FBIM Transactions
DOI 10.12709/fbim.03.03.01.20

PROBLEMI SA KOJIMA SE SUOČAVA IT SEKTOR U BORBI PROTIV PRANJA NOVCA U SRBIJI

PROBLEMS FACED BY IT SECTOR IN SERBIA IN COMBATING MONEY LAUNDERING

Dragan Ž. Đurđević, Miroslav D. Stevanović

Apstrakt

Države nastoje da spreče skrivanje prihoda i poresku evaziju, kako bi prikupile sredstva za javne potrebe i suzbile dominaciju nekontrolisanih ličnih interesa kao posledicu nelegalnih tokova novca. Informacione tehnologije (IT) unapređuju metode poreske evazije, korupcije i ilegalnih novčanih tokova, a ujedno i nove oblasti primene IT u suzbijanju i borbi protiv legalizacije nezakonitih prihoda i njihove upotrebe za društveno neprihvatljive svrhe. Pranje novca, korupcija i utaja poreza takođe su globalni problem. Međunarodni monetarni fond (MMF) je 2005. godine procenio da se opere oko 1,6 % od vrednosti kojom ukupno operišu banke i finansijski sektor. Kolika bi to suma mogla biti ukazuje podatak da je ukupni opticaj vrednosti 2013. godine iznosio oko 225 biliona dolara. Otuda su nastojanja da se politike borbe protiv pranja novca (AML) definišu na međunarodnom nivou i vodeća uloga međunarodnih tela, Finansijske akcione taktičke grupe (FATF) i Kancelarije UN za droge i kriminal (UNODC). Globalna finansijska vrednost u opticaju, više od tri puta premašuje vrednost globalnog bruto društvenog proizvoda (BDP). U tom svetlu, važno je uspostaviti metod praćenja tokova novca, u uslovima kada oni nisu odraz tržišta roba i usluga. U globalnom finansijskom okruženju, Srbija se suočava sa posledičnim problemima. Prema Global Financial Integrity i njihovoj proceni kumulativnog ilegalnog finansijskog toka iz 2013. godine, od 2002. do 2011. godine, sa 49,367 milijardi američkih dolara, Srbija je četvrti najveći izvoznik ilegalnog kapitala u Evropi, a petnaesti u svetu.

Cilj ovog rada je da ukaže na probleme sa kojima su suočeni korisnici i nosioci razvoja IT u AML. Oni s jedne strane potiču od stanja međunarodnih ekonomskih odnosa, a s druge od birokratskih ograničenja forenzičkog računovodstva.

Ključne reči: *IT sektor, pranje novca, utaja poreza, korupcija, prikrivanje, konverzija, transfer, integracija, bitkoin, virtuelne šeme, forenzičko računovodstvo*

Abstract

Nations seek to prevent concealment of incomes and evasion of taxes, in order to collect the funds for public purposes, and to prevent the domination on the basis of illicit money flow of uncontrolled interests. Information technologies (IT) advance the methods of evasion, corruption and illicit money transfers, and also open new areas of application of IT in suppression and combat against legalization of illegal incomes and their use for socially unacceptable purposes. Today, tax evasion, corruption and money laundering are also a global problem. The International Monetary Fund (IMF) estimated in 2005 that around 1.6% of the total amount globally

Adresa autora zaduženog za korespodenciju:
Dragan Đurđević
djurdjevic.dragan@gmail.com

operated by the banks and financial services sector is laundered. How large that sum could be, indicate the data that in 2013 the global financial assets flow amounted to around 225 billion US dollars. Hence, the endeavors to define the policies against money laundering (AML) on international level, and the leading role of international bodies, Financial Action Task Force (FATF) and United Nations Office on Drugs and Crime (UNODC). The global financial flow exceeds by more than threefold the value of the global gross product (GDP). In light of that fact, it is essential to establish a method of tracking the flows of money, in the circumstances in which it is not a reflection of the markets of goods and services. In such global financial environment, Serbia is faced with consequent problems. According to the Global Financial Integrity (2013) estimate of the cumulative illicit flow in the period 2002 - 2011, with US$49.367 billion dollars, it is the fourth exporter of illicit capital in Europe, and fifteenth in the World.

The intention of this paper is to indicate the problems facing users and developers of IT in AML. On one side they stem from the state of international economic relations, and on the other from bureaucratic limitations of forensic accounting.

Keywords: *IT Sector, money laundering, tax evasion, corruption, concealment, conversion, transfer, integration, bitcoin, virtual schemes, forensic accounting*

1. UVOD

Ilegalni tokovi novca uzrokuju brojne poremećaje na tržištu: investiranje u sektore sa manjim rizikom od otkrivanja, umesto u one sa višim prinosom; rast cena, a posebno nekretnina; rast potrošnje, a posebno uvoza robe široke potrošnje; smanjenje izvoza i ekonomskog razvoja; nelojalnu konkurenciju; negativan uticaj na direktne strane investicije zbog podrivanja realnog sektora i naduvavanja nekih sektora; korupciju; i jačanje sumnjivih prihoda i distribucije bogatstva, (Unger, 2007). Zato je važan zadatak države da onemogući pranje novca, pojavu korupcije i poresku evaziju.

Konvencija UN protiv transnacionalnog organizovanog kriminala iz 1988, proklamuje pranje novca (i korupciju) ilegalnim. Konvencija o suzbijanju finansiranja terorizma iz 1999. utvrđuje mere koje su države dužne da primenjuju radi sprečavanja i suzbijanja finansiranja terorista i terorističkih organizacija, kao i obavezu nadzora u cilju sprečavanja i suzbijanja kretanja sredstava za tu svrhu. Konvencija protiv korupcije iz 2003. afirmiše protivpravnost pranja prihoda od teških krivičnih dela i uspostavlja obavezu država da urede dužnosti banaka i finansijskih institucija na planu suzbijanja ove pojave, da obrazuju tela za finansijske obaveštajne poslove, kao i na široku međunarodnu saradnju. Savet bezbednosti UN je 2001. godine, delujući na osnovu Glave VII Povelje UN, usvojio odluku kojom utvrđuje obavezne mere za sprečavanje, suzbijanje i uskraćivanje utočišta finansijskom prometu i operacijama koje su u funkciji finansiranja terorizma (FT) i radi praćenja njihove primene uspostavio Komitet protiv terorizma. Kao odraz univerzalne političke saglasnosti o obavezi borbe protiv pranja novca Generalna skupština UN je 2006. godine usvojila Globalnu strategiju protiv terorizma i plan akcije, a u tom okviru i obavezu primene principa FATF. Ovo telo je osnovala grupa 7 najrazvijenijih država (G7), 1989. godine, u situaciji kada je vrednost ilegalne trgovine drogom u SAD i Evropi dostigla 124 milijarde dolara, a prihodi od toga raspoloživi za pranje 84 milijarde dolara, odnosno 0,8% BDP SAD i Evrope, odn. 0,5 % globalnog BDP. Prema proceni FATF, trgovina drogom čini oko četvrtinu prihoda od kriminalnih aktivnosti, a pranje zarade samo iz te delatnosti obuhvata 2% globalnog BDP. FATF, zajedno sa regionalnim telima, Međunarodnim monetarnim fondom (MMF) i Svetskom bankom, ocenjuje pridržavanje država međunarodnih principa AML. Ove principe (40) države implementiraju u vidu politika vezano za: sprečavanje ML, FT i koordinaciju; pranje novca i konfiskacije; FT i širenja oružja za masovno uništenje; preventivne mere; transparentnost i stvarno vlasništvo pravnih lica i aranžmana (trustova); ovlašćenja i odgovornosti nadležnih vlasti i institucionalne mere; i međunarodnu saradnju. Države ostvaruju principe u okviru svojih: pravnih sistema; mera finansijskih institucija, privrede i struke; institucionalnih mera; i međunarodne saradnje. U okviru ovih oblasti, principi obuhvataju: opseg inkriminacije pranja novca; privremene mere i konfiskacije; finansijsku poverljivost; postupanje sa klijentima i

dokumentima; prijavljivanje sumnjivih transakcija i pridržavanje; mere odvraćanja od ML i FT; mere u odnosu na države koje se ne pridržavaju preporuka; propise i nadzor; kompetentne vlasti, ovlašćenja i resursi; transparentnost javnih lica i aranžmana; konvencije; međusobna pravna pomoć i ekstradicija; i drugi oblici saradnje.

Primarni cilj AML je zaštita integriteta finansijskog sistema. U središtu tog sistema su banke, čije su usluge ključne za uredno funkcionisanje tržišne ekonomije. AML obuhvata i rad finansijskih i nefinansijskih institucija koje vrše monetarne usluge, promet nekretnina, konsalting i sl, koje su značajne za finansijski sistem, ali ne i za svakodnevno funkcionisanje tržišta. Procesne potrebe AML uslovile su razvoj pravnih aspekata računovodstva u posebnu disciplinu koja se bavi finansijskim istragama koje mogu dovesti do sudskog postupka, kao i primenom finansijskih činjenica u rešavanju sudskih postupaka. Forenzičko računovodstvo se sve šire primenjuje, a time i njegovo poimanje za korišćenjem računovodstvenih, revizorskih i istražnih veština u pravnim stvarima kao i njegova primena u dokazivanju ekonomskih transakcija, (Owojori & Asaolu, 2009).

2. OPŠTI PROBLEMI IT U AML

Pred korisnicima i nosiocima razvoja IT, prvi problem u AML je izbor parametara čije praćenje i analiza omogućava blagovremeno i pouzdano saznanje o nezakonitom novčanom toku, ili transakciji. Finansijske operacije i novac danas se tretiraju kao roba, što je izmenilo principe razmene na tržištu. Likvidnost više ne teži u realni sektor, već se iz njega izvlači i usmerava u tržište hartija od vrednosti, radi dizanja kreditnog potencijala. Raspoloživi kreditni iznosi se upumpavaju u spekulativni promet hartija od vrednosti, što generiše kreditne aranžmane, bez pokrića u robi i uslugama, a proizvođače roba i pružaoce usluga gura u sve dublja zaduženja. Statistička služba EU je 2013 godine usvojila smernice (ESA 2010), koje čak predviđaju iskazivanje prihoda od ilegalnih aktivnosti u BDP, pod stavkom usluga, pri čemu se aproksimacija prihoda od prostitucije vrši na strani ponude, a trgovine drogom na strani tražnje. Na taj način, evropske države mogu da iskažu viši BDP i tako uvećaju potencijal za povlačenje sredstava na tržištu kapitala.

Drugi problem je vezan za razvoj instrumenata i tehnika tzv. „industrije odbrane prihoda“, u okviru upravljanja finansijama, (Winters, 2011). Jedna od takvih tehnika je korišćenje poslovnih mogućnosti i sloboda koje pružaju države i teritorije izvan prebivališta, odn. sedišta (ofšor) i finansijske operacije kroz banke koje nude posebne usluge privatnosti i tajnosti (ofšor bankarski centri), odnosno korišćenje računa kod banaka koje u odnosu na državu sedišta (prebivališta) neće lako sprovesti mere represije na računu, niti će matičnoj državi korisnika slati informacije o poslovanju (ofšor bankarstvo). Podaci UN, MMF, Svetske banke i Banke za međunarodna poravnanja (BIS) ukazuju da je u ofšor sistem krajem 2012. godine bilo plasirano između 21 i 32 biliona dolara, (Henry, 2012). U tehnike odbrane prihoda spadaju i alternativno investiranje metodom koji štiti ulagača od tržišne neizvesnosti (hedž fondovi); ulaganje u operacije koje nemaju pristup institucionalnim investitorima (rizični privatni kapital); i konsultantske usluge. Ulaganje u hedž fondove ostvaruje stalni rast i u prvoj polovini 2014. dostiglo je 2.8 biliona dolara, (HFR, 2014). Vrednost kojom upravlja industrija rizičnog privatnog kapitala beleži rast i u 2013. godini je dostigla 3,5 biliona dolara, (Preqin, 2014). Uz to, procenjuje se da će prihodi od konsaltinga (ljudski resursi, IT, strategija, operacije, upravljanje i savetovanje) u 2014. godini dostići 431 milijardu dolara, (Plunkett Research, 2014). U finansijskom prometu su razvijeni i instrumenti koji omogućuju nezavisnost finansijskog tržišta od BDP. Odraz toga je tržište instrumenata zasnovanih na spekulativnim formulama (finansijskih derivativa), poput osiguranja gotovinskih kupovina, budućih ugovora, rekupovina i opcija. Vrednost derivativa u opticaju je 2002. godine iznosila oko 106 biliona, a 2013. je, dostigla 710 biliona dolara, (BIS, 2014), dok globalni BDP, prema podacima Svetske banke, iznosi oko 75 biliona dolara, (The World Bank, 2014).

Treći problem u primeni IT u AML su indikatori rizika u poslovanju banaka koji proističu iz potrebe realizovanja finansijskih tokova i ostvarivanja dobiti u postojećim uslovima na tržištu (Tabela 1). Primeri sankcija za najveće nezakonite novčane tokove ukazuju da se one utvrđuju vansudskim sporazumima sa vlastima. Pri tome, ni najviši iznosi poravnanja ne prelaze 15% prijavljene

Tabela 1: Sankcionisane banake za nezakonito poslovanje

Banka	Sumnjiva delatnost pranja novca	Sankcija
BNP Paribas	2005-2009 najmanje 2.663 telegrafskih transfera za klijente iz država pod sankcijama, u visini oko 8 milijardi USD	2014. poravnanje, oko 8,9 milijardi USD, da se izbegne krivični postupak
HSBC	2006–2009. iz filijala u Meksiku i Kolumbiji 15 milijardi USD gotovine bez kontrole porekla; 60 biliona USD godišnje telegrafskih transfera iz država pod sankcijama, bez nadzora...	2012. 1,921 milijarda USD da se izbegne krivični postupak
Standard Chartered	2001 - 2008 prikrivanje i dvojno iskazivanje 60.000 transakcija u Iran, u visini od 250 milijardi USD.	2012. 677 miliona USD, dogovor sa tužilaštvom
ING	Od 1990.-tih - 2007. falsifikovani izveštaji o 20.000 transakcija sa državama pod sankcijama u visini od najmanje 2 milijarde USD, Udeo u bankama iz kojih su vršeni transferi, školjke kompanije u Holandiji i ogranak u Belgiji za izbegavanje kontrole transfera u USD.	2012. 619 miliona USD, poravnanje sa regulatornim telima SAD
JP Morgan	2005. preko 1.700 telegrafskih transfera za lica prema kojima su zavedene sankcije, u visini od 178,5 miliona USD; 2009. garancije za akreditive. Nisu po nalogu OFAC dostavili dokumenta o transferima 2010-2011. za Kartum; 2008. upravljanje nenaplativim hipotekama	2011. 88.3 miliona USD, dogovor sa Departmanom Trezora 2013. 13 milijardi USD poravnanja zbog upravljanja hipotekama
Barclays	Od 1990-tih - 2006, prebacili stotine miliona USD kroz finansijski sistem SAD za račun banaka iz Irana, Burme, Libije, Kube i Sudana	2010. 298 miliona USD, dogovor sa tužilaštvom
RBS (ABN AMRO)	2005–2007 falsifikovali isprave o transakcijama „stotina miliona“ USD	2010. 500 miliona USD, dogovor sa tužilaštvom
Credit Suisse	1996 – 2006 falsifikovali isprave radi sprovođenja transakcija iz Sudana, Burme, Kube i Liberije, i najmanje 4.775 transfera, od preko 480 miliona USD, za račun fizičkih i pravnih lica iz Irana.	2009. 538 miliona USD, dogovor sa tužilaštvom, kao deo nagodbe sa Departmanom pravde
Lloyds Banking	Skrivanje informacija o klijentima za vršenje transfera	2009. 350 miliona USD, sporazum sa tužiocima.
Riggs Bank	Prikrivala račune koje je vodila za diktatore Nguemu Obasogoa i Augusta Pinočea (Ekvatorijalne Gvineje 700 miliona USD, Čile 10 miliona USD).	2004. priznali krivicu; kazna 16 miliona USD

Izvor: (Roosevelt Malloch & Mamorsky, 2013)

Tabela 2: Sankcionisane banake u aferi LIBOR i EURIBOR (zbirno, Evropa i SAD, do dec. 2013.)

Citigroup Inc	Poravnanje 95 miliona USD
Deutsche Bank AG	Poravnanje 983,7 miliona USD
HSBC Holdings	Poravnanje 107 miliona USD
ICAP PLC	Poravnanje 87,4 miliona USD
J.P. Morgan Chase	Poravnanje 108,4 miliona USD
Lloyds Banking Group	Poravnanje 370 miliona USD

Royal Bank of Scotland	Poravnanje 1,14 milijardi USD
Societe Generale	Poravnanje 604,7 miliona USD
RP Martin Holdings	Poravnanje 0,2 miliona USD
Rabobank Groep	Poravnanje 1,07 milijardi USD
UBS AG	Poravnanje 1,52 milijarde USD
Barclays	Poravnanje 453,6 miliona USD

Izvor: (WSJ, 2004)

šestomesečne dobiti tih banaka, (Hansen, Reuter, & Messick, 2014). Iz navedenog, a posebno nakon mahinacija sa Londonskom međubankarskom stopom (Tabela 2), stiče se utisak da su u globalnom finansijskom sistemu "vrednosti poverenja, odgovornosti i saradnje toliko podrivene da je sistemska prevara postala normalnost", (Roosevelt Malloch & Mamorsky, 2013). Naime, stopa koju banke međusobno naplaćuju trebalo bi da odražava finansijsko stanje bankarskog sektora. Komitet od 16 banaka prijavljuje stopu koju su međusobno naplaćivale i, nakon što se 4 najviše i najniže odbace, prosek ostalih objavljuju kao Libor. Ispostavilo se da su vodeće banke prikazivale manje stope da bi se stvorila veća tražnja ili prikrili problemi, ili više stope na zahtev trejdera. Teško je utvrditi koliki je deo obrta bio zahvaćen, ali se ukupna vrednost derivativa koji se kamate po Liboru samo u 2011. godini procenjuje na više stotina biliona dolara. Libor utiče na hipoteke i zajmove i ova mahinacija je pogodila tržište deset puta veće veličine od realne svetske ekonomije, čime je podriven finansijski poredak i savesni investitori. Nakon otkrića, američke Federalne rezerve (FED) su od svojih banka otkupile deo nenaplativih instrumenata i tako ih posredno dokapitalizovale, bez kamate, novcem iz budžeta. Izuzetost najvećih banaka od pravne odgovornosti je dodatno osnažena nefunkcionalnom regulativom. Kako su od 2008. do 2012. razvijene države u svoje vodeće banke upumpale oko 600 milijardi dolara, da bi ih spasile od nelikvidnosti, Bazelski komitet za nadzor bankarstva je 2012. usvojio regulatorni okvir za banke (Basel III), koji je fokusiran na problem spornog kapitala banaka, koji sadrži preko pet stotina strana i skoro osamdeset jednačina. Isti pristup je uočljiv i na nacionalnim nivoima. Obrazac kvartalnog izveštaja FED za 2014. godinu ima 2.271 rubriku; a američki zakon o reformi bankarskog sektora iz 2010. godine je do 2013. stigao do 3.200 strana sa samo 39 % celovito uređenih pravila, (CNBC, 2014).

Četvrti izvor problema IT u AML proističe iz činjenice da ukupni kapital u opticaju, prema pokazateljima MMF iz 2007. godine, kada je bio najviši, iznosi oko 11 biliona USD, tj. da predstavlja oko 19 % globalnog BDP, (The World Bank, 2013). To, samo po sebi, uslovljava objektivnu potrebu sa prikupljanjem gotovine u opticaju, što primorava banke da iznalaze načine da do nje dođu, bez obzira na poreklo. Tako su i države interesno prinuđene da trpe metode koje banke iznalaze radi aktiviranja kapitala, uprkos štetnih posledica nelegalnih tokova novca, usled integrisanja ilegalnih prihoda u finansijski sistem. Uz to, analize ilegalnih tokova novca iz država u razvoju ukazuju na posledicu u vidu dodatnog bogaćenja najbogatijih na štetu najsiromašnijih. Procenjuje se da ilegalni tok novca u državama u razvoju „potiče od pranja novca, poreske evazije i korupcije". Alexander Richard (2013), navodi i insajdersku trgovinu kao samostalan izvor ilegalnog novca. Taj novac „najčešće izlazi kroz komercijalni finansijski sistem". Uz manji investicioni potencijal, dodatnu štetu po države u razvoju predstavlja i urušavanje javnih rashoda. Procenjuje se da iz njih, kao posledica poreske evazije, godišnje odlazi oko 1 bilion dolara. Uprkos tome, Konvencija protiv mita OEBS fokusirana je samo na suzbijanje davanja mita, ali ne i na primanje.

3. PROBLEM PRISTUPA U PRAKSI

Kao izvor novca za pranje, pažnju međunarodne zajednice prva je privukla trgovina drogom. Kancelarija UN za droge i kriminal (UNODC) osnovana je 1997, sa zaduženjem da sprovodi globalni program protiv ML, prihoda od kriminala i FT. Umesto na usaglašavanje opštih pravila i zajedničke akcije u okviru mandata UN, UNODC je fokusiran na izradu studija i preseka saznanja. (UNODC, 2011) Iako nema operativnih zadataka, ovo telo ima unutrašnje organizacione jedinice: za analizu pretnji, politika i javnih poslova; za primenu zakona, organizovani kriminal i AML; za integrisani program i nadzor, za korupciju i ekonomski kriminal; i za globalni program AML. Posledica toga je da još uvek nema ni nacrta međunarodnog ugovora koji bi uredio obaveznu koordiniranu akciju protiv legalizacije prihoda, pa ni onog koji potiče od kriminala.

Nedelotvornost režima AML potiče i iz interesa kojima pranje novca koristi. Procenjuje se da je 2012. godine preko 8 biliona dolara bilo od strane fizičkih lica pohranjeno u poreskim rajevima, a najviše u britanskim prekomorskim teritorijama i entitetima zavisnim od Krune, kao i u Švajcarskoj, (Dransfield, 2013). Analize ukazuju da se većina priliva u ofšor centre, narednih godina očekuje iz

izrastajućih ekonomija. Kapital teži da izbegne poreska opterećenja i da bude u bankarskom sistemu odakle će imati pristup investicionom bankarstvu, koje je koncentrisano u nekoliko finansijskih centara. Zvanični kapital odlazi iz izrastajućih u razvijena tržišta, dok privatni kapital teži u suprotnom smeru. Finansijski instrumenti su 2010. godine bili koncentrisani u tri regiona: Evropa – 33%, SAD i Kanada - 31%, Azija/Pacifik – 29%, dok su na Bliskom istoku i Africi - 3.5%, a u Južnoj Americi - 3.0%. Iz toga proističe podudarnost interesa najbogatijih lica i vodećih finansijskih institucija, ali i država njihovih prebivališta i sedišta. U takvim uslovima, na međunarodnom nivou konsenzus je bio moguć samo o neprihvatljivosti pranja prihoda od kriminala, ali ne i računovodstvenih i pravnih metoda denacionalizacije novca. Prema proceni MMF, u predstojećem periodu najveći razvoj očekuje u izrastajućim ekonomijama. Realno, međunarodni finansijski sistem, koncipiran u korist najmoćnijih država i privilegovanih investicionih banaka, neće prestati da privlači kapital ne birajući sredstva, a nastojaće, jedino, da ograniči druge učesnike na tržištu.

Pristup problemu ilegalnih finansijskih tokova je naglašeno birokratski. Na planu AML, preko 180 država je prihvatilo redovne procene i nadovezujuće mehanizme koje predviđa globalna mreža FATF. Na planu poreske evazije, Globalni forum za transparentnost i razmenu informacija u svrhu poreza vrši monitoring standarda, dok na planu mita, Radna grupa za mito OEBS nadgleda pridržavanje potpisnica obaveza prihvaćenih u Konvenciji za borbu protiv mita stranih javnih zvaničnika u međunarodnim poslovnim transakcijama. Ovi mehanizmi ne obezbeđuju sankcionisanje finansijskih institucija i bankarskih organizacija koje sprovode neracionalne transfere, ni zaplenu i povraćaj imovine, što podriva svrsishodnost međunarodnih standarda AML i nadgledanja njihove primene, osim za potrebe evidencija i analiza. U tom pravcu se oblikuju napori i u okviru UN. Naime, saglasnost o obavezi država da primenjuju mere AML postoji samo na planu borbe protiv transnacionalnog organizovanog kriminala, trgovine drogom i FT, ali ne i na planu suzbijanja denacionalizacije novca i poreske evazije. Otuda, rizik operacija pranja novca svodi se na prihode iz kriminala ili ako je namenjen za finansiranje terorizma. Pozitivan primer pristupa pranju novca predstavlja ideja iz Zakona o pridržavanju poreskih obaveza vlasnika računa u inostranstvu iz 2014. godine, koji obavezuje državljane SAD da prijave imovinu u inostranstvu, a poresku administraciju ovlašćuje da pribavlja informacije o tome od trećih država. Na taj način se uvodi kontrola odliva novca, a samim tim i njegovog ilegalnog toka, odnosno pranja, bez obzira na poreklo i svrhu korišćenja.

Uticaj ilegalnog prometa samo u trgovini drogom, falsifikovanju, trafikingu ljudi, akciznim robama i krivičnim delima protiv životne sredine procenjuje se na oko 1,5 biliona dolara godišnje, (Picard, 2013). Logično je da u stanju endemske nelikvidnosti, međunarodni finansijski sistem ne može da priušti, sebi, da ne stavi ovaj novac u funkciju. U tom pravcu su ustrojeni i međunarodni računovodstveni principi. Pomenuta metodologija o obračunu nezakonitih prihoda Evrostat proističe iz Sistema nacionalnih obračuna MMF (SNA) iz 1993, koji je usvojen od strane Statističke komisije UN 2009. i noveliran 2010. Kako bi se omogućili kreditni aranžmani međunarodnih finansijskih institucija, SNA (1993.) proklamuje da “ilegalna dobra i usluge moraju biti ubeležene u sistem”. Prva država koja je objavila primenu ovakvog obračuna BDP bila je Kolumbija, 1999. godine. Međutim, spekulacije da proizvodnja droge ima koren u ekonomskim uzrocima, do danas nisu potvrđene utvrđivanjem bilo kakve značajne veze između postojanja i obima gajenja koke sa BDP ili indeksom razvoja. U Evropi, se ispostavilo, da je Mađarska još od 1994. godine uračunavala prihode od prostitucije u svoj BDP, (Bloomberg, 2014).

4. PRIMENA INFORMACIONE TEHNOLOGIJE U AML

Brz rast informacionih tehnologija, a posebno Interneta doveo je do praktičnih, pravnih i etičkih pitanja, koja se odnose na privatnost i zaštitu ličnosti, učesnika u elektronskim komunikacijama. Mogućnosti koje otvaraju sofisticirane tehnike, “celokupno ljudsko znanje se udvostručilo između 1900-1950, od tada se udvostručava svakih 5-8 godina (Čekerevac, 2009)“, posebno zbog nedovoljnog poznavanja, stvaraju rizik od pranja novca i finansiranja terorizma, zbog čega im se mora uvažiti značaj i pokloniti posebna pažnja. Bezbednosni propusti nastaju kod onih davaoca usluga plaćanja preko interneta, koji

omogućavaju otvaranje računa i obavljanje transakcija bez identifikovanja i evidentiranja podataka o korisniku. Na ovaj način se omogućava da nakon aktivacije računa, novac može biti upućen na bilo koju destinaciju u svetu, a da se pritom izbegne bankarski sistem. U ove načine transfera mogu se uvrstiti i kreditne i debitne kartice. U pojedinim državama, prema propisima u vezi sa AML i finansiranja terorizma (FT), pružaoci usluga sistema elektronskog plaćanja nisu obuhvaćeni u lica i ustanova čije su aktivnosti povezane sa novcem i imovinom. Analogno tome, za njih ne važe zakoni protiv pranja novca i finansiranja terorizma i zahtevi koji iz njih proizilaze. Ovi propusti otvaraju mogućnosti za pranje novca i legalizaciju novca stečenog na nezakonit način.

Bezbednost informacija i službenih podataka predstavlja jedno od ključnih pitanja, za sve organizacione i poslovne sisteme. Podatak, kao kategorija, sam po sebi predstavlja izazov i podstiče znatiželju kod onih koji imaju potrebu da ga poseduju. Legalni izvori podataka moraju biti adekvatno zaštićeni i o njima se mora voditi odgovarajuća sistemska briga. Savremeni metodi prikupljanja, klasifikovanja, obrade, arhiviranja i čuvanja podataka, osim efikasnosti, brzine obrade i trajnosti medijuma - nosača podataka, doneli su i gomilu nerešenih pitanja iz oblasti bezbednosti i zaštite podataka. Digitalni oblik zapisa podataka, koji se koristi u informacionim sistemima, omogućio je čuvanje na desetine miliona podataka na fizički zanemarljivom prostoru. Arhive podataka papirnog oblika, nekada merene u kubnim metrima, danas su dostupne na prostoru veličine nekoliko mm^2. Ovako mali fizički obim postaje predmet velikih stručnih polemika o metodama zaštite i neporecivosti podataka. Da bi sprečila i preventivno delovala svaka iole ozbiljna organizaciona celina mora predvideti odgovarajuća normativna akta, tehnike i metode u skladu sa razvojem i napretkom primenjenih tehničkih standarda nad datim podacima. Neophodno je dodeliti stepen poverljivosti svim podacima - dokumentima, i na taj način izvršiti njihovu preliminarnu zaštitu (Petrović, 2004).

5. KIBER PRANJE NOVCA

Indikatori koji ukazuju na pranje novca u klasičnom platnom prometu, predstavljali su osnov za formiranje liste indikatora u kiber platnom prometu. Prvi znaci mogućeg pranja novca ili finansiranja terorizma su neuobičajene aktivnosti u vidu postojanja jednog ili više indikatora:

- lica koja drže veliki broj računa kod istog pružaoca usluga plaćanja preko interneta;
- nepodudarnosti između podnetih identifikacionih podataka klijenta i IP adresa;
- sumnjive IP adrese i sumnjiva korisnička imena mogu da se koriste za otkrivanje toka prljavog novca;
- logovanja ili pokušaj logovanja sa nepouzdanih IP adresa ili korisničkih ID koji su ranije prepoznati kao sumnjivi; pokušaji smeštanja već prepoznatih nepouzdanih „kukija“;
- telegrafski transferi od donatorskih organizacija u korist firmi sa sedištima u zemljama poznatim kao bankarska ili poreska utočišta;
- uplate uglavnom od nepoznatih trećih stranaka nakon kojih odmah dolazi do podizanja gotovine ili međunarodnih transfera;
- izdavanje čekova, naloga za plaćanje ili drugih finansijskih instrumenata, koji su sekvencijalno numerisani, u korist istog lica ili firme, ili lica i firmi čija imena slično zvuče;
- aranžmani podizanja gotovine u kojima se uplate (na primer u SAD) neposredno povezane sa podizanjem gotovine sa bankomata u problematičnim zemljama. Obrnute transakcije ove vrste su takođe sumnjive;
- preduzeća sa uobičajeno pasivnim prometom, ili novo osnovana preduzeća, obavljaju neobično mnogo transakcija, što nije u skladu sa profilom lica;
- korišćenje više računa za prikupljanje sredstava, koja se prenose u korist istih primalaca u drugim zemljama;
- transakcije novca čije su poreklo ofšor zone, zemlje koje se ne pridržavaju međunarodnih dogovora u oblasti borbe protiv pranja novca i finansiranja terorizma, itd;
- akumulacija kapitala (transferi između bankovnih računa povezanih lica, ili donacije bez razumnog osnova);
- uplate uglavnom gotovinski ili putem

instrumenata sa osobinama gotovine (na primer pri-peid kartice), obično ispod zakonskog praga za prijavljivanje.
- ustanovljavanje čvrstih poslovnih odnosa ili vršenje transakcija elektronskim izjavama, elektronskim dokumentima elektronskog potpisa ili drugog oblika bez prisustva klijenta;
- nejasni podaci o poslovnim aktivnostima klijenta ili razlozima za korišćenje metoda plaćanja preko interneta umesto klasičnih metoda (uobičajenih za firme i komercijalna plaćanja);
- transakcije ili podizanje novca (u obliku gotovine, čekova, telegrafskih transfera, itd.) pod uslovima koji ne odgovaraju prethodnim uslovima o depozitima i dr.

Savremeni svet informatičkog poslovanja, digitalnog potpisa, e-bankarstva, velikih brzina obavljanja finansijskih transakcija otvara i neslućene mogućnosti analitičkog i statističkog rasuđivanja, u svim segmentima njegove implementacije. U sklopu toga nameće se potreba, u svrhu praćenja aktivnosti koje se odnose na pranje novca za finansiranje terorizma, za formiranjem određenih baza podataka. Formiranjem baza podataka i baza izveštaja o aktivnostima pranja novca koji se koristi u finansiranju terorizma omogućio bi se detaljan statistički i analitički izvor materijala koji bi u sinergiji sa drugim finansijskim alatima i odgovarajućim naučnim doktrinama, omogućio ranu prognozu i pretpostavku kretanja odgovarajućih fondova kroz transakcije na osnovu zabeleženih i pokušanih aktivnosti tokom analitičkog perioda.

Ovakve vrste baza moraju da sadrže, osim elementarnih podataka koji se sastoje od identifikacionih podataka učesnika u transakcijama, vremenu izvršenja transakcija, broju obavljenih među transakcija, koje vode prema konačnoj – završnoj transakciji, i podatke o izveštajima u kojima su se učesnici sumnjivih transakcija spominjali, a da iste nisu realizovane ili da nisu ostvarene, bilo zbog odustajanja njihovih učesnika, bilo zbog intervencije ovlašćenog osoblja finansijskih obaveštajnih jedinica.

Ova vrsta podataka bi se morala prikupljati u realnom vremenu "on-line" na jednom centralizovanom mestu. Odgovarajućom programskom podrškom vršilo bi se selektivno odlučivanje i ažuriranje podataka, u smislu formiranja baza koje bi sadržavale podatke o svim aktivnostima u "zajedničkoj platnoj mreži" koja bi bila "mreža svih finansijski transakcionih mreža", (Đurđević, 2013). Na tom mestu bi se beležile aktivnosti koje se odnose na sve dnevne transfere veće od obaveznog zakonskog praga izveštavanja, kao i podaci o broju učestalosti pojavljivanja odgovarajućih učesnika u transakcijama do dozvoljenog transakcionog limita, do evidentiranih samih pokušaja pranja novca koje bi sistem detektovao. Ovakva kategorija podataka bi morala biti pod obaveznim nadzorom Uprave za sprečavanje pranja novca - centralne finansijske obaveštajne jedinice. Principi zaštite i čuvanja ove vrste podataka bi svakako morali biti preuzeti iz prakse, do sada najzastupljenijih kriptoloških metoda i načina korišćenja podataka, uz poštovanje svih bezbednosnih procedura koje prate sisteme kripto zaštite. Primenom metoda: trasiranja, indukcije, dedukcije, generalizacije, komparacije, mikro i makro finansijske analize, statističkih i drugih savremenih instrumenata sa visokim procentom tačnosti, može se predvideti naredni korak "monitorisanog klijenta".

6. PLASTIČNI I VIRTUELNI NOVAC

Elektronska trgovina hartijama od vrednosti, drugim robama i uslugama i elektronski platni promet, omogućavaju servisiranje znatno većeg obima veoma složenih transakcija, ali je istovremeno sve teže analitički pratiti, a još teže ući u prirodu svake pojedinačne transakcije i to samo onih koje prolaze kroz legalne kanale. Elektronska trgovina (e-trgovina) uopšteno otvara nove mogućnosti ali kreira i nove probleme. Detaljnom analizom studije, (FATF, 2010) koja je zasnovana na pregledu značajnih obelodanjenih sumnjivih aktivnosti i identifikaciji određenog broja karakteristika sumnjivih aktivnosti povezanih sa ovom vrstom kartica definisani su sledeći indikatori:

- Strukturirana plaćanja u gotovom za neizmirene iznose kredita, odnosno salda na kreditnim karticama.
- Pokušaj "treće strane" da plati u gotovom u ime vlasnika kartica.
- Zloupotrebe kreditnih kartica, (korišćenje izgubljenih ili ukradenih kartica od strane trećih lica).

- Korišćenje avansa u gotovom sa računa kreditne kartice, da bi se kupili čekovi na donosioca,
- Korišćenje avansa u gotovom sa računa kreditne kartice, da se elektronski prebace fondovi na inostrane destinacije,
- Ulaganja avansnih depozita na štedne ili tekuće račune.

Prethodno navedene karakteristike predstavljaju samo deo obelodanjenih aktivnosti, koje mogu biti označene kao samostalni čin, ali isto tako mogu biti deo šire šeme aktivnosti povezane sa različitim finansijskim kriminalima, kao i pranja novca i terorističkog finansiranja.

7. VIRTUELNE ŠEME

U dokumentu „Virtual currency schemes", (ECB, 2012) ECB je obrazložila fenomen nazvan Virtuelne šeme. Ova pojava je nastala ubrzanim razvojem interneta i inicirala razvoj i primenu virtuelnih valuta. U početnom stadijumu razvoja virtuelnih valuta, primena je bila ograničena na zatvorene grupe i mahom se odnosila na igrice, kladionice i sl. Eksperti evropske centralne banke, brzo su uočili moguće opasnosti i potencijale masovnog korišćenja ovog resursa. Detaljnom analizom uočenih aktivnosti od strane kreatora virtuelnih valuta uočene su tri kategorije šema:

I. potpuno zatvorene šeme, korišćene u onlajn igrama;
II. virtuelne šeme koje imaju jednosmerni tok (obično prema unutra), za pravi novac kupuje se „virtuelna valuta" koja se koristi za virtuelna dobra i usluge na internetu, izuzetno za realna dobra i usluge;
III. virtuelne šeme koje imaju dvosmerno kretanje novca, mogu se menjati u/iz realne valute, i koriste se kako za kupovinu virtuelnih, tako i realnih dobara i usluga.

Bitno obeležje pobrojanih šema je nepostojanje posrednika na relaciji kupac - prodavac. Nedostatak regulatornog i zakonskog okvira, omogućava privatnom, nefinansijskom subjektu, da u njenom kreiranju, razmeni i korišćenju izmiče monitoringu i reviziji. Analitičkim pristupom sagledavanju razlika između virtuelnih šema i e-novca, uočava se sledeće: rizik e-novca vezan je samo za zloupotrebe informacionih sistema, dok kod virtuelne šeme, pored rizika od zloupotrebe informacionih tehnologija, postoji kreditni i rizik likvidnosti, kao apsolutno nepredvidive kategorije.

U daljem tekstu pomenutog dokumenta zapaža se zabrinutost eksperata na budući uticaj ovih šema na ekonomiju i reputaciju centralne banke, ukazujući na sledeće, da one u ovom trenutku:

- ne nose rizik na cenovnu stabilnost, sve dok je ukupan obim virtuelnog novca relativno mali;
- ne mogu uticati na finansijsku stabilnost, sve dok je njihov upliv u realnu ekonomiju zanemariv, i ne postoji šira mreža prihvatilaca;
- budući da nisu monitorisane i kontrolisane, svaki učesnik u šemi to radi na sopstveni rizik;
- mogu predstavljati izazov za državne organe, jer zbog svoje prirode lako mogu postati instrument za pranje novca i finansiranje kriminalnih aktivnosti;
- mogu imati negativan uticaj na reputaciju centralne banke, budući da je njihov rast nepredvidiv, i ekspanzija takve valute može stvoriti utisak da centralna banka ne radi svoj posao;
- nisu podložne reviziji, nameću obavezu centralnoj banci da se priprema za iznalaženje rešenja u smislu kontrole i nadzora kretanja ove valute.

Pojava virtuelnih moneta je od strane šire društvene zajednice tretirana kao jedna od tehničkih inovacija, sa predznakom rizično, nepouzdano, verovatno kratkotrajno, međutim moramo naglasiti da je isti put prošao i plastični - kartični novac, kasnije prihvaćen i uvučen u regulatorni okvir. Jedan od argumenata koji je, u prvo vreme, privukao zaluđenike za tehnologiju, internet i investitore avanturiste je taj, što ove monete ne kontrolišu centralne banke koje, opet, kontrolišu vlade. Svetskim moćnicima ne odgovara korišćenje paralelnih, virtuelnih valuta, jer one omogućavaju zaobilaženje globalnih pravila. Iza virtuelnih moneta ne stoje centralne banke, njihovu vrednost utvrđuje mnoštvo računara a poseduju i prirodnu zaštitu od inflacije i prevare.

U poplavi virtuelnih valuta koja je poslednjih pet godina uzela maha, (Bitcoin, Litecoin, Peercoin, Dogecoin, Namecoin, Blackcoin, Darkcoin ...) primat u međunarodnim okvirima zauzeo je Bitcoin (BtC), valuta sa virtuelnom šemom bazirana na „pear to pear" mreži.

Bitcoin (BtC) virtuelna valuta, se pojavila 2009. godine i najverovatnije je delo japanskih programera mada se na internet forumima ovo delo pripisuje Satoši Nakamotu. Sistem je baziran na BitTorrent protokolu za deljenje fajlova preko interneta. Jedan bitkoin u svom izvornom obliku predstavlja niz digitalnih potpisa, šire o tome (Čekerevac & Čekerevac, 2014). Imalac ove valute poseduje par ključeva, javni i tajni, koji su smešteni lokalno, u računaru vlasnika, formirajući virtuelni novčanik. Gubitkom ovih ključeva došlo bi do gubitka „novca“. Kako se emitovanje ovog novca zasniva na veoma komplikovanim kripto algoritmima i ne zavisi od drugih valuta, odluka vlada i centralnih banaka, teoretski, može se reći da je zaštićen od monetarnog udara i finansijskih instrumenata koji bi mogli uticati na njegovu vrednost. Vrlo je značajno naglasiti, u prilog stabilnosti ove valute, algoritamska procena da je maksimalan mogući broj bitkoina u opticaju ograničen na 21 milion, što ograničava nekontrolisanu emisiju. Najjednostavniji način za posedovanje ove valute je putem prodaje ili pružanjem usluge elektronskim putem, odnosno naplatom u pomenutoj valuti. Drugi, daleko teži i nepovoljniji način, je da se uključite u jedan složen proces putem interneta u operaciju koja se zove „rudarenje“. Veliki broj zemlja i njihove poreske vlasti bore se s problemom regulative novonastalog virtuelnog tržišta, dok neke sa visokom dozom realnosti vide upotrebu bitkoina kao mogućnost za izbegavanje poreza, pranje novca, finansiranje terorizma, i mogućnosti da je samo mašta ograničenje za valutu, koja u sekundi može preći sa jednog, na drugi kraj sveta, bez kontrole treće strane i monitoringa. Rusija je proglasila transakcije bitkoinima nelegalnim, (RT, 2014), a Kina je zabranila svojim bankama da prihvataju trgovanje u toj virtuelnoj valuti, a ima poziva da to isto uradi SAD, (FINRA, 2014). Singapur je uveo porez na trgovinu bitkoinima, a bitkoine registruje kao robu. Preporuka ECB je detaljno praćenje mogućeg rizika na cenovnu, finansijsku stabilnost i platni sistem, kroz praćenje interakcija bitkoina i realnog sveta. Ono što se sa sigurnošću može ustanoviti bitkoin je ušao u tokove realnih ekonomija, i da se ovim fenomenom danas bave ekonomisti, pravnici, IT stručnjaci, hakeri, centralne banke, bezbednosne službe.

8. ULOGA FORENZIČKE REVIZIJE U SPREČAVANJU PRANJA NOVCA U SRBIJI

Revizija informacionih sistema (*IS*), informacionih sistema za podršku poslovnom odlučivanju (*MIS*) i informacionih tehnologija šire uzev (*IT*) se kreće u pravcu revizorskog pregleda sistema kontrola u okviru implementirane informacione tehnologije određenog poslovnog, javnog ili čisto privatnog u građanskom smislu reči entiteta. U praksi se ova vrsta revizorskog pregleda sprovodi u sadejstvu sa drugim, rekli bi smo primarnim tipom revizije, sa statutarnom revizijom finansijskih iskaza, kao i sa internom revizijom koja je u suštini unutrašnja usluga firme samoj sebi. Savremeni pristup od sredine prve decenije XXI veka je da se ova oblast klasifikuje kao revizija IT. Stoga se IT revizija može definisati kao: *"...proces prikupljanja i vrednovanja* revizorskih *dokaza o informacionim sistemima organizacije, praksama i operacijama"* (Ljutić & Polić, 2002). Pribavljeni revizorski dokazi kroz proces IT revizije se potom evaluiraju sa ciljem da mogu da obezbede da su informacioni sistemi poslovne organizacije bezbedni, da su sredstva odnosno IT resursi zaštićeni, da se održava integritet poslovnih podataka i evidencija, da IT funkcioniše efektivno i efikasno da bi se ostvarivali ciljevi i rezultati firme.

Cilj IT revizije je sličan cilju revizije finansijskih iskaza – da proučava i evaluira osnovne elemente interne kontrole, što bi se paralelno moglo odrediti kao funkcionisanje interne kontrole u suzbijanju pranja novca. Efektivnost i efikasnost IT sistema se procenjuje u odnosu na nacionalnu regulativu i međunarodne standarde, smernice, obaveze, konvencije i najbolju praksu, posebno u domenu zaštite informacionih sredstava, sa ciljem da se kroz IT reviziju sprovede vrednovanje sposobnosti organizacije u domenu informacionih sistema u pogledu raspoloživosti, poverljivosti i integriteta.

Revizija informacionih sistema se temelji na potrebama ispomoći finansijskoj reviziji, pa se stoga smatra veoma mladom naukom, ovaj tip revizije iziskuje sve više praktičnih znanja revizora iz informacionih tehnologija kao i njihovu adekvatnu primenu prilikom obavljanja revizorskih aktivnosti. Ključnu tačku u reviziji informacionih sistema čini procena efikasnosti internih kontrola informacionog sistema. Skup internih kontrola, sa stanovišta revizije informacionih sistema

predstavlja sistem koji ima ulogu rane detekcije, uočavanja, sprečavanja i reprograma neželjenih efekata i procesa u informatičkom okruženju.

Rukovodstvo finansijske institucije u sadejstvu sa rukovodstvom IT sektora, implementira, ocenjuje efikasnost internih kontrola unutar informacionog sistema i solidarno snosi odgovornost za moguće propuste i rizike, koji za posledicu mogu imati finansijski gubitak, poremećaj poslovnih procesa, gubitak poslovnog ugleda, gubitak tržišta, smanjenje konkurentne sposobnosti i drugo. Pored, sad već standardne revizije informacionih sistema, imamo i pojavu podsistema u ovoj oblasti kao što su: revizija kontrola na nivou entiteta, revizija centra podataka, revizija opšte mrežne opreme, revizija mrežne i komunikacione infrastrukture, revizija windows operativnih sistema, revizija middleware i baza podataka, revizija aplikacija, revizija kompanijskih projekata, revizija okvira i standarda, kao i forenzičko računovodstvo. Poštujući zakonske obaveze koje su nastale na osnovu članstva u međunarodnim organizacijama ili poštujući preporuke strukovnih udruženja, sprovođenje revizije informacionih tehnologija, naročito u forenzičke svrhe, odvija se kroz regulative i smernice centralnih banaka svake zemlje. Tim se zakonima, raznim dodatnim aktima i propratnim propisima regulišu neophodne kontrole koje se implementiraju, kako bi se rizik izveštavanja smanjio na prihvatljiv nivo.

Veliki problem za revizora u procesu testiranja podataka predstavlja potreba za utvrđivanjem verzije programske aplikacije koja se koristi u procesu rada u odnosu na aplikaciju koja je data na reviziju, zapravo teško je doći do sigurnog pokazatelja da se ne radi o unapred pripremljenoj zameni, kako bi se obmanuo revizor. Radi utvrđivanja kvaliteta rada računovodstvenog softvera često je neophodno da se testiranje ugrađenih revizorskih kontrola i njihovih mogućnosti sprovede na aktuelnim - pravim podacima, normalno, uz mere predostrožnosti pripremom sigurnosnih kopija i drugih preduslova, kako bi se obezbedio maksimalan konfor revizoru i maksimalna obezbeđenost vlasniku informacionog sitema. Shvativši realnu opasnost od pranja novca, kao dela organizovanog kriminala internacionalnog karaktera, strukovna udruženja su krenula u razvoj sopstvene strategije za borbu protiv pranja novca kroz sektor finansija, platnog prometa i informacionih tehnologija, definišući određene preporuke i okvire.

Kako postoji više metodologija i standarda koji se bave ovom problematikom, izbor je na revizoru, da odabere pristup i način rada, a na raspolaganju su: Cobit, ITIL, COSO, ISO 17799, ISO 9000. Potrebno je naglasiti da se kod svih pobrojanih standarda, efikasnost kontrola meri istom mernom skalom, ocenama zrelosti od 0 do 5. Jedan od najpopularnijih okvira ili standard kontrole informacionih sistema je Cobit (Control Objectives for Information and Related Technologies). Cobit je svetski prihvaćen standard u okviru koga se nalaze propisane individualne kontrole za određene delove informacionog sistema i povezane procese u okviru njega. Udarna snaga Cobit-a je razvoj jasnih preporuka, dobre prakse uz kontrolu aplikacija informacionih tehnologija u privatnom i državnom sektoru. Ovaj standard je razvijen od strane ISACA-e, ISACF-a i IT Governance instituta. Primenom Cobit standarda korisnici (menadžeri, rukovodioci, revizori) imaju mogućnost efikasnijeg rukovođenja i kontrole procesa informacionih sistema i pridruženih tehnologija (Brand & Boonen, 2010). Cobit sadrži 34 kontrolna cilja kojima definiše "uspeh" ispunjenosti funkcionalnih ciljeva informacionog sistema sa oko 300 detaljnih informatičkih kontrola, raspoređenih u četiri kategorije: "Planiranje, organizacija rada i upravljanje IS", "Razvoj i implementacija IS", "Isporuka i podrška radu IS" i "Nadzor i procena rada IS".

9. BORBA PROTIV PRANJA NOVCA U REPUBLICI SRBIJI

Početkom 2009. godine usvojen je Zakon o sprečavanju pranja novca i finansiranja terorizma, koji predstavlja nove napore u ovoj oblasti, sa naglaskom na usaglašavanje domaćeg s međunarodnim zakonodavstvom i standardima iz ove oblasti, a pre svega s propisima i standardima Evropske unije. Usvajanjem Nacionalne strategije za borbu protiv pranja novca i finansiranja terorizma, Vlada Republike Srbije je unapredila svoje aktivnosti sa ciljem da se na osnovu opisa i analize zakonodavnog, institucionalnog i operativnog okvira borbe protiv pranja novca i finansiranja terorizma daju preporuke za unapređenje sistema sprečavanja pranja novca i finansiranja terorizma. Zakonodavni okvir je

predvideo krivično delo pranja novca i sankcionisao ga članom 231. Krivičnog zakonika („Službeni glasnik RS, br. 85/05, 88/05, 107/05, 72/09 i 111/09). Osim pravnog uređenja, postoji potreba daljeg razvoja informacione tehnologije i saradnje između zaposlenih koji su angažovani na poslovima sprečavanja pranja novca i finansiranja terorizma i zaposlenih u drugim delovima banke (npr. zaposleni koji se bave informacionom tehnologijom), (Stojanović, Petrović, & Stepanović, 2010). Budući da se 26 banaka izjasnilo da ima softver za prepoznavanje sumnjivih transakcija, uz primenu određenog broja indikatora, ima prostora za dodatno napredovanje u ovoj oblasti, kako bi sve banke imale odgovarajuće softvere.

10. ZAKLJUČAK

Novac se pere kroz transakcije koje dopuštaju zakoni, ili izostanak efikasne kontrole finansijskog tržišta, ali i globalna ekonomija. U te svrhe je razvijen niz tokova roba, novca i obligacionih instrumenata, od tradicionalnih poput nekretnina, zabava i igara na sreću, do sve kompleksnijih, poput tržišta derivativa i primene havala sistema. Njihovo presecanje, a posebno u uslovima endemske globalne nelikvidnosti, ne može se ostvariti metodama liberalne države. Pravni i knjigovodstveni metodi opterećeni su uticajem globalne situacije i postaju instrumentalizovani, te se razvijaju kao nepregledni birokratizovani sistemi koji onemogućavaju efikasnu kontrolu i smisaono tumačenje pokazatelja. Ukoliko je tržište manipulisano od strane organizovanog kriminala, tržište i administracije ne mogu da deluju ukoliko se ne ostvari kontrola rizičnih sektora u kojima u dodir dolaze poslovni svet i siva zona, (Costa, 2014). To je segment u kojem je informacija od suštinskog značaja. Otuda uspešnost AML zavisi od istraživanja i dokumentovanja tokova novca, što uz obaveštajni rad, zavisi i od primene IT. Ovlašćeni revizori informacionih sistema (forenzičari), zasnivaju radne procese i aktivnosti na međunarodnim standardima revizije kao zvaničnoj polaznoj osnovi. Koristeći upitnik za sticanje revizorskog mišljenja, revizori nastoje da maksimalno ispoštuju sve preporuke iz utvrđene šeme kontrolnog procesa, na osnovu kojih se formira: jasno, klasifikovano, nedvosmisleno, precizno, pouzdano, korektno, neopterećeno mišljenje (Senft & Gallegos, 2009). Forenzička revizija IT u sprečavanju pranja novca u Republici Srbiji, ima perspektivu. Nadležni regulatorni organ i supervizor Narodna banka Srbije u okviru svojih ovlašćenja data zakonom, sprovodi program kontinuiranog stručnog obrazovanja, osposobljavanja i usavršavanja zaposlenih, što će svakako za rezultat imati veliki doprinos u borbi protiv pranja novca.

Redovnim ažuriranjem liste indikatora za prepoznavanje sumnjivih transakcija za banke, i njenom implementacijom i prilagođavanjem u svojim softverima, banke se svakako približavaju svetskim normama u ovoj oblasti, budućnost je u standardizaciji i primeni jedinstvenog softvera od strane svih banaka.

CITIRANI RADOVI

BIS. (2014, 10 08). *Statistical release: OTC derivatives statistics at end-December 2013.* Retrieved from BIS: http://www.bis.org/statistics/derstats.htm

Bloomberg. (2014, 10 18). *Hungary Sizes Up Prostitution, Drugs, Boosting GDP.* Retrieved from Bloomberg: http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a89aBu5maiAU

Brand, K., & Boonen, H. (2010). *IT Governance based on Cobit 4.1 - A Management Guide.* Van Haren Publishing. Retrieved from http://www.vanharen.net/Samplefiles/9789087531164_it-governance-based-on-cobit-4.1-a-management-guide.pdf

CNBC. (2014, 10 12). *Dodd-Frank turns 3, but slew of rules are still unwritten.* Retrieved from CNBC: http://www.cnbc.com/id/100906282

Costa, A. M. (2014). *The checkmate Pendulum: From fiction to reality.* Amazon.

Čekerevac, P., & Čekerevac, Z. (2014, 03 11). *Bitcoin – prednosti i rizici.* Retrieved from FBIM Transactions: http://www.meste.org/fbim/fbim_srpski/FBIM_najava/V_Cekerevac.pdf

Čekerevac, Z. (2009). *Internet tehnologije i Internet poslovanje.* Kruševac: FIM ICIM+.

Dransfield, S. (2013, 05 22). *Lost tax haven cash enough to end extreme poverty - twice over.* Retrieved from Oxfam: http://www.oxfam.org.uk/blogs/2013/05/tax-haven-cash-enough-to-end-extreme-poverty

Đurđević, D. Ž. (2013). Primena informacione tehnologije u suzbijanju pranja novca. *Zbornik radova konferencije: Informaciona bezbednost 2013.* Beograd: Društvo za Informacionu Bezbednost Srbije (DIBS).

ECB. (2012, 10). *Virtual Currency Schemes.* Retrieved from European Central Bank: http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

FATF. (2010, 10). *Report: Money Laundering Using New Payment Methods.* Retrieved from FATF/OECD, Paris: http://www.fatf-gafi.org/media/fatf/documents/reports/ml%20using%20new%20payment%20methods.pdf

FINRA. (2014, 07 05). *Bitcoin: More than a Bit Risky.* Retrieved from Financial Industry Regulatory Authority (FINRA): http://www.finra.org/investors/protectyourself/investoralerts/fraudsandscams/p456458

GFI. (2013, 12). *Illicit financial flows from developing countries: 2002-2011.* Retrieved from Global Financial Integrity (GFI): http://iff.gfintegrity.org/iff2013/Illicit_Financial_Flows_from_Developing_Countries_2002-2011-HighRes.pdf

Hansen, K., Reuter, P., & Messick, R. (2014, 02 10). *Illicit Financial Flows from Developing Countries: Measuring OECD Responses.* Retrieved from OECD: http://www.oecd.org/corruption/Illicit_Financial_Flows_from_Developing_Countries.pdf

Henry, J. S. (2012, July). *The Price of Offshore Revisited: New estimates for "missing" global private wealth, income, inequality and lost taxes.* Retrieved from Tax justice network: http://www.taxjustice.net/cms/upload/pdf/Price_of_Offshore_Revisited_120722.pdf

HFR. (2014, 10 15). *Global Hedge Fund Industry Report: Second Quarter 2014.* Retrieved from Hedge Fund Research (HFR): https://www.hedgefundresearch.com/?fuse=products-irglo

Ljutić, B. Ž., & Polić, S. (2002). *Revizija informacione tehnologije, Most revizije i informacione tehnologije.* Beograd: Narodna banka Jugoslavije: Zavod za obračun i plaćanje.

Owojori, A. A., & Asaolu, O. (2009). The Role of Forensic Accounting in Solving the Vexed Problem of Corporate World. *European Journal of Scientific Research, 29*(2), 183.

Petrović, S. R. (2004). *Zaštita računarskih sistema.* Beograd: Beograd: Viša železnička škola.

Picard, J. (2013). Global Scale and Impact of Illicit Trade. In M. Miklaucic, & J. Brewer, *Convergence: Illicit Networks and National Security in the Age of Globalization* (pp. 52-57). Center for Complex Operations (U.S. Army, NDU).

Plunkett Research. (2014, 10 05). *Plunkett's Consulting Industry Almanac 2014.* Retrieved from Plunkett Research: http://www.plunkettresearch.com/consulting-market-research/industry-statistics

Preqin. (2014, 10 05). *2014 Global Private Equity Report.* Retrieved from Preqin: https://www.preqin.com/item/2014-preqin-global-private-equity-report/1/8194

Richard, A. (2013). *Insider dealing and money laundering in the EU: Law and regulation.* Farnam, UK: Ashgate Publishing.

Roosevelt Malloch, T., & Mamorsky, J. (2013). *The end of ethics and a way back: How to fix a fundamentally broken global financial system.* Singapur: Wiley.

RT. (2014, 02 06). *Bitcoins cannot be used in Russia - Prosecutor General's Office.* Retrieved from Russia Today: http://rt.com/business/bitcoin-russia-use-ban-942/

Senft, S., & Gallegos, F. (2009). *Information Technology Control and Audit* (Third ed.). Boca Raton, USA: Taylor & Francis Group LLC.

Stojanović, R. M., Petrović, R. S., & Stepanović, R. (2010). Značaj informacione tehnologije u bankarstvu na suzbijanju krivičnog dela prevare kao savremenog vida kriminala pod okriljem "legalnog" poslovanja. *Bezbednost, 52*(2), 81-96.

The World Bank. (2013, 05). *Mapping global gross capital flows through 2030* . Retrieved from The World bank: http://siteresources.worldbank.org/EXTDECPROSPECTS/Resources/476882-1368197310537/GrossKflowProjection_WP.pdf

The World Bank. (2014, 09 24). *World Development Indicators database.* Retrieved from The World Bank: http://data.worldbank.org/data-catalog/GDP-ranking-table

Unger, B. (2007). *The scale and impacts of money laundering, Edward Elgar Publishing, Čeltenam (UK) i.* Cheltenham, UK: Edward Elgar Publishing.

UNODC. (2011, 10). *Research report: Estimating the global proceeds of crime.* Retrieved from UN Office on Drugs and Crime (UNODC): https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf

Winters, J. (2011). *Oligarchy.* Cambridge: Cambridge University Press.

WSJ, T. W. (2004, 10 10). *The Libor Settlements, Retrieved from .* Retrieved from The Wall Street Journal: http://online.wsj.com/news/articles/SB10001424127887324616604578302321485831886

Datum prve prijave: 15.10.2014
Datum prijema korigovanog članka: 10.11.2014
Datum prihvatanja članka: 26.12.2014

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Đurđević Ž, D., & Stevanović D, M. (2015, Jan 15). Problemi sa kojima se suočava IT sektor u borbi protiv pranja novca u Srbiji. (Z. Čekerevac, Ed.) *FBIM Transactions, 3*(1), 174-187. doi:10.12709/fbim.03.03.01.20

*Style – **Chicago** Sixteenth Edition:*

Đurđević Ž, Dragan, and Miroslav Stevanović D. 2015. "Problemi sa kojima se suočava IT sektor u borbi protiv pranja novca u Srbiji." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 3 (1): 174-187. doi:10.12709/fbim.03.03.01.20.

*Style – **GOST** Name Sort:*

Đurđević Ž Dragan and Stevanović D Miroslav Problemi sa kojima se suočava IT sektor u borbi protiv pranja novca u Srbiji [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, Jan 15, 2015. - 1 : Vol. 3. - pp. 174-187.

*Style – **Harvard** Anglia:*

Đurđević Ž, D. & Stevanović D, M., 2015. Problemi sa kojima se suočava IT sektor u borbi protiv pranja novca u Srbiji. *FBIM Transactions,* 15 Jan, 3(1), pp. 174-187.

Style – **ISO 690** Numerical Reference:

Problemi sa kojima se suočava IT sektor u borbi protiv pranja novca u Srbiji. **Đurđević Ž, Dragan and Stevanović D, Miroslav.** [ed.] Zoran Čekerevac. 1, Beograd : MESTE, Jan 15, 2015, FBIM Transactions, Vol. 3, pp. 174-187.