infotehnoloogiline tase oluliselt kõrgem ja seega ka vastava valdkonnaga seonduvad riskid on oluliselt suuremad.

Küberkuritegevuse kõrge tase kasvab terves maailmas, kuid Eesti peaks olema siinkohal eriti ettevaatlik, kuna meil on tavaliselt kõrgem tase infotehnoloogiliste vahendite kasutamise osas. Aina enam tehinguid (sh finantstehinguid) tehakse virtuaalse keskkonna vahendusel, samuti on levinud kelmused, sh arvutikelmused ja identiteedivargused (teiste isikute ID kaartidega tehingute tegemine jne)[1]. Eesti siseriikliku rahapesu ja terrorismi rahastamise alase riskihinnangu tulemuste kohaselt on arvutikelmused enim levinud eelkuriteod rahapesu kuritegudele.

Virtuaalriskide maandamine ja küberkuritegevuse ennetus

Rahapesu ja terrorismi rahastamise tõkestamise valdkonnas on infotehnoloogilisi riske arvestatud juba vastava regulatsiooni koostamisel ning antud riskide maandamiseks on Eesti kehtestanud võrreldes teiste riikidega mõnevõrra rangema regulatsiooni - nt on finantsasutused kohustatud esmase ärisuhte loomisel isiku tuvastama näost näkku viibides temaga samas kohas (nn *face to face* nõue), et säilitada ärisuhte loomisel personaalse usalduse tekkimise võimalus (vastandina tehnoloogiliselt vahendatud ärisuhte loomisele). Võrreldes oma lähinaabritega (eelkõige Läti ja Venemaa) on Eesti suutnud oma finantsruumi ja majanduskeskkonda edukalt kaitsta suurematest rahapesu ja terrorismi rahastamise skeemidest ja skandaalidest, mis tõendab omakorda, et mõnevõrra rangem regulatsioon on põhjendatud ja vajalik. Ka viimases MONEYVAL-i Eesti IV hindamisvoorus leidsid rahvusvahelised eksperdid, et eelpool nimetatud näost näkku tuvastamise meede on sobiv meede riskide maandamiseks, mis on seotud Eesti kõrge infotehnoloogilise tasemega.

Eestis on otsustatud rangemalt reguleerida alternatiivseid maksevahenduse teenuse pakkujaid, kuna praktikas osutus probleemiks Venemaa päritoluga alternatiivne maksevahend (WebMoney), mille teenust hakati aktiivselt kasutama, et kurjategijad *phishingu* teel saadud rahasid kätte saaksid. WebMoney käive on päevas ca 400 000 tehingut (http://www.webmoney.ru/rus/information/statistic/index.shtml). Bitcoinide päevane tehingute maht ca 75 000 tehingut (https://blockchain.info/charts/n-transactions). 2013 WebMoney käive oli 19 miljardit USD

[1] Vt Kuritegevus Eestis 2013, kättesaadav: http://www.kriminaalpoliitika.ee/sites/www.kriminaalpoliitika.ee/files/elfinder/dokumendid/18._kuritegevus_eestis_2013.pdf

(http://www.webmoney.ru/rus/information/statistic/years.shtml ja Bitcoinide oma kalkuleeritult ilmselt väiksem (https://blockchain.info/charts/estimated-transaction-volume-usd?timespan=1year&showDataPoints=false&daysAverageString=7&show_header=true&scale=0&address=).

E-residentsus:

E-residentsuse kontseptsiooni ja vastavate isikut tõendavate dokumentide seaduse (edaspidi nimetarud *ITDS*) muudatuste lähtekohaks on eelkõige korrakaitseõigus ja mõjuanalüüsis on kirjeldatud karistusõiguslikke aspekte (vt. täpsemalt eelnõu 699SE seletuskiri).

Tuleb silmas pidada, et korrakaitseõiguses kasutatav „ohu" mõiste ei kattu täielikult finantssektori õiguslikus regulatsioonis kasutatava „riski" mõistega. Panganduse probleemiks ei ole niivõrd finantsriskide olemasolu iseenesest, vaid raskused ja valearvestused riskide hindamisel. ITDS seletuskiri ei ole kahjuks analüüsinud ega arvestanud finantssektori riskijuhtimise ja – hinnastamise spetsiifikat.

Nii Euroopa Liidu kui Eesti õigusaktid käsitlevad käesoleval ajal riske **määratletavate riskidena** (või kindlustatavate riskidena) sarnaselt tänapäeva majandusteaduses aktsepteeritava lähenemisega. Kirjanduses räägitakse statistiliste andmete alusel kvantifitseeritavatest riskidest. Õigusaktidega on kehtestatud nõuded riskide parameetrite hindamise, alusandmete kogumise ja vastavate empiiriliste andmete statistilistes mudelites kasutamise kohta. Krediidiasutuse usaldatavusnormatiivide regulatsiooni kohaselt peavad krediidiasutused koguma riskide hindamiseks **andmeid varasemate sündmuste** kohta, et statistiliste mudelite abil mõõta ja kalkuleerida oma tegevusega kaasnevaid riske. Krediidiasutus on kohustatud koguma empiirilisi andmeid, et oma igapäevasest majandustegevusest tulenevaid riske tuvastada, mõõta, juhtida ja jälgida. Andmete kogumise nõuete tõttu on muutunud palju täpsemaks riskide hinnastamine. Seega - krediidiasutuse omavahendite suurus (s.o. kapitalivajadus) sõltub otseselt krediidiasutuse krediidi-, turu-, operatsiooni- ja muude riskide tasemest, riskidele antud hinnangutest.

Alates 2007. aastast on kehtinud muuhulgas ka operatsiooniriski kapitalinõue. Määruse 575/2014 art 4 p 52 kohaselt on operatsioonirisk - risk saada kahju sisemiste protsesside, inimeste tegevuse ja süsteemide ebaadekvaatse toimimise või mittetoimimise või väliste sündmuste tagajärjel, mis hõlmab ka õiguslikku riski.

Operatsiooniriski riskiindikaatoriteks on näiteks arvutisüsteemide lubamatu kasutamine, tungimine infosüsteemi või arvutisse ning informatsiooni vargused. Operatsiooniriskideks on muuhulgas teise isiku identiteedi vargus või konto lubamatu kasutamine ja kindlasti ka rahapesu, terrorismi rahastamise ning rahvusvaheliste finantssanktsioonide rakendamise nõuete rikkumise juhtumid, samuti kõrvalekalded kliendi usaldusväärsuse hindamise regulatsioonist, samuti vaidlused seoses nõustamisega, vead tehingute tegemisel, sh vead

kliendi andmetes, vead andmete säilitamises ja andmevahetuses. Krediidiasutus on kohustatud koguma andmeid ja esitama Finantsinspektsioonile aruandeid operatsiooniriski kahjujuhtumite ja intsidentide kohta.
Lähtudes eeltoodust tuleks e-residentsuse pakkumisega seonduvaid riske täiendavalt analüüsida. Eraldi tuleks tähelepanu pöörata e-residentsusest lähtuvatele riskidele finantssektoris: (a) kas ja kuidas raskendab e-residentsus rahapesu ja terrorismi rahastamise tuvastamist ja tõkestamist; (b) kas e-residentsuse pakutavad võimalused teevad Eesti finantssektorist rahapesu ja terrorismi rahastamise sihtmärgi?

Virtuaalvaluutad

Viimastel aastatel on plahvatuslikult kasvanud virtuaalvaluutade kasutamise trend. Nimetatud uusi trende ja nende mõjusid on hinnatud Euroopa Pangandusjärelevalve (European Banking Authority, edaspidi nimetatud *EBA*) ja rahapesuvastase töökonna *Financial Action Task Force* (edaspidi nimetatud FATF) poolt. Nii EBA kui FATF-i asjakohased analüüsid[2] on näidanud, et virtuaalrahad kätkevad endas väga suuri rahapesu ja terrorismi rahastamise riske tänu eelkõige oma anonüümsusele. Lähtudes eeltoodust on erinevates töögruppides alanud arutelud kuidas virtuaalrahade teemasid tuleks reguleerida (sh analüüsib FATF asjakohaste standardite täiendamise võimalusi).

Eestis on virtuaalrahade vahendajad rahapesu ja terrorismi rahastamise tõkestamise seaduse (edaspidi nimetatud *RahaPTS*) kohustatud subjektis, sh tuleb neil taotleda vastav tegevusluba Rahapesu andmebüroolt. Antud regulatsioon põhineb siseriiklikul vastaval analüüsil (täpsemad põhjendused toodud RahaPTS seletuskirjas).

Hiina, Tai Kuningriik ja Venemaa on virtuaalrahade kasutamist veelgi rangemalt piiranud või nende kasutamist lausa täielikult keelanud. Litsentseerimise kohustuse on kehtestanud nt USA, Saksamaa ja Prantsusmaa. Virtuaalrahade reguleerimise võimalusi arutatakse aktiivselt mitmete hetkel menetluses olevate Euroopa Liidu direktiivide eelnõude raames (nt IV rahapesuvastase direktiivi eelnõu ja makseteenuste II direktiivi eelnõu raames). Lisaks on Euroopa Kohtus pooleli virtuaalvaluutade käibemaksustamise teemaline vaidlus.

Lähtudes eeltoodust ja arvestades teema aktuaalsust ning pooleliolevaid (sh vaidlust Euroopa Kohtus) arutelusid, ei ole hetkel mõistlik antud vallas kehtivat seadusandlust kergekäeliselt muuta. Muutes regulatsiooni on oht, et seda tuleb peagi uuesti teha, mis võib tekitada täiendavaid kulutusi ettevõtjatele.

---

[2] EBA virtuaalvaluutade teemaline analüüs on kättesaadav: http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf
FATF-i virtuaalvaluutade teemaline analüüs on kättesaadav: http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Järeldused

Uued paradigmad ja infotehnoloogilised arengud finantssektoris vajavad kahtlemata kõrgendatud tähelepanu ja nimetatud teemade käsitlemisel tuleb alati arvestada ka võimalikke ohtudega. Õige tasakaalu leidmine regulatsioonides on äärmiselt oluline.