Visoko sudsko i tužilačko vijeće Bosne i Hercegovine
Visoko sudbeno i tužilajsko vijeće Bosne i Hercegovine
Високи судски и тужилачки савјет Босне и Херцеговине
High Judicial and Prosecutorial Council of Bosnia and Herzegovina

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Agency for Development and Cooperation SDC

Cyber kriminal, pranje novca i finansijske istrage

PROJEKAT

Jačanje tužilačkih kapaciteta u sistemu krivičnog pravosuđa

PRIJEDLOG EDUKATIVNOG MODELA

CYBER CRIME, PRANJE NOVCA I FINANSIJSKE ISTRAGE

Autori

Miralem Porobić
Mirsad Bajraktarević

Sarajevo, februara 2012.godine

SADRŽAJ

1. CYBER CRIME, PRANJE NOVCA I FINANSIJSKE ISTRAGE 13

1.1. Uvod 13
1.2. Opis edukativnog modela 13
1.3. Ishod edukativnog modela 14
2. CYBER CRIME 15

2.1. Pojam i korištenje termina cyber kriminal 15
2.2. Karakteristike Cyber kriminala 15
2.3. Pojavni oblici cyber kriminala 16
2.3.1. Cyber kriminal u užem smislu 16
2.3.2. Cyber kriminal u širem smislu 16
2.4. Međunarodni akti i krivično materijalni i krivično procesni standardi za borbu sa cyber kriminalom 16
2.4.1. Konvencija o kibernetičkom/cyber kriminalu 16
2.4.1.1. Krivična djela protiv povjerljivosti, integriteta i disponibilnosti kompjuterskih podataka i sistema 17
2.4.1.1.1. Nedozvoljen pristup (član 2. Konvencije) 17
2.4.1.1.2. Nezakonito presretanje (član 3. Konvencije) 17
2.4.1.1.3. Povreda integriteta (ometanje) podataka (član 4. Konvencije) 17
2.4.1.1.4. Povreda integriteta (ometanje) sistema (član 5. Konvencije), ... 18
2.4.1.1.5. Zloupotreba uređaja (član 6 Konvencije) 18
2.4.1.2. Kompjuterska krivična djela 19
2.4.1.2.1. Kompjutersko falsificiranje/krivotvorenje(član 7.Konvencije) 19
2.4.1.2.2. Kompjuterska prevara/prevare koje su u vezi sa kompjuterom (član 8.Konvencije) 19
2.4.1.3. Krivična djela u vezi sadržaja 19
2.4.1.3.1. Krivična djela koja se odnose na dječiju pornografiju(član 9.Konvencije) 19
2.4.1.4. Krivična djela u vezi napada na intelektualnu svojinu i odnosna prava 20
2.4.1.4.1. Krivična djela koja se odnose na kršenje autorskih i njima sličnih prava(član 10. Konvencije) 20
2.4.2. Dodatni Protokol uz Konvenciju o kibernetičkom kriminalu o kriminalizaciji akta rasizma i ksenofobije počinjenih putem kompjuterskih sistema 20
2.4.2.1. Širenje rasnog i ksenofobnog materijala pomoću kompjuterskog sistema (član 3. Dodatnog protokola) 20
2.4.2.2. . Prijetnja motivirana rasizmom i ksenofobijom (član 4. Dodatnog protokola) 21
2.4.2.3. Uvreda motivirana rasizmom ili ksenofobijom (član 5 Dodatnog protokola) 21
2.4.2.4. . Poricanje, bitno umanjivanje, dobravanje ili opravdanje genocida ili zločina protiv čovječnosti (član 6.Dodatnog protokola) 21
2.4.3. Implementacija odredbi Konvencije o kibernetičkom/cyber kriminalu u bosanskohercegovačko krivično i krivično procesno pravo 22
2.4.3.1. Krivični zakoni 22

2.4.3.1.1. Komparacija odredaba krivičnih zakona Republike Srpske, Federacije Bosne i Hercegovine i Brčko Distrikta preko kojih su implementirane odredbe člana 2. do 9.Konvencije. 22
2.4.3.1.1.1. Oštečenje računarskih podataka i programa 23
2.4.3.1.1.2. Računarska sabotaža 24
2.4.3.1.1.3. Oštečenje računarskih podataka i programa 24
2.4.3.1.1.4. Računarska prevara 24
2.4.3.1.1.5. Neovlašteni pristup zaštičenom računaru,računarskoj mreži,telekomunikacionoj mreži (zaštičenom sistemu) i (mreži) elektronsk(e)oj obrad(e) i podataka 25
2.4.3.1.1.6. Spriječavanje i ograničavanje pristupa javnoj računarskoj mreži 25
2.4.3.1.1.7. Neovlašteno korištenje računara i računarske mreže 25
2.4.3.1.1.8. Računarsko krivotvorenje 26
2.4.3.1.1.9. Ometanje rada sistema i mreže elektronske obrade podataka 26
2.4.3.1.1.10. Krivična djela koja se odnose na dječiju prornografiju 26
2.4.3.1.1.11. Iplementacija krivičnih djela u vezi sa napadom na intelektualnu svojinu i odnosna prava 28
2.4.4. Implementacija odredaba Dodatnog Protokola uz Konvenciju o kibernetičkom kriminalu o kriminalizaciji akta rasizma i ksenofobije počinjenih putem kompjuterskih sistema 29
2.4.5. Primjena međunarodnih standarda koji su inaugurisani Konvencijom i Dodatnim protokolom u krivično-procesnom zakonodavstvu BiH, Federacije BiH, Republike Srpske i Brčko Distrikta BiH. 30
2.4.6. Šta su informacijske i komunikacijske tehnologije? 34
2.4.6.1. Hrdver (Hardware) 34
2.4.6.2. Softver (Software) 35
2.4.6.3. Računarska mreža 36
2.4.6.3.1. Osnovne komponente računarske mreže 36
2.4.6.3.2 .Mrežni standardi/Standardi računarskih mreža 37
2.4.6.4. Vrsta računarskih mreža 37
2.4.6.4.1. Vrsta računarske mreže prema kriteriju pokrivanja geografskog prostora 37
2.4.6.4.2. Vrsta računarski mreža prema kriteriju titulara vlasništva 38
2.4.6.4.3. Vrsta računarskih mreža prema kriteriju korištene tehnike prijenosa podataka 38
2.4.6.4. Standardizacija prijenosa podataka u računarskim mrežama 39
2.4.6.5. OSI referentni model 39
2.4.6.6. Komunikacijski protokoli 39
2.4.6.7. Uređaji za povezivanje mreža različitih arhitektura 39
2.4.6.7.1. Mrežni premosnik/most 40
2.4.6.7.2. .Mrežni usmjrenik 40
2.4.6.7.3. .Mrežni pristupnik/poveznik 40
2.4.6.8. Internet 40
2.4.7. Cyber kriminal i digitalni dokazi 42
2.4.8. Procedure i principi prikupljanja digitalnih dokaza 42
2.4.9. Integrisani model digitalne istrage 43
2.4.9.1. Forenzika 43

2.4.9.1.1. Digitalna forenzika 43
2.4.9.1.2. . Digitalni dokaz 44
2.4.9.2. Prijem i procesiranje forezničkog zahtijeva 44
2.4.9.3. Upravljanje istragom 45
2.4.9.3.1. Rukovanje i zadržavanje dokaza 45
2.4.9.3.2. Procesno ispitivanje 45
2.4.9.3.3. Razvijanje tehničkih procedura 45
2.4.9.3.4. Ispitivanje dokaza 46
2.4.9.3.4.1. Princip 46
2.4.9.3.4.2. Procedura 46
2.4.9.3.5. Proučavanje istražnog slučaja 46
2.4.9.3.6. Razmatranje lica mjesta 47
2.4.9.3.7. Procesuiranje istražnog mjesta 47
2.4.9.3.8. Pravne okolnosti 48
2.4.3.9. Ispitivanje dokaza 48
2.4.3.10. Pribavljanje dokaza 48
2.4.3.10.1. Princip 48
2.4.3.10.2. Procedure 48
2.4.3.11. Ispitivanje dokaza 51
2.4.3.11.1. Princip 51
2.4.3.11.2. Procedure 51
2.4.3.11.3. Korak 1 – Pripremanje 51
2.4.3.11.4. Korak 2 – Izdvajanje 51
2.4.3.12. Fizičko izdvajanje 52
2.4.3.13. Logičko izdvajanje 52
2.4.3.13.1. Korak 3 – Analiza i izdvajanje podataka 52
2.4.3.14. Vremenski raspon analize 52
2.4.3.15. Analiza skrivenih podataka 53
2.4.3.16. Analiza datoteka i aplikacija 53
2.4.3.17. . Vlasništvo i posjedovanje 54
2.4.3.17.1. Korak 4 – Zaključak 54
2.4.3.18. Dokumentovanje i izvještavanje 54
2.4.3.18.1. . Princip 54
2.4.3.18.2. Procedura 54
2.4.3.19. Istražiteljske bilješke 54
2.4.3.20. . Istražni izvještaj (Examiner's report) 55
2.4.3.21. Kratak pregled rezultata istrage 56
2.4.3.22. Detaljni rezultati istrage 56
2.4.3.23. Riječnik 56
2.4.3.24. Rukovanje digitalnim dokazima na licu mjesta 56

2.4.3.25. Elektronski uređaji-vrste opis potencijalnih dokaza 57
2.4.3.26. Računarski sistemi 57
2.4.3.26.1. Otvoreni i zatvoreni računarski sistemi 57
2.4.3.27. Uređaji za pohranjivanje podataka 58
2.4.3.28. Hard diskovi 58
2.4.3.29. Izmjenjivi mediji 59
2.4.3.30. Memorijski stikovi(Thumb drives/keychains/memory stick/flwsh drives) 59
2.4.3.31. Memorijske kartice 59
2.4.3.32. Ručni uređaj(Handheld devices) 60
2.4.3.32. Periferni uređaji 60
2.4.3.33. Ostali izvori potencijalnih digitalnih dokaza 61
2.4.3.34. Računarska mreža 61
2.4.3.35. Alati i oprema za istrage 62
2.4.3.35.1. Alati i materijali koji se koriste za prikupljanje digitalnih dokaza 62
2.4.3.36. Obezbjeđenje i ispitivanje lica mjesta 63
2.4.3.37. Preliminarni intervjui i ispitivanje 64
2.4.3.38. Dokumentovanje lica istražnog mjesta 65
2.4.3.39. Prikupljanje dokaza na licu istražnog mjesta 65
2.4.3.40. Računari ,komponente i ostali uređaji 66
2.4.3.41. Razmatranje situacije 66
2.4.3.42. Ako je kompjuterski sistem isključen 67
2.4.3.42.1.Prikupljanje digitalnih dokaza sa kompjuterskih sistema tipa desktop-a, tower-a, i mini računara 67
2.4.3.42.2. Prikupljanje digitalnih dokaza sa kompjuterskih sistema tipa laptopa, notebook-a ili netbook-a 68
2.4.3.43. Ako je kompjuterski sistem uključen 68
2.4.3.44. Dodatni dokazi u drugim obliku 69
2.4.3.45. Ostala elektronika i periferni uređaji kao potencijalni dokazi 69
2.4.3.46. Kompjuterski sistemi u poslovnom okruženju 70
2.4.3.47. Pakiranje,transport i skladištenje prikupljenih dokaza 70
2.4.3.48. Procedure pakiranja 71
2.4.3.49. Transportne procedure 71
2.4.3.50. Procedure skladištenja 72
2.4.3.51. Elektronski kriminal i kategorisanje digitalnih dokaza 72
2.4.3.51.1. Zloupotrebljavanje i iskorištavanje djece 73
2.4.3.51.2. Upadi u kompjuterski sistem 73
2.4.3.51.3. Falsifikovanje/krivotvorenje/Counterfeiting 74
2.4.3.51.4. Istraživanje ubistva 74
2.4.3.51.5. Porodično naselje, prijetnje i iznude/ucjene 74
2.4.3.51.6. Email prijetnje,uznemiravanje i praćenje 75
2.4.3.51.7. Kockanje/klađenje 75
2.4.3.51.8. Krađa identiteta 75

2.4.3.51.9. Narkotici 76
2.4.3.51.10. Online prevare ekonomske prirode 76
2.4.3.51.11. Prostitucija 77
2.4.3.51.12. Piratstvo softverom 77
2.4.3.51.13. Telekomunikacijske prevare 78
2.4.3.51.14. Terorizam 78
3. PRANJE NOVCA 79
3.1. Uvod 79
3.2. Pojam i karakteristike pranja novca 79
3.3. Faze pranja novca 80
3.3.1. Prva faza – plasman/polaganje (placement) 82
3.3.2. Druga faza – uslojavanja/pokrivanje (layering) 82
3.3.3. Treća faza- integracije/prožimanja (integration) 83
3.4. Slabe tačke u procesu pranja novca 84
3.5. Cyber kriminal i pranje novca 84
3.6. Elektronsko bankarstvo 84
3.6.1. Definicija i obuhvat elektronskog bankarstva 85
3.6.2. Podjela elektronskog bankarstva 85
3.6.3. Distributivna mreža elektronskog bankarstva 85
3.6.3.1. Pos terminali 86
3.6.3.2. Telefonsko (kućno) bankarstvo 86
3.6.3.3. SMS bankarstvo 86
3.6.3.4. Internet bankarstvo 86
3.6.3.4.1. Prednosti internet bankarstva 87
3.6.3.4.2. Nedostaci internet bankarstva 87
3.6.3.5. Bankomati 88
3.6.3.6. Zabrinutosti u vezi sa sprečavanjem pranja novca koje donosi cyber kriminal 88
3.6.4. Elektronsko bankarstvo u BiH 88
3.6.5. Elektronsko bankarstvo i pranje novca 90
3.7. Korespondentno bankarstvo 92
3.8. Elektronsko plaćanje 93
3.8.1. Notacijski/bezgotovinski sistem elektronskog plaćanja 93
3.8.1.1. E-ček 93
3.8.1.2. Kreditne kartice 93
3.8.1.3. Debitne kartice 94
3.8.1.4. Zloupotrebe kreditnih i debitnih kartica 95
3.8.1.5. Pametne/Smart kartice 95
3.8.2. Simbolički sistem elektronskog plaćanja 97
3.8.2.1. E-gotovina 97
3.8.2.2. Problemi u prenosu e-novčanica 98

3.8.2.3. Plaćanje e-gotovinom 98
3.8.2.3.1. On-line 98
3.8.2.3.2. Off-line 98
3.8.2.4. Nedostaci u plaćanju elektronskim novcem 99
3.8.2.5. Mikroplaćanje 99
3.8.2.6. Rizici pri korištenju elektronskog novca 99
3.8.2.7. Zakonski preduslovi za korištenje e-novca 99
3.8.2.8. Elektronski novac u praksi 100
3.8.2.9. Rizici u sistemu elektronskog plaćanja 100
3.8.3. Elektronski transfer sredstava i međubankarsko plaćanje 100
3.9. Međunarodni propisi i standardi kojim se regulira sprečavanje pranja novca 101
3.9.1. Konvencija Ujedinjenih naroda protiv nezakonitog prometa opojnih droga i psihotropnih tvari 101
3.9.2. Konvencija 141. Vijeća Europe o pranju, traganju, privremenom oduzimanju i oduzimanju prihoda stečenog krivičnim djelom (Strazburg 1990) 101
3.9.3. Konvencija Vijeća Europe o pranju, traganju, privremenom oduzimanju i oduzimanju prihoda stečenog krivičnim djelom te o finansiranju terorizma 102
3.9.4. Preporuke FATF-a 103
3.9.4.1. Preporuke vezane za sprječavanje pranja novca 103
3.9.4.2. Preporuke vezane za sprječavanje financiranja terorizma 105
3.9.5. Direktiva 91/308/EEC o sprječavanju korištenja financijskog sistema u svrhu pranja novca 106
3.9.6. Direktiva 2001/97/EC kojom se mijenja Direktiva 91/308/EEC 107
3.9.7. Direktiva 2005/60/EZ o sprječavanju korištenja financijskog sustava u svrhu pranja novca i financiranja terorizma 107
3.9.8. Direktiva 2006/70/EZ koja utvrđuje provedbene mjere za Direktivu 2005/60/EZ 109
3.9.9. Uredba br. 1889/2005 o kontroli ulaska i izlaska gotovine iz Zajednice 109
3.10. Cyber kriminal, nedobronamjerni programi namijenjeni cyber bankarstvu i pranje novca 110
3.10.1. Programi za praćenje unosa znakova s tipkovnice (eng. Keyloggers) 111
3.10.2. Trojanski konj 112
3.10.3. Otimanje autenticiranih sjednica /veza 112
3.10.4. Preuzimanje kontrole nad podacima u predlošcima (eng. form grabbing) 113
3.10.5. Pharming 113
3.10.6. Nedobronamjerni višefazni programi 113
3.10.7. Lažno predstavljanje 114
3.11. Trendovi cyber kriminala i pranja novca u 2012.godini 114
3.12. Novac mazga (money mule)/pranje novca 115
3.13. Cyber mafija 115
3.14. Mjere prevencije za sprečavanje krivičnog djela pranja novca 116
3.14.1. Procjena rizika 116
3.14.2. Identifikacija i praćenje klijenta 116
3.14.3. Ograničenja/zabrane u poslovanju sa klijentom kao mjera za sprečavanje pranja novca 117

3.14.4. Obavještavanje o sumnjivim transakcijama 117
3.14.5. Obaveze i zadaci lica koja obavljaju profesionalne djelatnosti u provođenju mjera za sprečavanje pranja novca 118
3.14.6. Uloga Finansijsko obavještajne jedinica u provođenju mjera sprečavanja pranja novca 118
3.14.7. Međunarodna suradnja 119
3.14.8. Kontrola prenosa gotovog novca preko državne granice 119
3.14.9. Interna kontrola, revizija i nadzor nad radom obveznika u vezi sa provođenjem mjera za sprečavanje pranja novca 120
3.14.10. Stručno obrazovanje,osposobljavanje i usavršavanje 121
Saradnja i koordinacija na unutrašnjem planu u sprovođenju mjera sprečavanja pranja novca 121
3.15 Krivično djelo pranja novca u međunarodnom pravu 122
3.16. Kriminalizacija pranja novca u BIH 123
3.17. Kriminalističke mjere i metodi otkrivanju, razjašnjavanju i dokazivanju krivičnog djela pranja novca 125
3.17.1. Otkrivanje krivičnog djela pranja novca 125
3.17.2. Kako se dolazio do saznanja da je izvršeno krivično djelo pranja novca 126
3.17.3. Razjašnjavanje i dokazivanje krivičnog djela pranja novca 127
3.18. Pranje novca I finansijske istrage 128
4. FINANSIJSKA ISTRAGA 129
4.1. Pojam i cilj finansijske istrage 129
4.2. Međunarodni akti kojim su uspostavljena načela i standardi za vođenje finansijskih istraga i oduzimanje, odnosno konfiskaciju imovine stečene kriminalom. 130
4.2.1. Konvencije UN protiv nezakonitog prometa opojnih droga i psihotropnih supstanci 130
4.2.2. Konvencija o pranju novca, istragama, zaplijeni i konfiskaciji dobiti od kriminala 130
4.2.3. Krivičnopravna konvencija o korupciji (Criminal Law Convention on Corruption, Strasbourg 1999),... 131
4.2.4. Međunarodna konvencija o suzbijanju finansiranja terorizma (International Convention for the Suppression of the Financing of Terrorism, New York 1999), ... 131
4.2.5. Konvencija UN protiv transnacionalnog organizovanog kriminala (UN Convention Against Transnational Organized Crime, Palermo 2000), ... 131
4.2.6 Konvencija UN protiv korupcije (United Nations Convention against Corruption, Merida 2003). 132
4.2.7. Plan aktivnosti Savjeta Europe: Sprječavanje i kontrola organizovanog kriminala: Strategija Evropske uniju za početak novog milenijuma 132
4.2.8. Konvenciji Savjeta Europe o pranju, otkrivanju, zaplijeni i konfiskaciji prinosa kažnjivih djela i finansiranja terorizma iz 2005. godine (Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, Warsaw, 2005), ... 132
4.2.9. Okvirna odluka Vijeća EU o konfiskaciji prihoda, sredstava i imovine povezane sa kriminalom (Council Framework Decision on Confiscation of Crime-Related Proceeds, Instrumentals and Property)14, ... 133
4.3. Zašto je potrebno provesti finansijske istrage 134
4.4. Koji su efekti oduzimanja nezakonito stečene imovine? 134
4.5. Oduzimanje imovinske koristi stečene krivičnim djelom 134
4.6. Prošireno oduzimanje imovinske koristi stečene krivičnim djelom 135

4.7. Način oduzimanja imovinske koristi pribavljene krivičnim djelom 136
4.8. Postupak oduzimanja imovinske koristi pribavljene krivičnim djelom 137
4.9. Kada treba početi sa finansijskom istragom? 138
4.10. Postupak provođenja finansijske istrage 139
4.10.1. Otkrivanje krivičnog djela i počinioca (krivične istrage) 140
4.10.2. Utvrđivanje prihoda/imovinske koristi stečenih krivičnim djelom (vrsta i iznos) 140
4.10.3. Ekonomske kategorije poslovnih događaja koje određuju finansijski položaj pojedinca 141
4.10.3.1.. Prihod odnosno neto prihod 142
4.10.3.2. Troškovi 142
4.10.3.3. Imovina 143
4.10.3.4. Obaveze 143
4.10.4. Metoda rekonstrukcije novčanog toka i neto vrijednosti 143
4.10.4.1. Rekonstrukcija novčanog toka 144
4.10.4.2. Rekonstrukcija neto vrijednosti/kapitala vlasnika 144
4.10.5. Metod dokazivanja na osnovu neto vrijednosti 145
4.10.6. Metod dokazivanja na osnovu troškova 149
4.11. Zakonski osnovi za primjenu metoda finansijske istrage u bosanskohercegovačkom zakonodavstvu 151
4.12. Intervju/uzimanje izjava kao podrška u vođenju finansijske istrage 151
4.12.1. Tehnika i taktika vođenje intervjua 153
4.13. Posebne istražne radnje kao podrška finansijskoj istrazi 154
4.13.1. Nadzora i tehničkog snimanja telekomunikacija 155
4.13.2. Pristup kompjuterskim sistemima i kompjutersko sravnjenje podataka 156
4.13.3. Nadzor i tehničko snimanje prostorija i tajno praćenje i tehničko snimanje osoba,transportnih sredstava i predmeta koji stoje u vezi sa njima 157
4.13.4. Korištenje prikrivene istražitelja , korištenje informator , simulirani i kontrolirani otkup predmeta i simulirano davanje potkupnine 157
4.13.5. Posebnih istražnih radnji nadzirani prijevoz i isporuka predmeta krivičnog djela 158
4.14. Kako tumačiti i koristiti rezultate finansijske istrage 159
4.15. Modeli međunarodna suradnja u postupcima oduzimanja prihoda/imovine stečenih krivičnim djelima . 159
4.15.1. Pomoć u istrazi 160
4.15.2. Zajedničke istrage i primjena posebnih istražnih 160
4.15.3. Sprovođenje privremenih mjera zamrzavanja odnosno privremenog oduzimanja prihoda stečenih kriminalom 161
4.15.4. Realizacija pomoći u oduzimanju, vraćanju ili razmijeni prihoda stečenih kriminalom 161
4.16. Međunarodne organizacije putem kojih se podstiče implementacija mehanizama za oduzimanje prihoda stečenih kriminalom 162
4.16.1. INTERPOL 162
4.16.2. GRECO 163
4.16.3. Radna grupa za finansijske akcije (FATF) 163
4.16.4. EGMONT GRUPA 164

4.16.5. MONEYVAL 164
4.16.6. CARDS 165
4.17 Institucije koje generišu posjeduju I čuvaju dokumentaciju, evidenciju , poslovne knjige, finansijske izvještaje i drugu dokumentaciju o prihodim, rashodima/troškovima, imovini i sredstvima i obavezama pravnih i fizičkih lica 165
4.17.1. Centralna banka Bosne i Hercegovine 166
4.17.2. Državna agencija za istrage i zaštitu, Finansijsko obavještajni odjel, ... 166
4.17.3. Uprava za indirektno oporezivanje Bosne I Hercegovine 167
4.17.4. Agenciju za identifikacijske isprave, evidenciju i razmjenu podataka BiH. 167
4.17.5. Porezna/Poreske uprave Federacije Bosne I Hercegovine i Republike Srpske 167
4.17.6. Komisija za hartije od vrijednosnih RS, Komisija za vrijednosne papire F BIH i Zakon o tržištu hartija od vrijednosti BD BiH 168
4.17.7. Sarajevska i Banjalučka Berze 168
4.17.8. Registar vrijednosnih papira u Federaciji BiH 169
4.17.9. Centralni registar Hartija od vrijednosti RS 169
4.17.10. Agencije za informatičke i posredničke usluge F BiH(Sarajevo i Mostar) 170
4.17.11. Agencija za posredničke, informatičke i finansijske usluge Banja Luka 171
4.17.12. Javna i privatna preduzeća/društva za distribuciju električne energije, ptt usluga, RTV pretplate, usluge mobilne telefonije, zemnog gasa, vode i kanalizacije te usluge odvoza smeća i održavanje zajedničkih dijelova zgrada 171
4.17.13. Fond za penzijsko invalidsko osiguranje Republike srpske Federalni zavod za penzijsko/mirovinsko invalidsko osiguranje 171
4.17.14. Fond zdravstvenog osiguranja Brčko Distrikta Bosne i Hercegovine 172
4.17.15. Zavod zdravstvenog osiguranja i reosiguranja Federacije Bosne i Hercegovine i Zavodi zdravstvenog osiguranja u Kantonima 172
4.17.16. Fond zdravstvenog osiguranja Republike Srpske 173
4.17.17. Agencija za rad i zapošljavanje BiH, Zavod za zapošljavanje F BiH, Javna ustanova Zavod za zapošljavanje RS, Zavod za zapošljavanje Brčko Distrikta BiH 173
4.17.18. Općinski organi/Uredi za katastar/Javni registar 174
4.17.19. Sudovi nadležni za upis pravnih lica u registar 174
4.17.20. Općinski/osnovni sudovi-Zemljišne knjige 175
4.17.21. BH Direkcija civilne avijacija 175
4.17.22. Kapetanije za unutrašnju i Kapetanije za pomorsku plovidbu 176
4.17.23. Banke 176
4.17.24. Mikrokreditne organizacije 176
4.17.25. Lizing društva 177
4.17.26. Agencije za bankarstvo F BiH I RS 177
4.17.27. Investiciono-razvojna banka Republike Srpske 178
4.17.28. Razvojna banka Federacije BiH 178
4.17.29. Agencija za osiguranje depozita BiH 178

4.17.30. Društva za osiguranje 179
4.17.31. Agencija za osiguranje u BIH , Agencija za nadzor osiguravajućih društva u F BIH i RS 179
4.17.32. Notari 180
4.17.33. Poslovni subjekti (preduzeća ili privredna društva) 180
4.17.34. Udruženja i fondacija 181
4.17.35. Ministarstvo unutrašnjih poslova Republike Srpske, Kantonalna ministarstva unutrašnjih poslova i Javni registar Brčko Distrikta. 182
4.18. Sistem računovodsve i knjijigovodstva a u BIH 182
4.18.1. Obveznici primjene zakona 184
4.18.2. Razvrstavanje pravnih lica 185
4.18.3. Sistem računovodstva i knjigovodstva 186
4.18.3.1. Knjigovodstvene isprave 187
4.18.3.2. Poslovne knjige 187
4.18.3.2.1. Vođenje poslovnih knjiga 189
4.18.3.3. Kontni okvir 189
4.18.3.4. Popis imovine i obaveza 190
4.18.3.5. Obračun amortizacije 191
4.18.3.6. Usaglašavanje potraživanja i obaveza 191
4.18.3.7. Zaključivanje poslovnih knjiga i utvrđivanje finansijskog rezultata 191
4.18.3.8. Način i rokovi čuvanja knjigovodstvene dokumentacije 192
4.18.3.9. Finansijsko izvještavanje 193
4.18.3.10. Godišnji izvještaj o poslovanju 195
4.18.3.11. Konsolidirani finansijski izvještaj 195
4.18.3.12. Predaja polugodišnjih i godišnjih finansijskih izvještaja 196
4.18.3.13. Nadzor 197
4.18.3.14. Revizija finansijskih izvještaja 198
4.18.3.14.1. Obveznici revizije 198
4.19. Poslovne knjige i evidencije za obavljanje samostalne djelatnosti 199
5. LITERATURA 201
5.1. Osnovna literatura 201
5.2. Naučni radovi 201
5.3. Objavljeni članci 201
5.4. Presude Suda BiH 202
5.5. Priručnici 202
5.6. web stranice 203
5.7. Pomočni linkovi i informacije 204

1. CYBER CRIME, PRANJE NOVCA I FINANSIJSKE ISTRAGE

1.1. Uvod

Informatičko-komunikacijska revolucija i širenje globalne svjetske računarske mreže-Interneta sa sobom su donijeli nove oblike društveno neprihvatljivog ponašanja koje je trebalo na adekvatan način kriminalizirati. Pokazalo se, međutim, kako nacionalna zakonodavstva više nisu dostatna za efikasno reguliranje sve većeg broja novih društvenih odnosa koji traže pravnu regulaciju. Iz istorijske vizure posmatrajući savremeno društvo odlikuju brojne specifičnosti i ozbiljni problemi koji uglavnom imaju globalnu dimenziju za razliku od modernog društva čije je bitno obilježje bilo nacionalno. Historijski je potvrđeno da niti jedan normativni sistem nije uspio do kraja obuhvatiti sve relevatne društvene odnose.

Globalne računarske mreže stvorile su mogućnosti za nove oblike kriminala. Pojavljuje se "poseban, sufisticiran, prodoran, tehnički potkovan, beskrupulozan, opsjednut, ponekad osvetoljubiv pojedinac kome je teško suprotstaviti se, a još teže zaustaviti ga". On sve češće ne želi da bude sam već mu je potrebno društvo, kao što mu je neophodna i "publika". Lakoća "vršljanja" cyber prostorom daje mu osećaj moći i neuhvatljivosti. Ovi osećaji nisu bez razloga, jer stvarno ga je izuzetno teško otkriti u momentu činjenja djela, što, uglavnom, predstavlja i "pravi" trenutak za njegovo identifikovanje i hvatanje. S druge strane, Internet koji je toliko ranjiv i nesiguran zbog ogromnog broja korisnika, otvorenosti i neregulisanosti je i idealno skrovište kriminalaca različitog tipa.U takvom okruženju i sa takvim pojedincima sve se češće pokušavaju izboriti ne samo mnoga nacionalna prava, međunarodne organizacije i asocijacije, već se uključuje i "privatni sektor" i korisnici ne bi li se ublažile negativne posljedice i smanjili gubici koji nastaju zbog kriminalnih aktivnosti.

Tradicionalne kriminalne grupe i organizacije modernizuju se korišćenjem ICT, a *cyber prostor* postaje sredina u kojoj deluju i koja im istovremeno služi kao skrovište. Ono postaje i okruženje u kome nastaje poseban tip kriminala – *cyber kriminal.*

1.2. Opis edukativnog modela

Svjesni činjenice da se društva u cijelom svijetu sve više oslanjaju na informacijske i komunikacijske tehnologije i sve veće ovisnosti društava o njima i kao takvo postaje podložno prijetnjama kao što je *cyber kriminal*. Zbog svega toga sudije, tužioci i pripadnici agrencija za sprovođenje zakona moraju biti spremni da se efikasno i efektivno bave *cyber kriminalom* i dokazima u elektronskoj formi.

Edukativni model „Cyber crime, pranje novca i finansijske istrage" namjenjen je edukatorima odnosno tužiocima i pripadnicima agencija za sprovođenje zakona u Bosni i Hercegovini i ima za cilj da kroz popularnu formu i sadržaj na pristupačan i interaktivan način svom budućim učesnicima edukacije pruži adekvatna temeljna znanja o *cyber crime*, digitalnim dokazima kao i pranju novca kao posljedici *cyber crime* i finansijskim istragama kao najmočnijem alatu za bornu protiv svih vrsta krivičnih dijela koja su imovinski motivisana.

U realnom okruženju danas ne postoji ICT sistem koji je apsolutno siguran i otporan na cyber aktivnosti, bilo da su u pitanju napadi sa Interneta, uključujući brojne maliciozne programe ili se radi o napadu ljudskog faktora, poput hakera, krakera, vandala , cyber terorisa ili cyber mafije. Sadržajem ovog edukativnog modela nastoji se u svjetlu međunarodnih

standarda razjasniti u toriji i praksi uveliko rasprostranjen pojam cyber crime, predstaviti njegove osnovne karakteristike, identificirane pojavne oblike, lokalnu i globalnu opasnost i predstaviti neke od modaliteta uspješnog suprostavljanja istom. Posebna pažnja je posvećena je procesnom pitanju sticanje, čuvanja , upotrebe i dokazivanja preko digitalnih dokaza, osobito s obzirom na međunarodne trendove u tom smislu.U okviru edukativnog modela u kontekstu elektronskog poslovanja, cyber kriminala i pranja novca i međunarodnih standarda podcrtan je značaj finansijske istragae kao najznačajnijeg i najefikasnijeg alata za oduzimanje nezakonito stečene imovine I predstavljeni neki od metoda za efikasno vođenje finansijske istrage.

1.3. Ishod edukativnog modela

Nakon implementacije ovog edukativnog modela očekuje se da tužioci i pripadnici agencije za provođenje zakona na fonu opredjeljenja sadržanih u dokumentu radne grupe u okviru Projekta o kibernetičkom kriminalu i Lisabosnke mreže institucija za edukaciju sudija i tužilaca Vijeća Europe, steknu osnovna znanja o pitanjima vezanim za cyber kriminala i elektronske dokaze koja uključuju, ali se ne ograničavaju na:

- ✓ kompjutere i mreže: način njihovog funkcioniranja, osnovne pojmove rada Interneta, uloge dobavljača internet usluga;
- ✓ Cyber crime: način na koji se informacijske i komunikacijske tehnologije koriste za izvršenje krivičnih djela;
- ✓ Međunarodni standardi i domači zakoni (uključujući i sudsku praksu);
- ✓ Integrisanin model digitalne forenzičke nistrage,
- ✓ Stvarna i mjesna nadležnost;
- ✓ Elektronski dokazi: pojam, tehničke procedure i zakonska pitanja,
- ✓ Međunarodna suradnja[1].

Nakon implementacije ovog modela tužioci i pripadnici agencija za sprovođenje zakona bi trebakli da mogu:

- ✓ Otkriti krivična djela i počinioce ciber kriminala;
- ✓ Povezati kriminalnu radnju sa odredbama domačeg zakona;
- ✓ Odobriti, planirati, voditi i usmjeravati istražne radnje;
- ✓ Narediti, nadzirati i usmjeravati pretres i oduzimanje kompjuterskih sistema i elektronskih dokaza;
- ✓ Realizirati međuagencijsku i međunarodnu suradnju;
- ✓ Ispitati osumnjičene, svjedoke i vještake;
- ✓ Prikupiti, čuvati i prezentirati elektronske dokaze[2],
- ✓ Otkriti ,razjasniti i dokumentovati krivično djelo pranja novca počinjeno uz podršku IKT,
- ✓ Efikasno i efektivno provesti finansijsku istragu paralelnu sa krivičnom istragom,
- ✓ Utvrditi i privremeno oduzeti ili zaplijeniti imovinu za koju se osnovano sumnja da je stečena krivičnim djelom.

[1] Vidi Dokument za edukaciju sudija i tužilaca Vijeća Europe koji je sačinila Radne grupe u okviru Projekta o kibernetičkom kriminalu i Lisabonske mreže,Strazbur,2008.godine strana 12.
[2] Vidi Dokument za edukaciju sudija i tužilaca Vijeća Europe koji je sačinila Radne grupe u okviru Projekta o kibernetičkom kriminalu i Lisabonske mreže,Strazbur,2008.godine strana 12.

2. CYBER CRIME

2.1. Pojam i korištenje termina cyber kriminal

Najpotpunija definicija cyber kriminala data je u dokumentu „Kriminal vezan za kompjutersku mrežu“ (Report of Committee II, Workshop on crimes related to the computer network) sa Desetog Kongresa Ujedinjenih Nacija, posvećenog prevenciji kriminala i tretmanu počinilaca koji je održan u Beču od 10 do 17. aprila 2000. godine (Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, Wienna, 10-17 April 2000. godine). Radna grupa eksperata u sadržaju izvještaja pod cyber kriminalom podrazumjeva „kriminal koji se odnosi na bilo koji oblik kriminala koji se može izvršavati sa kompjuterskim sistemom i mrežama, u kompjuterskim sistemima i mrežama ili protiv kompjuterskih sistema i mreža“. To je kriminal koji se odvija u elektronskom okruženju. Ako se pod kompjuterskim sistemom podrazumjeva „svaki uređaj ili skup međusobno povezanih uređaja, kojim osigurava ili čiji jedan ili više elemenata osiguravaju, prilikom izvršenja nekog programa, automatiziranu obradu podataka[3]“ onda je očigledno da bez kompjuterskih sistema i kompjuterskih mreža nema ni cyber kriminala. Pojam cyber kriminala je kompleksan i zbog čega ga mnogi smatraju tzv “kišobran terminom“ koji „pokriva“ raznovrsne kriminalne aktivnosti uključujući napade na kompjuterske podatke i sisteme, napade vezane za računare, sadržaje ili intelektualnu svojinu.

Pravni osnov za postupanje u ovoj oblasti je ustanovljen usvajenjem Convention on Cybercrime (usvojena u Budimpešti 23.11.2001.g.) koji je preveden kao Konvencija o visokotehnološkom kriminalu ili kao Konvencije o kibernetičkom kriminalu. Ne želeći se upuštati u jezičko tumačenje značenja riječi „kibernetika“, niti to upoređivati sa značenjem riječi „cyber“, u ovom tekstu će se uglavnom koristiti termini „cyber kriminal“ i „cyber krivična djela“.

Takođe u okviru edukacije po ovom edukativnom modulu treba istači da pod pojmom cyber krivičnih djela treba svrstati samo krivična djela kod kojih je upotreba kompjutera/računala odnosno kompjuterskog sistema ili kompjuterske mreže bitna za biće krivičnog djela, a ne sva krivična djela u kojima se na neki način kao sredstvo izvršenja pojavljuje kompjuter/računalo sa pripadajućom perifernom opremom.

Kao ilustraciju navedene tvrdnje krivično djelo „krivotvorenje novca“ nije cyber krivično djelo bez obzira da li se počinitelj prilikom krivotvorenja novca služio kompjuterom/računalom. Biće krivičnog djela krivotvorenje novca [4] je izrada lažnog novca ili preinačenje pravog novca s ciljem da ga stavi u opticaj, a kompjuter/računalo uključujući skener i štampač se tu pojavljuju kao tehnička sredstva za lakše počinjenje krivičnog djela.

2.2. Karakteristike Cyber kriminala

Imajući sve to u vidu može se konstatovati da je cyber kriminal takav oblik kriminalnog ponašanja kod koga je cyber prostor okruženje u kome se kompjuterske mreže pojavljuju kao cilj, sredstvo/alat, dokaz i okruženje izvršenja krivičnog djela. Pri tome se pod cyber prostorom podrazumjeva :

---

[3] Vidi Konvenciju o cybercrime Vijeća Europe od 23.novembra 2011.godine („Službeni glasnik BiH“,broj 06/06 Međunarodni ugovori), Član 1. stav 1.pod a).-Definicije

[4] Vidi Krivičnog zakona BiH,član 205

- Vrsta "zajednice" sačinjene od mreže kompjutera u kojoj se elementi tradicionalnog društva nalaze u obliku bajtova[5] i bitova[6], ili
- „Prostor" koji kreiraju kompjuterske mreže.

2.3. Pojavni oblici cyber kriminala

Različiti dokumenti na različite načine klasifikuju pojavne oblike cyber kriminala. Tako se u dokumentu „Kriminal vezan za kompjutersku mrežu" („Report of Committee II, Workshop on Crimes Related to the Computer Network") sa Desetog Kongresa Ujedinjenih nacija posvećenog prevenciji kriminala i tretmanu počinilaca, navodi da postoje dvije sub kategorije cyber kriminala i to:

2.3.1. Cyber kriminal u užem smislu

podrazumjeva svako nezakonito ponašanje usmjereno na elektronske operacije protiv sigurnosti kompjuterskih sistema i podataka koji se njima obrađuju;

2.3.2. Cyber kriminal u širem smislu

podrazumjeva svako nezakonito ponašanje vezano za ili u odnosu na kompjuterski sistem i mrežu, uključujući i takav kriminal kakvo je nezakonito posjedovanje, nuđenje i distribuiranje informacija preko kompjuterskih sistema i mreža.

2.4. Međunarodni akti i krivično materijalni i krivično procesni standardi za borbu sa cyber kriminalom

S obzirom na činjenicu da su globalne računarske mreže kreirale brojne mogućnosti za pojavu novih oblika kriminala i profila njegovih izvršilaca.Pojedinci i grupe koristeći brojnost korisnika globalnih mreža i njihovu otvorenost i neregulisanost gotovo nesmetano djeluju u cyber prostoru čineči brojna krivična djela sa brojnim negativim posljedicama i ogromnim materijalnim gubicima.Praksa je pokazala da je cyber kriminal veoma teško otkriti u momentu njegovog činjenja pogotovosa pravnim alatima koje daju nacionalna zakonodavstva. I pored toga što je pred međunarodnom zajednicom dugi niz godina bili aktuelni ogromni izazazovi i pritetnje koje sa sobom nosi cyber kriminal ona je tek nakon niz godina uz brojne kompromise napokon usaglasila sadržaj svojesvrsnog multilateralnog sporazuma koji je posebno usmjeren na probleme cyber kriminala i isti je uobličen u Konvenciju o cyber kriminalu.

2.4.1. Konvencija o kibernetičkom/cyber kriminalu

Konvenciju o kibernetičkom kriminalu donijelo je Vijeće Europe[7] 23. novembra 2001.godine, a Bosna i Hercegovina je istu ratificirala 25. marta 2006. godine[8]. Konvencija o kibernetičkom kriminalu predstavlja oblik međunarodnog ugovora kojim su države članice

---

[5] Bajt (eng.byte) je jedinica informacije sastavljena od osam bitova (npr.10110010). Suvremeni kompjuteri rade s podacima od 8, 16 ,32 i 64 bita. Najčešće se koriste veće jedinice: Kilobajt (KB) =1024 Bajta; Megabajt (MB)=1048576 Bajta; Gigabajt (GB)=1073741824 Bajta i Terabajt (TB)=1099511627776 Bajta.

[6] Bit je kombinacija engleskih riječi binary digit, što u prijevodu znači binarnim broj (0 ili 1). Bit je temeljna jedinica za informaciju, a fizički je predstavljena jednim impulsom poslanim kroz elektronski sklop ili tačkom na magnetskom disku.

[7] Viječe Europe osnovano je 1949. godine s ciljem uspostavljanja uskih veza među državama članicama,ostvarivanja načela koja su njihova zajednička baština i unapređivanja njihovog privrednog i socijalnog napretka. Vijeće Europe ne donosi propise koji su neposredno obavezujući u državama članicama, već samo priprema ugovore koje države članice trebaju ratificirat.

[8] Vidi „Službeni Glasnik Bosne i Hercegovine-Međunarodni ugovori ", broj 06/06

Vijeća Europe[9] i ostale države potpisnice uobličile zajednički odgovor na razvoj novih kompjuterskih tehnologija, zasnovan na vrijednostima Vijeća Europe. Ova Konvencija spada u krug takozvanih okvirnih konvencija s obzirom na činjenicu da njene odredbe nisu direktno primjenjive, tako da bi ih svaka država trebala implementirati u nacionalno zakonodavstvo.

Zbog svoje specifičnosti i vremena donošenja, važno je napomenuti da je Savjet evropske zajednice još 1991. godine donio Direktivu o zaštiti kompjuterskih programa[10] u kojoj su date osnovne postavke zaštite kompjuterskih programa.

Konvencija o cyber kriminalu predvidjela je četiri grupe krivičnih djela:

2.4.1.1. Krivična djela protiv povjerljivosti, integriteta i disponibilnosti kompjuterskih podataka i sistema

2.4.1.1.1. Nedozvoljen pristup (član 2. Konvencije)

Po pitanju inkriminiranja ponašanja iz člana 2. Konvencije od država članica/ potpisnica se traži da usvoje takve legislativne i ostale neophodne mjere da bi se sankcioniralo namjerno bespravno pristupanje kompjuterskim sistemima kao cjelini ili nekom njegovom djelu. Sadržajem odredbe ovog člana se članicama daje mogućnost da uslove da djelo mora biti učinjeno kršenjem sigurnosnih mjera sa namjerom pribavljanja kompjuterskih podataka ili sa nekom drugom nečasnom namjerom ili učinjeno u vezi sa kompjuterskim sistemom koji je povezan sa drugim kompjuterskim sistemom.

2.4.1.1.2. Nezakonito presretanje (član 3. Konvencije)

U pitanje inkriminacije ponašanja iz člana 3. Konvencije - nezakonito presretanje, od država članica i potpisnica se traži da usvoji takve legislativne i ostale neophodne mjere, da bi se u njenom nacionalnom pravu, kao krivično djelo okvalifikovalo bespravno presretanje prenosa kompjuterskih podataka koji nisu javne prirode, ka kompjuterskom sistemu, od njega ili unutar sistema, u što spada i elektromagnetna emisija iz kompjuterskih sistema kojom se prenose takvi podaci, a kada je učinjena sa namjerom i uz pomoć tehničkih uređaja. Članicama odnosno potpisnicima se daje mogućnost da propišu uslov da krivično djelo nezakonitog presretanja mora biti učinjeno sa nečasnim namjerama ili učinjeno u vezi sa kompjuterskim sistemom koji je povezan sa drugim kompjuterskim sistemom.

Također trebalo bi razmotriti opravdanost uvođenja kvalifikovanog oblika krivičnog djela nezakonitog presretanja kada je objekt radnje kompjuterski podatak, program ili sistem tjela državne vlasti, javne ustanove ili privredna društva od posebnog javnog interesa ili je prouzrokovana znatna šteta, a što opravdano treba da predviđa i težu propisanu kaznu.

2.4.1.1.3. Povreda integriteta (ometanje) podataka (član 4. Konvencije)

Sadržajem odredaba ovog člana obavezuju se članice odnosno potpisnice Konvencije da usvoje takve zakonske i druge neophodne mjere da bi se utemeljilo kao krivično djelo

[9] "Međunarodni ugovor se sastoji u saglasnosti dvaju ili više subjekata međunarodnog prava s ciljem da se postigne određeni učinak po međunarodnom pravu, stvarajući odnos prava i dužnosti između njegovih stranaka" - Degan, Vladimir-Đuro: Međunarodno Pravo, Rijeka, 2000., str.121.

[10] Orginalan naziv: Council Directive of 14. May 1991 on the Legal Protection of Computer Programs.

učinjeno sa namjerom bespravnog oštećenja, brisanje, kvarenje, mijenjanje ili prikrivanje i poništavanje kompjuterskih podataka. Drugim stavom istog člana Konvencije data je mogućnost potpisnicama da mogu usloviti da krivična djela iz stava 1. uzrokuju značajne štete.

2.4.1.1.4. Povreda integriteta (ometanje) sistema (član 5. Konvencije),

Odredbama ovog člana svaka članica odnosno potpisnica treba da usvoje zakonodavne i druge neophodne mjere da bi se u nacionalnom krivičnom pravu, kao krivično djelo, kvalifikovalo bespravno i u većem stepenu ometanje funkcionisanja kompjuterskih sistema putem unošenja, prenošenja, oštećenja, brisanja, kvarenja ili prikrivanja kompjuterskih podataka, ukoliko je učinjeno sa namjerom.

2.4.1.1.5. Zloupotreba uređaja (član 6 Konvencije)

Temeljem odredaba člana 6. Konvencije svaka članica odnosno potpisnica treba da usvoji legislativne i ostale neophodne mjere da bi se u njenom nacionalnom pravu kao krivično djelo,ukoliko je učinjeno sa namjerom i bespravno, okvalifikovalo slijedeće:

a. Proizvodnja, prodaja, nabavka radi upotrebe, uvoz, distribucija i drugi vidovi stavljanja na raspolaganje:

   - Sredstava, što podrazumjeva i kompjuterske programe, projektovane ili preuređene prvenstveno u svrhu izvršenja nekog od krivičnih djela iz člana 2-5. Konvencije.
   - Kompjuterskih lozinki, šifri za pristup, ili sličnih podataka putem kojih se može pristupiti kompjuterskom sistemu kao cjelini ili nekom od njegovih dijelova sa namjerom da bude upotrijebljen u svrhu izvršenja nekog od krivičnih djela navedenih u članovima 2-5, i

b. Posredovanje neke od stvari navedenih u stavovima pod a. prva ili druga alineja s namjerom da se upotrijebi u svrhu izvršenja nekog od krivičnih djela navedenih u članovima 2-5. Članice odnosno potpisnice Konvencije mogu kroz nacionalne zakone usloviti da se mora posjedovati određen broj pomenutih stvari da bi postojala krivična odgovornost.

c. Ovaj član se ne može interpretirati kao onaj koji nameće krivičnu odgovornost u slučaju kada proizvodnja, prodaja, dobijanje na korištenje, uvoz, distribucija ili drugi oblici stavljanja na raspolaganje citirani u paragrafu 1. člana 6. Konvencije nemaju za cilj činjenje prekršaja kako je to ustanovljeno shodno članovima 2 do 5. Konvencije, kao u slučaju ovlaštenih pokušaja ili zaštite kompjuterskog sistema.

Ostavljena je i mogućnost svakoj strani da ne primjenjuje paragraf 1 člana 6.Konvencije pod uslovom da se to ograničenje ne odnosi na prodaju, distribuciju ili svako drugo stavljanje na raspolaganje stvari citiranih u paragrafu 1(a) i (2).

2.4.1.2. Kompjuterska krivična djela

2.4.1.2.1. Kompjutersko falsificiranje/krivotvorenje(član 7.Konvencije)

Svakoj strani odnosno potpisnici se, u skladu sa sadržajem odredbama člana 7., daje mogućnost da usvoji zakonske i druge mjere za koje se ukaže potreba kako bi utemeljile kao krivično djelo, shodno internom pravu, unošenje, izmjena, brisanje ili ukidanje, namjerno i bespravno, kompjuterskih podataka, proizvodeći neautentične podatke, u namjeri da oni budu uzeti u obzir ili korišteni u legalne svrhe kao da su autentični, pa bili oni ili ne čitki i nerazumljivi. Potpisnicima se daje mogućnost da u nacionalnom pravu uslove da postoji namjera prevare ili slična nečasna namjeru da bi se ustanovila krivična odgovornost.

2.4.1.2.2. Kompjuterska prevara/prevare koje su u vezi sa kompjuterom (član 8.Konvencije)

Odredbom člana 8. Konvencije obavezuju se potpisnici Konvencije da usvoje legislativne i ostale, neophodne mjere, da bi se u njihovom nacionalnom pravu, kao krivično djelo, okvalifikovalo nanošenje imovinske štete drugim licima, kada se to učini bespravno i sa namjerom na slijedeći način:

- Bilo kakvim unošenjem, mijenjanjem, brisanjem ili prikrivanjem kompjuterskih podataka,
- Bilo kakvim ometanjem funkcionisanja kompjuterskih sistema,

sa namjerom prevare ili drugom nečasnom namjerom da se bespravno pribavi ekonomska dobit za sebe ili za druga lica

2.4.1.3. Krivična djela u vezi sadržaja

2.4.1.3.1. Krivična djela koja se odnose na dječiju pornografiju(član 9.Konvencije)

Odredbama člana 9.Konvencije se obavezuju potpisnici da usvoje, legislativne i druge neophodne, mjere, da bi se u njenom nacionalnom pravu, kao krivično djelo, okvalifikovale slijedeće radnje, ako se učine namjerno i bespravno:

(1) Proizvodnja dječije pornografije u cilju njene distribucije preko kompjuterskih sistema;
(2) Nuđenje ili stavljanje na raspolaganje dječije pornografije preko kompjuterskih sistema;
(3) Distribucija ili prenošenje dječije pornografije preko kompjuterskih sistema;
(4) Pribavljanje dječije pornografije preko kompjuterskog sistema za sebe ili za druga lica;
(5) Posjedovanje dječije pornografije u kompjuterskom sistemu ili na medijima za smještanje kompjuterskih podataka;

Uz napomenu da izraz „dječija pornografija“ u smislu stava 1. obuhvata pornografski materijal koji vizuelno prikazuje:

(a) Maloljetnike koji učestvuju u eksplicitnom seksualnom činu;
(b) Lice po čijem izgledu se može zaključiti da je maloljetnik, koje učestvuje u seksualnom činu;
(c) Realističke slike koje predstavljaju maloljetnika koji učestvuje u eksplicitnom seksualnom činu;

Izraz „maloljetnik“ iz stava 2. obuhvata sva lica mlađa od 18.godina, a potpisnici mogu postaviti nižu starosnu granicu, koja ne smije biti manja od napunjenih 16 godina. Pored navedenog data je mogućnost potpisnicima da ne primjenjuju u cjelini ili djelimično stavove 1(d), 1(c), 2(b) i 2(c).

2.4.1.4. Krivična djela u vezi napada na intelektualnu svojinu i odnosna prava

2.4.1.4.1. Krivična djela koja se odnose na kršenje autorskih i njima sličnih prava(član 10. Konvencije)

Sadržajem odredaba člana 10. Konvencije svaka potpisnica je obavezna da usvoji takve legislativne i ostale neophodne mjere, da bi se u njenom nacionalnom pravu, kao krivično djelo, okvalifikovalo kršenje autorskih prava definisanih u zakonima te članice koji se odnose na obaveze koje je ona preuzela po Praškom aktu od 24. Juna 1971. godine, Konvenciji iz Berna o zaštiti literarnih i umjetničkih djela, Međunarodnoj konvenciji iz Rima o zaštiti izvođača, proizvođača fonograma i emisionih organizacija (Rimska Konvencija), Sporazumu o komercijalnim aspektima prava na intelektualnu svojinu i WIPO ugovoru o autorskim pravima, izuzimajući moralna prava sadržana u tim Konvencijama, kada su ta djela učinjena namjerno, u obimu koji ih kvalifikuje da imaju komercijalni karakter, a učinjena su pomoću kompjuterskih sistema.

Konvencija daje mogućnost potpisnicima da u ograničenom broju slučajeva ne primjenjuju krivičnu odgovornost po stavovima 1. 2. člana 10. Konvencije, pod uslovom da na raspolaganju stoje druge vrste efikasnih pravnih sredstava i da ta rezerva ne negira međunarodne obaveze te članice definisane u međunarodnim instrumentima navedenim u stavu 1. i 2.

2.4.2. Dodatni Protokol uz Konvenciju o kibernetičkom kriminalu o kriminalizaciji akta rasizma i ksenofobije počinjenih putem kompjuterskih sistema

Dodatni protokol uz Konvenciju o kibernetičkom kriminalu o kriminalizaciji akta rasizma i ksenofobije počinjenih putem kompjuterskih sistema donijelo je Vijeće Europe 28.01.2003.godine. Dodatni protokol zahtijeva od zemalja sudionica ,kriminalizaciju širenja rasističkih i ksenofobnih sadržaja putem kompjuterskih sistema,kao i rasističko i ksenofobno obojene prijetnje i uvrede,te negiranje holokausta i ostalih genocida.

2.4.2.1. Širenje rasnog i ksenofobnog materijala pomoću kompjuterskog sistema (član 3. Dodatnog protokola)

Obavezuju se države potpisnica na usvajanje zakonodavnih i drugih mjera kako bi se ,u skladu sa njihovim domaćim pravom,utvrdilo kao krivično djelo, ako je počinjeno namjerno i neovlašteno,distribuiranje ili omogućavanje dostupnim javnosti na neki drugi način ,rasnog i ksenofobnog materijala,pomoću kompjuterskog sistema.

Pri tome država potpsnica može zadržati pravo da ne zahtijeva krivičnu odgovornost za ponašanje utvrđeno odredbama stava 1. člana 3. Dodatnog protokola ako „rasni i ksenofobni matrijal“ zagovara,propagira ili potiče diskriminaciju koja nije povezana sa mržnjom ili nasiljem,ukoliko postoje drugi efikasni lijekovi.

Također,država potpisnica može zadržati pravo da ne primjenjuje odredbe stava 1.člana 3.Dodatnog protokola u onim slučajevima diskriminacije u kojima,zbog načela o slobodi izražavanja utvrđenih u njenom domaćem pravu,ne može omogućiti korištenje efikasnih pravnih lijekova iz stava 2.člana 3.

2.4.2.2. . Prijetnja motivirana rasizmom i ksenofobijom (član 4. Dodatnog protokola)

Svaka država potpisnica treba usvojiti pottebne zakonske i druge mjere kako bi se, u skladu s njezinim domaćim pravom, utvrdilo kao kriviččno djelo, ako je počinjeno namjerno i neporavdano, slijedeće ponašanje:prijetnje, putem kompjuterskog sistema, počinjenjem teškog krivičnog djela prema odredbama njenog domaćeg prava(a) osobama zbog njihove pripadnosti nekoj grupi koja se razlikuje prema rasi,boji kože,porijeklu,nacionalnom i etničkom porijeklu te vjeri, ako se ona koristi kao povod za bilo koje od spomenutog ili (b) grupi osoba koja se razlikuje prema bilo kojem od spomenutih obilježja.

2.4.2.3. Uvreda motivirana rasizmom ili ksenofobijom (član 5 Dodatnog protokola)

Svaka država potpisnica će usvojiti sve potrebne zakonodavne i druge mjere kako bi se, u skladu sa njezinim domaćimpravom, utvrdilo kao krivično djelo, ako je počinjeno namjerno i neopravdano, slijedeće ponašanje: javno vrijeđanje, pomoću kompjuterskog sistema (a) osoba zbog njihove pripadnosti nekoj grupi koja se razlikuje prema rasi,boji kože, porijeklu, nacionalnom ili etničkom porijeklu te vjeri, ako se ona koristi kao povod za bilo koje od spomenutog, ili (b) grupe osoba koja se razlikuje prema bilo kojem od spomenutih obilježja.

Pored navedenog, država potpisnica može:

- Zahtijevati da krivično djelo iz stava 1. ovog člana mora za posljedicu imati da osoba ili grupa osoba, također iz stava 1.bude izložena mržnji, preziru ili poruzi, ili
- Zadržati pravo da ne primjenjuje, u cjelini ili samo neki njegov dio, stava 1. ovog člana.

2.4.2.4. Poricanje, bitno umanjivanje, dobravanje ili opravdanje genocida ili zločina protiv čovječnosti (član 6.Dodatnog protokola)

Države potpisnice će usvojiti potrebne zakonodavne i druge mjere kako bi se ,u skladu sa njihovim domaćim pravom,tretiralo kao krivično djelo, ako je počinjeno namjerno i neopravdano, ponašanje: distribuiranje ili omogućavanje dostupnim putem kompjuterskog sistema javnosti ili na neki drugi način , materijala kojim se poriče ,bitno umanjuje, odobravaju ili opravdavaju djela genocida ili zločina protiv čovječnosti, onako kako su ona utvrđena u međunarodnom pravu i priznata kao takva u konačnim i obavezujućim odlukama međunarodnog vojnog suda, osnovanog Londonskim sporazumom od 08.04.1945.godine, ili bilo kojeg međunarodnog suda osnovanog odgovarajućim međuunarodnim instrumentima ičiju nadležnost priznaju te države.

Pored navedenog države potpisnice mogu:

- Predvidjeti da poricanje ili bitno umanjivanje iz stava 1. Opvog člana mora biti počinjeno u namjeri da potakne mržnju, diskriminaciju ili nasilje prema nekom pojedincu ili grupi pojedinaca na temelju rase, boje kože, porijekla, nacionalnog ili

etničkog porijekla te vjere,ako se ona koristi kao povod za bilo koje od spomenutog, ili može

- Zadržati pravo da ne primjenjuje,u cjelini ili samo jedan dio,stava 1.obog člana.

2.4.3. Implementacija odredbi Konvencije o kibernetičkom/cyber kriminalu u bosanskohercegovačko krivično i krivično procesno pravo

Konvencija o cyber/kibernetičkom kriminalu Vijeća Europe, bez obzira na brojne i žučne reakcije i kritike je prvi cjelovit formalni potpisani i široko prihvaćeni multilaterarni sporazum usmjeren na probleme *cyber* kriminala. Sadržaj Konvencije o cyber kriminalu(u daljem tekstu Konvencija) polazi od promjena nastalih procesom globalizacije kopjuterskih mreža, ogomnih mogućnosti da kompjuterske mreže i elektronske informacije budu iskorištene za počinjenje krivičnih djela i da dokazi vezani za ta krivična djela budu pohranjeni, čuvani i prenešeni putem tih mreža.Također, pri tome ne treba zaboraviti potrebu za zaštitom legitimnih intersa prilikom korištenja i razvitka informatičkih tehnologija i spoznaju da efikazna borba protiv cyber kriminala imperativno zahtijeva povećanu ,brzu, uhodanu međunarodnu saradnju u krivičnopravnim predmetima.

Nakon stupanja na snagu Knvencije u odnosu na Bosnu i Hercegovinu slijedila je implementacija odredbi krivičnog materijalnog i procesnog prava Konvencije u državni i nedržavna Krivične i krivilno procesne zakone.

2.4.3.1. Krivični zakoni

Sadržajem odredbi Krivičnog zakona BiH[11] za razliku od ostala tri nedržavna Krivična zakona (Federacije BiH, Republike Srpske i Brčko Distrikta BiH) nisu implementirane preporučene odredbe krivično metrijalnog prava već je to „dogovorno prepušteno“ u nadležnost nedržavnim krivičnim zakonima.

Slijedom navedenog „dogovora“ u okviru krivičnih zakona Republike Srpske,Federacije Bosne i Hercegovine i Brčko Distrikta u modificiranoj formi i sadržaju stupulirane preporučene odredbe krivično materijalnog prava iz Konvencija kako slijedi:

2.4.3.1.1. Komparacija odredaba krivičnih zakona Republike Srpske, Federacije Bosne i Hercegovine i Brčko Distrikta preko kojih su implementirane odredbe člana 2. do 9.Konvencije.

Član KZ RS	**Naziv krivičnog djela**	**Član KZ F BIH**	**Naziv krivičnog djela**	**Član KZ BD BiH**	**Naziv krivičnog djela**
292a	Oštečenje računarskih podataka i programa	393	Oštečenje računarskih podataka i programa	387	Oštečenje računarskih podataka i programa
292b	Računarska sabotaža	392	Računarska sabotaža	392	Računarska sabotaža
292v	Izrada i unošenje računarskih virusa	-	-	-	-
292g	Računarska prevara	389	Računarska prevara	389	Računarska prevara

[11] Vidi “Slžbeni glasnik BiH”,broj 3/03,32/03,37/03,54/04,61/04,30/05,53/06,55/06,32/07,8/10)

292d	Neopvlašteni pristup zaštičenom računaru, računarskoj mreži, telekomunikacionoj mreži i elektronskoj obradi podataka	391	Neovlašteni pristup zaštičenom sistemu i mreži elektronske obrade podataka	391	Neovlašteni pristup zaštičenom sistemu i mreži elektronske obrade podataka
292đ	Spriječavanje i ograničavanje pristupa javnoj računarskoj mreži	-	-	-	-
292e	Neovlašteno korištenje računara i računarske mreže	-	-	-	-
-	-	388	Računarsko krivotvorenje	388	Računarsko krivotvorenje
-	-	390	Ometanje rada sistema i mreže elektronske obrade podataka	390	Ometanje rada sistema i mreže elektronske obrade podataka
175	Neovlašteno fotografisanje	189	Neovlašteno optičko snimanje	186	Neovlašteno optičko snimanje
199	Iskorištavanje djece i maloljtnih lica za pornografiju	211	Iskorištavanje djeteta ili maloljtnika radi pornografije	208	Iskorištavanje djeteta ili maloljetnika radi pornografije
-	-	212	Upoznavanje djeteta s pornografijom	209	Upoznavanje djeteta sa pornografijom
200	Proizvodnja i prikazivanje dječije pornografije	-	-	-	-

Analizom sadržaja odredbi državnog i nedržavnih zakona se može zaključiti da se obaveza preuzeta potpisom i ratifikacijom Konvencije u pogledu krivično metrijalnog prava uglavnom ispoštovala i da su krivična djela predviđena odredbama Konvencije u modificiranoj formi i sadržaju ugrađana u nove glave i odredbe nedržavnih krivičnih zakona u Bosni i Hercegovini. Za odredbe člana 393 do 398 iz Glave XXXII - Krivična djela protiv sistema elektronske obrade podataka[12] , člana 387 do 392. iz Glave XXXII - Krivična djela protiv sistema elektronske obrade podataka[13] i člana 292a do 292e iz Glave XXIVa Krivična djela protiv bezbjednosti računarskih podataka[14] može se reči da su djelimično usaglašene i po nazivu i sadržaju i može se zaključiti da nezanatne razlike nisu suštinske prirode .Radi kvalitetnog, potpunog i cjelovitog uvida u svako od zakonskih nedržavnih rješenja komparirati ćemo svaki od istih ili sličnih članova koji su sadržani u nedržavnim krivičnim zakonima.

2.4.3.1.1.1. Oštečenje računarskih podataka i programa

Sadržaj odredaba člana 292a Krivičnog zakona Republike Srpske je propisano krivično djelo „Oštečenje računarskih podataka i programa“ u okviru kojeg su utvrđen nedopuštene i kažnjive radnje koje, ako se počine neovlašteno, za posljedicu imaju nepotrebljive računarske

[12] Vidi Krivični zakon Federacije Bosne i Hercegovine („Službene novine F BiH“,broj:36/03, 37/03, 21/04 , 69/04, 18/05, 42/10 i 42/11),

[13] Vidi Krivični zakon Brčko Distrikt Bosna i Hercegovine („Službeni glasnik BD BiH“, broj:10/03, 6/05, 21/10, 47/11, 52/11),

[14] Vidi Krivični zakon Republike Srpske (“Službeni glasnik RS”,broj: 49/03,108/04,37/06, 70/06, 73/10, 1/12)

podatke i programa.Vrsta(novčana kazna i zatvor) i raspon kazne(od 3 mjeseca do 3 odnosno 5 godina) je uslovljen visinom štete koja prelazi limite od 10.000 KM i 30.000 KM .

Sadržajem odredaba člana 393. Krivičnog zakona Federacije BiH i člana 387.Krivičnog zakona Brčko Distrikta BiH su na sličan način utvrđene nedopuštene radnje i kažnjive radnje, koje ako se počine imaju za posljedicu neupotrebljive i nepristupačne tuđe računarske podake i programe.Pored navedenih nedopuštenih i kažnjivih radnji odredbe člana 393 i 387. idu šire te sankcioniraju i neovlašten pristup zaštičenim računarskim podacima i programima i neovlašteno presretanje njihovog prenosa te onemogučavanje i otežavanje rada i korištenja računarskog sistema ,računarskih podataka i programa ili računarske komunikacije.pored navedenog Također,pored navedenog sadržajem navedenih odredbi krivičnih zakona je sankcionisano činjenje krivičnih djela iz stava 1. do 3. navedenih članova u odnosu na računarski sistem,podatak ili program organa vlasti ,javne službe,javne ustanove ili privrednog društva od posebnog javnog interesa ili ako je tim činjenjem počinjena znatna materijalna šteta kao i onaj ko izrađuje, nabavlja, prodaje, posjeduje ili čini drugom dostupne posebne naprave , sredstva , računarske programe i podatke stvorene ili prilagođene radi učinjenja navedenih krivičnih djela.Vrsta(novčana kazna i zatvor) i raspon kazni zatvora (od 3 mjeseca do 3 odnosno pet godina) primjeren je vrsti krivičnog djela i nije vezan za nominalni iznos štete, kao u članu 292a Krivičnog zakona Republike Srpske.

U sva tri zakona je kroz imperativnu normu utvrđeno da se posebne naprave, sredstva,računarski programi ili podaci stvoreni, korišteni ili prilagođeni radu učinjenja krivičnih djela oduzimaju.

2.4.3.1.1.2. Računarska sabotaža

Sadržaj odredaba 292b (KZ RS), 398 (KZ F BIH) i 392(KZ BD BIH) na gotovo identičannačin regulišu krivično djelo računaske sabotaže.Razlika je minimalna ali uočljiva jer je odredbom 398 (KZ F BiH) za razliku od članova 292b i 392.(KZ BD BiH) pored navedenih nedopuštenih radnji i njihovih posljedica uveden i uslov da se istima prouzrokuje šteta navedenim subjektima veća od 500.000 KM. Vrsta(zatvor) i raspon kazni (od jedne do osam godina) utvrđenih odredbama člana 398 (KZ F BIH) i 392 (KZ BD BiH) su identični ,za¸razliku od raspona kazne zatvora (od šest mjeseci do pet godina) utvrđenog odredbama člana 292b (KZ RS).

2.4.3.1.1.3. Oštečenje računarskih podataka i programa

Odredbom člana 292v je utvrđeno da onaj ko izradi računarski virus sa namjerom da ga unese u tuđi računar,računarsku ili telekomunikacionu mrežu i ko unese računarski virus u tuđi računar ili računarski mrežu sa namjerom da prouzrokuje štetu čini krivično djelo koje je kažnjivo novčanom kaznom ili zatvorom u trajanju do 6 mjeseci odnosno dvije godine.

2.4.3.1.1.4. Računarska prevara

Sadržajem odrdaba člana 292g[15] (KZ RS), člana 395[16](KZ F BiH) i člana 389[17](KZ BD BiH) je utvrđeno krivično dijelo računarske prevare.Dok su odredbe članova članova 395[18](KZ F

[15] Vidi Krivični zakon Republike Srpske ("Službeni glasnik", broj 49/03, 108/04, 37/06, 70/06, 73/10, 1/12)
[16] Vidi Krivični zakon Federacije Bosne i Hercegovine ("Službene novine F BiH",broj 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11),

BIH) i 389[19].(KZ BD BiH) identične i na isti način sankcionišu svako neovlašteno u nošenje,oštečenje,izmjenu ili prikrivanje računarskog podatka iili programa ili svaki drugi način koji utiče na elektoronsku obradu podataka ,a koje imaju za cilj da počiniocu ili drugima pribave protupravnu imovinsku korist i time drugom prouzroči štetu. Vrsta(zatvor) i raspon kazne(od 6 mjeseci do pet ,deset odnosno dvanaeast godina) su primjerene visini pribavljene imovinske koristi i cenzusima koji prelaze 10.000 i 50.000 KM.Kazne za ovo krivično djelo su za nijansu rigoroznije u odnosu na isto krivično djelu u KZ RS.

Odredbe člana 292g[20] (KZ RS) na precizniji i sveobuhvatniji način utvrđuju krivično djelo , niže postavljaju cenzuse (10.000 KM i 30.000 KM) i blaže kazne po vrsti i rasponu od novčane kazne do kazne zatvora u trajanju od tri, osam odnosno 10 godina.

2.4.3.1.1.5. Neovlašteni pristup zaštičenom računaru, računarskoj mreži, telekomunikacionoj mreži (zaštičenom sistemu) i (mreži) elektronsk(e)oj obrad(e) i podataka

Odredabama člana 292d[21] (KZ RS), člana 397[22] (KZ F BiH) i člana 391 (KZ BD BIH) je utvršeno krivično djelo neovlašteni pristup zaštičenom računaru, računarskoj mreži, telekomunikacionoj mreži (zaštičenom sistemu) i (mreži) elektronsk(e)oj obrad(e) i podataka. Sadržajem navedenih odredbi se kroz sličan sadržaj bez materijalnih razlika utvrđuje da svako ko se kršeći mjere zaštite neovlašteno uključi u sistem(računar i računarska mreža) ili mrežu elektronske obrade podataka i upotrebi (ili snimi) podatke dobivene na navedeni način će se kazniti novčanom kaznom ili kauznom zatvora.Jedina matrijalna razlika što su kazne zatvora niže u odnosui na kazne predviđene za ovo krivično djelo u KZ F BiH i KZ BD BiH.

2.4.3.1.1.6. Spriječavanje i ograničavanje pristupa javnoj računarskoj mreži

Sadržajem odredaba člana 292đ[23] je utvrđeno da onaj ko neovlašteno spiječava ili ometa pristup javnoj računarskoj mreži će se kazniti novčanom kaznom ili zatvorom u trajannu do godinu dana.Ako ovo krivilčno djelo učini službeno lice u vršenjnu službene dužnosti kazniti će se zatvorom u trajanjnu do tri godine.Ovo krivično djelo kao posebno nije uvršteno u krivična djela Glava XXXII KZ F BIH i KZ BD BIH.

2.4.3.1.1.7. Neovlašteno korištenje računara i računarske mreže

Sadržajem odredaba člana 292e[24] je regulisano da onaj ko neovlašteno koristi računarske usluge ili računarsku mrežu u namjeti da sebi i drugima pribavi protupravnu imovinsku korist će se kazniti novčanom kaznom ili kaznom zatvora u trajanju do tri mjeseca.Gonjenje za ovo krivično dijelo pofduzima se po pijedlogu. Ovo krivično djelo nije uvršteno kao posebno u krivična djela Glava XXXII KZ F BIH i KZ BD BIH.

---

[17] Vidi Krivični zakon Brčko Distritkra Bosne i Hercegovine ("Službeni glasnik Bd BiH",broj 10/03, 6/05, 22/10, 47/11, 52/11),
[18] Vidi Krivični zakon Federacije Bosne i Hercegovine ("Službene novine F BiH",broj 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11),
[19] Vidi Krivični zakon Brčko Distritkra Bosne i Hercegovine ("Službeni glasnik Bd BiH",broj 10/03, 6/05, 22/10, 47/11, 52/11),
[20] Vidi Krivični zakon Republike Srpske ("Službeni glasnik",broj 49/03,108/04,37/06,70/06,73/10,1/12)
[21] Vidi Krivični zakon Republike Srpske ("Službeni glasnik",broj 49/03,108/04, 37/06,70/06, 73/10, 1/12)
[22] Vidi Krivični zakon Federacije Bosne i Hercegovine ("Službene novine F BiH",broj 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11),
[23] Vidi Krivični zakon Republike Srpske ("Službeni glasnik",broj 49/03, 108/04, 37/06, 70/06, 73/10, 1/12)
[24] Vidi Krivični zakon Republike Srpske ("Službeni glasnik",broj 49/03, 108/04, 37/06, 70/06, 73/10, 1/12)

2.4.3.1.1.8. Računarsko krivotvorenje

Identičnim sadržajem odredbi člana 394[25] (KZ F BiH) i 388[26](KZ BD BiH) se utvrđuje krivično djelo računarsko krivotvorenje.Navedenim članovima je utvrđeno da svako ko izradi,unese,izmjeni,izbriše ili učini neupotrebljivim računarske podatke koji imaju vrijednost za pravne odnose,s ciljem da se upotrijebe kao pravi ili sam upotrijebi te podatke ili progran će se kazniti novčanom kaznom ili kaznom zatvora do tri godine.Pored toga, sadržajem navedenih odredbi je utvrđeno da ako je ovo dijelo počinjenou odnosu na računarskle podatke ili programe tijela,javne službe,javnih ustanova ili privredbnih društava od posebnog javnog interesa ili je prouzrokovana znatna šteta kaznit će se dužom kaznom zatvora u trjanju od tri mjeseca do pet godina.Takođe onaj ko izrađuje ,nabavlja, prodaje, posjeduje ili čini drugima pristupačnim posebne naprave, sredstva, računarske programe ili računarske podatke stvorene ili prilagođene radi počinjenja već navedenih krivilčnih djela ovoh članova također će se kazniti novačanom kaznom ili kaznom zatvora ,a te naprave, sredstva, računarski programi ili podaci će vse odzeti. Ovo krivično djelo nije uvršteno kao posebno u krivična djela Glava XXIV KZ RS.

2.4.3.1.1.9. Ometanje rada sistema i mreže elektronske obrade podataka

Identičnim sadržajem odredbi člana 396[27] (KZ F BiH) i 390[28](KZ BD BiH) se utvrđuje krivično djelo Ometanje rada sistema i mreže elektronske obrade podataka.Navedenim odredbama utvrđeno je da svakoonaj ko neovlaštenim pristupom u sistem ili mrežu elektronske obrade podataka izazove zastoj ili poremeti rad tog sistema ili mreže ,kaznit će se novčanom kaznom ili kaznom zatvora do tri godine. Ovo krivično djelo nije uvršteno kao posebno u krivična djela Glava XXIV KZ RS.

2.4.3.1.1.10. Krivična djela koja se odnose na dječiju prornografiju

Krivična djela koja se odnose na dječiju pornografiju i koja su počinjena namjerno i bespravno nisu regulisana odredbama krivičnoh zakona Bosne i Hercegovine,već je ta oblast dogovorno prepuštena na regulaciju nedržavnim krivičnim zakonima.Na tom fonu je sadržajem odredbi člana 175[29] (Neovlašteno fotografisanje) iz GLAVE XVII- KRIVIČNA DJELA PROTIV SLOBODA I PRAVA GRAĐANA i članova 199[30] (Iskorištavanje djeteta radi pornografije) i 200[31] (Proizvodnja i prikazivanje dječije pornografije) iz GLAVE XIX-KRIVIČNA DJELA PROTIV POLNOG INTEGRITETA su utemeljena krivična djela koja se od dječiju pornografiju u Krivičnom zakonu Republike Srpske.Takođe slično je urađeno kroz sadržaj odredba člana 189[32] (Neovlašteno optičko snimanje) iz GLAVE XVII-KRIVIČNA DJELA PROTIV SLOBODE I PRAVA ČOVJEKA I GRAĐANINA i članova

[25] Vidi Krivični zakon Federacije Bosne i Hercegovine ("Službene novine F BiH",broj 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11),
[26] Vidi Krivični zakon Brčko Distritkra Bosne i Hercegovine ("Službeni glasnik Bd BiH",broj 10/03, 6/05, 22/10, 47/11, 52/11),
[27] Vidi Krivični zakon Federacije Bosne i Hercegovine ("Službene novine F BiH",broj 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11),
[28] Vidi Krivični zakon Brčko Distritkra Bosne i Hercegovine ("Službeni glasnik BD BiH", broj 10'/03, 6/05, 22/10, 47/11, 52/11),
[29] Vidi Krivični zakon Republike Srpske ("Službeni glasnik",broj 49/03, 108/04, 37/06, 70/06, 73/10, 1/12),
[30] Vidi Krivični zakon Republike Srpske ("Službeni glasnik",broj 49/03, 108/04, 37/06, 70/06 ,73/10, 1/12),
[31] Vidi Krivični zakon Republike Srpske ("Službeni glasnik",broj 49/03, 108/04, 37/06, 70/06, 73/10, 1/12)
[32] Vidi Krivični zakon Federacije Bosne i Hercegovine ("Službene novine F BiH",broj 36/03, 37/03, 21/04 ,69/04, 18/05, 42/10, 42/11),

211[33] (Iskorištavanje djeteta radi pornografije) i člana 212[34] (Upoznavanje djeteta sa pornografijom) iz GLAVE XIX-KRIVIČNA DJELA PROTIV POLNE SLOBODE I MORALA Krivičnog zakona Federacije Bosne i Hercegovine odnosno sadržajem člana 186[35] (Neovlašteno optičko snimanje) iz GLAVE XVII-KRIVIČNA DJELA PROTIV SLOBODE I PRAVA ČOVJEKA I GRAĐANINA te članova 208[36] (Iskorištavanje djeteta radi pornografije) i 209[37] (Upoznavanje djeteta sa pornografijom) iz GLAVE XIX-KRIVIČNA DJELA PROTIV POLNE SLOBODE I MORALA Krivičnog zakona Brčko Distrikta Bosne I Hercegovine.Navedene odredbe nedržavnih nkrivičnih zakona i pored sadržajne razlišitosti u suštini su dovoljno široke da podrazumjevaju odnosno obuvataju i krivična djela počinjena putem računarskog sistema.

Od razlika u sadržaju treba izdvojiti odredbe člana 175[38] (Neovlašteno fotografisanje) iz KZ RS koje su za razliku od odredaba člana 189 [39](Neovlašteno optičko snimanje) iz KZ F BiH i 186[40].(Neovlašteno optičko snimanje) iz KZ BD BIH su uopštenije i ne sadrže specifičnosti koje sadrži ovo krivično djelo u KZ F BiH i KZ BD BiH u odnosu na dijete ili maloljetnik.Toj veoma bitnoj sadržajnoj razlici valja i dodati i razlike u visini kazni za počinioce ovog krivičnog djela koje treba da su primjerene težini djela pogotovo u odnosu na djete ili maloljtnika.Stoga sadržajna razlika pri definisanju ovog krivičnog djela se odrazlia i na visinu kazne koja je u KZ F Bi H i KZ BD BiH gradirana prema druđtvenoj opasnosti i strožija nego u RZ RS.

Pored navedenog i sadržaji odredba člana 199[41] (Iskorištavanja djeteta radi pornografije) se razlikuje u odnosu na sadržaj odredaba člana 211[42](Iskorištavanje djeteta radi pornografije) i člana 208[43](Iskorištavanje djeteta radi prornografije jer je navedenim odredbama KZ F BiH i KZ BD BiH sadržaj iz člana 199[44].KZ RS proširen i pored identičnog teksta ima dodatak koji se odnosi na“ili posjeduje ili uvozi ili prodaje ili rastura ili prikazuje takav materijal“.Takođe navedenim odredbama je donji prag zatvorske kazne podignut na jednu godinu,a gornji prag je ostao na nivou koji je utvrđen navedenomodrebom Krivičnog zakona RS.

[33] Vidi Krivični zakon Federacije Bosne i Hercegovine (“Službene novine F BiH”, broj 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11),
[34] Vidi Krivični zakon Federacije Bosne i Hercegovine (“Službene novine F BiH”,broj 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11),
[35] Vidi Vidi Krivični zakon Brčko Distritkra Bosne i Hercegovine (“Službeni glasnik BD BiH”,broj 10/03,6/05,22/10,47/11,52/11),
[36] Vidi Krivični zakon Brčko Distritkra Bosne i Hercegovine (“Službeni glasnik BD BiH”,broj 10/03, 6/05, 22/10, 47/11,52/11),
[37] Vidi Krivični zakon Brčko Distritkra Bosne i Hercegovine (“Službeni glasnik BD BiH”,broj 10/03, 6/05, 22/10, 47/11, 52/11),
[38] Vidi Krivični zakon Republike Srpske (“Službeni glasnik”,broj 49/03, 108/04, 37/06, 70/06, 73/10, 1/12)
[39] Vidi Krivični zakon Federacije Bosne i Hercegovine (“Službene novine F BiH”,broj 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11),
[40] Vidi Krivični zakon Brčko Distritkra Bosne i Hercegovine (“Službeni glasnik BD BiH”,broj 10/03, 6/05, 22/10, n47/11, 52/11),
[41] Vidi Krivični zakon Republike Srpske (“Službeni glasnik”,broj 49/03,108/04,37/06,70/06,73/10,1/12),
[42] Vidi Krivični zakon Federacije Bosne i Hercegovine (“Službene novine F BiH”,broj 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11),
[43] Vidi Krivični zakon Brčko Distritkra Bosne i Hercegovine (“Službeni glasnik BD BiH”,broj 10/03, 6/05, 22/10, 47/11, 52/11),
[44]Vidi Krivični zakon Republike Srpske (“Službeni glasnik”,broj 49/03, 108/04, 37/06, 70/06, 73/10, 1/12)

Također,sadržajem odredaba člana 212[45](Upoznavanje djeteta sa pornografijom) iz KZ F BiH i člana 209[46](Upoznavanje djeteta sa pornografijom) iz KZ BD BIH su na identičan način utvrđene nedopuštene radnje koje su sankcionisane ovim krivičnim djelom ,a koje podrazumjevaju „prodaju, prikazivanje ili javno izlaganje.....spisa, slika, audio vilzuelnog matrijalai i drugih predmeta pornografsklog sadržaja djetetu ..... kao i kazne za navedeno djelo uz obavezu oduzimanja predmeta. Ovo krivično djelo nije uvršteno kao posebno u krivična djela Glava XXIX KZ F BiH i KZ BD BiH.

Odredbama člana 200[47].(Proizvodnja i prikazivanje dječije pornografije) iz KZ RS je vrlo detaljno utvrđeno značenje termina „dječija pornografija“ koja je u velikoj mjeri usaglašena sa odredbama člana 9. stav 2.tačka a).,b). i c).[48] Konvencije i utvrđeno krivično djelo za nuđenje, distribuciju, prikazivanje i javno izlaganje..... spisa,slika,audio-vizuelnih ili drugih predmeta koji predstavljaju dječiju pornografiju ili .....proizvodnja,nabavka,držanje i prikazivanje dječije pornografske predstave.Pored navedenog u odredbi ovog člana se pravi razlika za slučajeve kada je ovo djelo izvršeno preko sredstava javnog informisanja ili putem interneta i tome je prilagođena sankcija. Ovo krivično djelo nije uvršteno kao posebno u krivična djela Glava XXIX KZ F BiH i KZ BD BiH.

2.4.3.1.1.11. Iplementacija krivičnih djela u vezi sa napadom na intelektualnu svojinu i odnosna prava

Krivična djela koja se odnose na povredu autorskih i srodnih prava iz člana 10[49] Konvencije ,nisu propisana kao kaznena djela koja je moguće počiniti upotrbom računalnog sistema,ali su odredbe krivičnih djela iz člana 242[50].(Zloupotreba autorskih prava), člana 243[51] (Nedozvoljeno korištenje autorskih prava), člana 244[52] (Nedozvoljeno korištenje prava proizvođaća zvučne snimke) , člana 245[53] (Nedozvoljeno korištenje prava radiodifuzije) i člana 246[54] (Nedozvoljena distribucija satelitskog signala) Krivičnog zakona BiH dovoljno široki da obuhvataju i krivična djela počinjena pomoću računarskog sustema.

[45] Vidi Krivični zakon Federacije Bosne i Hercegovine (“Službene novine F BiH”,broj 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11),
[46] Vidi Krivični zakon Brčko Distritkra Bosne i Hercegovine (“Službeni glasnik Bd BiH”,broj 10/03, 6/05, 22/10, 47/11, 52/11),
[47] Vidi Krivični zakon Republike Srpske (“Službeni glasnik”,broj 49/03,108/04,37/06,70/06,73/10,1/12)
[48] Vidi Konvenciju o cybercrime Vijeća Europe od 23.novembra 2011.godine („Službeni glasnik BiH“,broj 06/06 Međunarodni ugovori), član 9,
[49] Vidi Konvenciju o cybercrime Vijeća Europe od 23.novembra 2011.godine („Službeni glasnik BiH“,broj 06/06 Međunarodni ugovori), Član 10,
[50] Vidi Krivični zakon Bosne i Hercegovine (“Službeni glasnik BiH”, broj 3/03, 32/03, 37/03, 54/04, 61/94, 30/05, 53/06, 55/06, 32/07, 8/10)
[51] Vidi Krivični zakon Bosne i Hercegovine (“Službeni glasnik BiH”,broj 3/03, 32/03, 37/03, 54/04, 61/94, 30/05, 53/06, 55/06, 32/07, 8/10)
[52] Vidi Krivični zakon Bosne i Hercegovine (“Službeni glasnik BiH”,broj 3/03, 32/03, 37/03, 54/04, 61/94, 30/05, 53/06, 55/06, 32/07, 8/10)
[53] Vidi Krivični zakon Bosne i Hercegovine (“Službeni glasnik BiH”,broj 3/03, 32/03, 37/03, 54/04, 61/94, 30/05, 53/06, 55/06, 32/07, 8/10)
[54] Vidi Krivični zakon Bosne i Hercegovine (“Službeni glasnik BiH”,broj 3/03, 32/03, 37/03, 54/04, 61/94, 30/05, 53/06, 55/06, 32/07, 8/10)

2.4.4. Implementacija odredaba Dodatnog Protokola uz Konvenciju o kibernetičkom kriminalu o kriminalizaciji akta rasizma i ksenofobije počinjenih putem kompjuterskih sistema

Sadržaj odredaba člana 3.,4.,5. i 6.[55]Dodatnog protokola uz Konvenciju o kribernetičkom kriminalu koje tretiraju širenje rasnog i ksenofobnog materijala pomoću računarskog sistema; prijetnje morivirane rasizmnom i ksenofobijom; uvrede motivirane rasizmom i ksenofobijom i poricanje, bitno umanjivanje ili opravdanje genocida ili zločina protiv čovječnosti.Navedene odredbe su djelimično implementirane u državni i nedržavne krivične zakone Bosne i Hercegovine. Naime sadržajem odredana člana 145a[56] (Izazivanje nacionalne, rasne i vjerske mržnje, razdora i netrepeljivosti) KZ BiH,člana 294a[57] (Izazivanje nacionalne, rasne i vjerske mržnje, razdora i netrepeljivosti) KZ RS, člana 163[58] (Izazivanje nacionalne, rasne i vjerske mržnje, razdora i netrepeljivosti) KZ F BiH i člana 160[59] (Izazivanje nacionalne, rasne i vjerske mržnje, razdora i netrepeljivosti) KZ BD BiH.

Iako državni i nedržavni krivični zakoni propisuju sankcije za krivično djelo „Izazivanje nacionalne, rasne i vjerske mržnje, razdora i netrepeljivosti“ sadržaj odredbi članova koji sankcionišu zakonima nedopuštena ponašanja nije identičan.Tako da sadržaj odredba člana 145a[60] državnog zakona sankcioniše se svako onaj ko javno izaziva ili raspiruje nacionalnu ,rasnu ili vjersku mržnju, razdor ili netrpeljivost među konstitutivnim narodima i ostalim, kao i drugim koji žive ili borave u Bosni i Hercegovini i dodatno sankcionišu svakog ko navedeno krivično djelo počini zloupotrebom svog položaja ili ovlaštenje.Za razliku od državnog zakona nedržavni su obuhvatniji pa pored modificiranih nedopuštenih radnji koje su obuhvaćene u državnim krivičnim zakonom sankcionišu i situacije u kojima je ovo krivično djelo učinjeno prinudom, zlostavljanjem, ugrožavanjem sigurnosti, izlaganjem popruzi nacionalnih, etničkih ili vjerskih simbola, oštećenjem tuđih stvari, skrnavljenjem spomenika, spomen obilježja ili grobova.Također, pored navedenog dodatno se sancionišu posljedice krivičnih djela iz stava 1. i 2. nedržavnih članova koje su dovele do eventualnih nereda, nasilja ili drugih teških posljedica za zajednilčki život naroda i ostalih koji žive u Republici Srpskoj, Federacije Bosne i Hercegovine i Brčko Distrika Bosne i Hercegovine.Materijali i predmeti koji nose nedopuštene poruke kao i sredstva za njihovu izradu, umnožavanje ili rasturanje se oduzimaju. I pored činjenicue da su društevenoj opasnosti koju nose ova krivična djela primjerene vrsta i visina kazni.KZ F BiH i KZ BD BIH predviđaju više kazne u odnosu na KZ RS i KZ BIH za počinioce ovih krivičnih djela.

[55] Vidi Dodatni protokol uz Konvenciju o cybercrime Vijeća Europe od 23.novembra 2011.godine („Službeni glasnik BiH“,broj 06/06 Međunarodni ugovori),
[56] Vidi Krivični zakon Bosne i Hercegovine (“Službeni glasnik BiH”,broj 3/03, 32/03, 37/03, 54/04, 61/94, 30/05, 53/06, 55/06, 32/07, 8/10),
[57] Vidi Krivični zakon Republike Srpske (“Službeni glasnik”,broj 49/03,108/04,37/06,70/06,73/10,1/12),
[58] Vidi Krivični zakon Federacije Bosne i Hercegovine (“Službene novine F BiH”,broj 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11),
[59] Vidi Krivični zakon Brčko Distritkra Bosne i Hercegovine (“Službeni glasnik Bd BiH”,broj 10/03, 6/05, 22/10, 47/11, 52/11),
[60] Vidi Krivični zakon Bosne i Hercegovine (“Službeni glasnik BiH”,broj 3/03, 32/03, 37/03, 54/04, 61/94, 30/05, 53/06, 55/06, 32/07, 8/10),

2.4.5. Primjena međunarodnih standarda koji su inaugurisani Konvencijom i Dodatnim protokolom u krivično-procesnom zakonodavstvu BiH, Federacije BiH, Republike Srpske i Brčko Distrikta BiH.

Sadržajem odredaba državnog Zakona o krivičnom postupku i nedržavnih zakona o krivičnom postupku nisu preuzeta krivično procesna rješenja sadržana u odredbama člana 16.[61](Hitna zaštita pohranjenih računarskih podataka),17[62](Hitna zaštita i djelimično otkrivanje podataka u prometu) , člana 18[63] (Nalog za proizvodnju), člana 19[64] (Pretrage i oduzimanje pohranjenih računarskih podataka), član 20[65] (Prikupljanje računarskih podataka u realnom vremenu) i člana 21[66] (Presretanje podataka o sadržaju) Konvencije o kibernetičkom/ciber kriminalu što za posljedici ima i brojne dileme od kojih ćemo se nekim baviti u nastavku.

S obzirom da je kao jedan od najrasprostranjenijih uređaja nosilaca digitalnih podataka, kompjuter, to će se kroz ovaj modul najviše pažnje i posvetiti kompjuterskoj forenzici, iako su principi skoro istovjetni u svim fazama analiza povezanosti digitalnih uređaja sa izvršenim krivičnim djelom.

Zakon o krivičnom postupku BiH, članom 51. st. 2.[67] ....“ obuhvata i pretresanje kompjutera i sličnih uređaja za automatsku obradu podataka koji su s njima povezani...“ Slične su odredbe i u Zakonima o krivičnom postupku u FBiH, RS i Brčko Distrikta BiH[68] (imajući u vidu da je ovaj modul namijenjen prvenstveno tužiocima, sudijama i drugim službenim licima koji poznaju materijalno i procesno krivično pravo, te da se radi o osnovnom modulu, to se neće kroz modul posebno zadržavati na odredbama zakona koji obrađuju ovu materiju, ali će se ipak ukazati na neophodnost posebne pažnje kod postupanja u vezi sa ovom vrstom krivičnih dijela i provođenja posebno propisanih postupaka u cilju otkrivanja i dokumentovanja krivičnog djela i izvršioca). [69] Prilikom izrade modula u kojem će se ukazati na povezanost materijalno pravnog i procesno pravnog elementa, sa načinom izvršenja, otkrivanja i dokazivanja krivičnih dijela iz ove oblasti, posvetiće se znatno veća pažnja konkretnim situacijama, nakon kojeg modula, uz redovnu obuku, pojedini tužioci i pripadnici agencija će morati biti usmjereni na specijalistički odnos prema ovoj oblasti. Brzina promjena, te

[61] Vidi Konvenciju o cybercrime Vijeća Europe od 23.novembra 2011.godine („Službeni glasnik BiH“,broj 06/06 Međunarodni ugovori),član 16.,
[62] Vidi Konvenciju o cybercrime Vijeća Europe od 23.novembra 2011.godine („Službeni glasnik BiH“,broj 06/06 Međunarodni ugovori),član 17.,
[63] Vidi Konvenciju o cybercrime Vijeća Europe od 23.novembra 2011.godine („Službeni glasnik BiH“,broj 06/06 Međunarodni ugovori),član 18.,
[64] Vidi Konvenciju o cybercrime Vijeća Europe od 23.novembra 2011.godine („Službeni glasnik BiH“,broj 06/06 Međunarodni ugovori),član 19.,
[65] Vidi Konvenciju o cybercrime Vijeća Europe od 23.novembra 2011.godine („Službeni glasnik BiH“,broj 06/06 Međunarodni ugovori),član 20.,
[66] Vidi Konvenciju o cybercrime Vijeća Europe od 23.novembra 2011.godine („Službeni glasnik BiH“,broj 06/06 Međunarodni ugovori),član 21.,
[67] Vidi Zakon o krivičnom postupku Bosne i Hercegovine (“Službeni glasnik BiH”,broj :3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 16/09,93/09,
[68] Vidi Zakon o krivičnom postupku BiH („ Službeni glasnik BiH“, broj: 03/03, 32/03, 36/03 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09, Zakon o krivičnom postupku FBiH 35/03, 37/03, 56/03, 78/04, 38/05, 55/06, 27/07, 53,07, 09/09, 12/10, Zakon o krivičnom postupku RS 50/03, 111/04, 115/04, 29/07, 68/07, 119/08, Zakon o krivičnom postupku Brčko Distrikt BiH 10/03, 48/04, 06/05, 06/05 (2), 12/07,14/07, 21/07
[69] Vidi Krivični zakon BiH 03/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07, 8/10 , Krivični zakon FBiH 36/03,37/03, 21/04, 69/04, 18/05,42/10, 42/11, Krivični zakon RS 49/03, 108/04, 37/06, 73/10; Krivični zakon Brčko Distrikta BiH 10/03, 45/04, 06/05, 21/10

prilagodljivost izvršenju krivičnih dijala, ukazuje na činjenicu da se i tužioci moraju usmjeravati prema kvalitetnoj obuci, te da se moraju povezivati radi razmjene iskustava.

U sadržajm odredba člana 20.stav 1 tačka u). i v).[70](Zakona o krivičnom postupku Bosne i Hercegovine), člana 20.stav 1 tačka r) i s).[71] (Zakona o krivičnom postupku Republike Srpske) , člana 21 stav 1.tačka u).[72] i v). (Zakona krivičnom postupku F BiH) i člana 20[73] (Zakona o krivičnom postupku Brčko Distrikt Bosne i Hercegovine) date su definicije pojmova kako je to definisano sadržajem odredaba člana 1 stav 1. tačka a) i b).[74] Konvencije o kibernetičkom/cyber kriminalu:

- "Kompjuterski sistem" je svaka naprava ili skup međusobno spojenih ili povezanih naprava od kojih jedna ili više njih na osnovu programa automatski obrađuje podatke.

- "Kompjuterski podaci" označava svako iskazivanje činjenica, informacija ili koncepata u obliku prikladnom za obradu u kompjuterskom sistemu, uključujući i program koji je u stanju prouzrokovati da kompjuterski sistem izvrši određenu funkciju.".

Kada se, nakon operativnog rada dođe do osnova sumnje da je izvršeno neko krivično djelo ili je u pripremi, uz korištenje kompjutera, to je potrebno i dokumentovati putem valjanih dokaza

Na temelju sadržaja odredaba člana 51 stav 2. i 3.[75] Zakona o krivičnom postupku Bosne i Hercegovine,člana 65.stav 2. i 3.[76] ZKP F BiH, članu 51.stav 2. i 3. [77] ZKP BD BiH, člana 115.stav 2. i 3.[78] Zakona o krivičnom postupku Republike Srpske, može izvući nekoliko vrlo bitnih elemenata koji omogućavaju provođenje postupka digitalne forenzike. Kao osnovno, potrebno je da postoji osnova za sumnju da se radom sa računarom učinilo neko djelo koje je zabranjeno, te da se pregledom tog računara može dokazati postojanje zabranjene radnje i lica koje je tu radnju poduzelo. Ovo znači da se neće pristupati provjeri računara kod postojanja osnova sumnje za svako krivično djelo, nego samo za krivična djela koja imaju povezanost sa radom računara. Kao što je naprijed već pojašnjeno, ne smatraju se sva krivična djela učinjena uz pomoć računara djela iz reda cyber crime.

[70] Vidi Zakon o krivičnom postupku Bosne i Hercegovine ("Službeni glasnik BiH",broj :3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 16/09,93/09,

[71] Vidi Zakon o krivičnom postupku RS(„Službeni glasnik RS ",broj 50/03, 111/04, 115/04, 29/07, 68/07, 119/08),

[72] Vidi Zakon o krivičnom postupku FBiH („Službene novine F BiH",broj: 35/03, 37/03, 56/03, 78/04, 38/05, 55/06, 27/07, 53,07, 09/09, 12/10,

[73] Vidi Zakon o krivičnom postupku Brčko Distrikt BiH („Službeni glasnik BD BiH",broj: 10/03, 48/04, 06/05, 06/05 (2), 12/07,14/07, 21/07,44/10.,

[74] Vidi Konvenciju o cybercrime Vijeća Europe od 23.novembra 2011.godine („Službeni glasnik BiH",broj 06/06 Međunarodni ugovori),član 1,stav 1.tačka a). i b)..,

[75] Vidi Zakon o krivičnom postupku Bosne i Hercegovine ("Službeni glasnik BiH",broj :3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 16/09,93/09,

[76] Vidi Zakon o krivičnom postupku FBiH („Službene novine F BiH",broj: 35/03, 37/03, 56/03, 78/04, 38/05, 55/06, 27/07, 53,07, 09/09, 12/10,

[77] Vidi Zakon o krivičnom postupku Brčko Distrikt BiH („Službeni glasnik BD BiH",broj: 10/03, 48/04, 06/05, 06/05 (2), 12/07,14/07, 21/07,44/10.,

[78] Vidi Zakon o krivičnom postupku RS („Službeni glasnik RS ",broj 50/03, 111/04, 115/04, 29/07, 68/07, 119/08),

U člana 51 stav 3.[79] ZKP BIH, 65.stav 3.[80] ZKP FBIH, članu 115 stav 3. [81]ZKP RS i članu 51. stav 3.[82]ZKP BD BIH je utvrđena obaveza da se pretresanje kompjutera i sličnih uređaja obavlja uz pomoć stručnog lica. Ovdje se može postaviti nekoliko pitanja. Da li se ova obaveza ima primjeniti i kod samog postupka izuzimanja računara ili kod pregleda (mislim da je neprikladan izraz pretresanje kompjutera) kompjutera na izdvojenom mjestu– forenzičkoj laboratoriji. Ako se ova obaveza odnosi i na obavezu prisustva stručnog lica i kod izuzimanja računara, onda je to posebno pitanje broja zaposlenih lica u policiji koji se mogu smatrati stručnim licem. Poznato je da još uvijek veliki broj policijskih stanica nije materijalno i tehnički opremljen, iz čega bi moglo da proizađe da nemaju ni stručnih lica iz ove oblasti. Termin «stručno lice» je izuzetno širok pojam, jer se osnovano može postaviti pitanje da li je samo inženjer informatike stručno lice, jer ni svi inženjeri informatike se ne znaju koristiti svim operativnim sistemima (Windovs, Linux, Mac i dr). Prilikom izuzimanja računarske opreme, vrši se ispitivanje administratora radi utvrđivanje u kojem operativnom sistemu i sa kojim programima radi računar, da li postoje posebno zaštićeni podaci, koje su ulazne šifre i sl. I ovdje treba imati pojašnjenje i razlikovati stručno lice u zavisnosti od vrste posla kojim treba da se bavi to «stručno lice» na licu mjesta. Npr. ako je nalog suda da se izuzme računar, sa dodatnom opremom, onda se mora znati postupak koji se mora provesti ako je računar uključen i u radnoj funkciji u trenutku izuzimanja, ili je računar isključen. Mora se znati da li je računar u radu kao pojedinačni ili je umrežen, da li je računar server, da li radi putem interneta, šta ima od vanjske podrške, koji su to uređaji koji bi mogli biti povezani sa računarom, a mogu imati tražene podatke i sl. To znači da to stručno lice mora znati kakve su tehničke mogućnosti uređaja koji su povezani sa računarom. Ranije je kružila šala o bezrazložnom izuzimanju i monitora, jer raniji monitori nisu imali memoriju, a novi tipovi monitora koji se mogu koristiti i kao TV imaju vlastitu veoma veliku memoriju, tako da i ta memorija može sadržavati potrebne dokaze. Ista je situacija sa skenerima, fax aparatima itd. Ovdje se dalje postavlja pitanje da li to stručno lice koje je učestvovalo u izuzimanju računara, može učestvovati i u pregledu računara i sačinjavanju izvještaja o sadržaju istog.

Odredbom člana 60.stav 4.[83] ZKP BIH, člana 74. st. 4.[84] ZKP FBiH ,člana 124.stav 4.[85] ZKP RS i je utvrđeno da pretresanju stana i ostalih prostorija prisustvuju dva punoljetna građanina kao svjedoci i oni bi trebali da potpišu zapisnik o pretresanju Postavlja se pitanje da li su dva punoljetna lica obavezna da prisustvuju i potpišu zapisnik o izuzimanju računara i druge opreme, te da li su obavezni da prisustvuju pretresanju kompjutera.

[79] Vidi Zakon o krivičnom postupku Bosne i Hercegovine ("Službeni glasnik BiH",broj :3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 16/09,93/09,

[80] Vidi Zakon o krivičnom postupku FBiH („Službene novine F BiH",broj: 35/03, 37/03, 56/03, 78/04, 38/05, 55/06, 27/07, 53,07, 09/09, 12/10,

[81] Vidi Zakon o krivičnom postupku RS („Službeni glasnik RS ",broj 50/03, 111/04, 115/04, 29/07, 68/07, 119/08),

[82] Vidi Zakon o krivičnom postupku Brčko Distrikt BiH („Službeni glasnik BD BiH",broj: 10/03, 48/04, 06/05, 06/05 (2), 12/07,14/07, 21/07,44/10.,

[83] Vidi Zakon o krivičnom postupku Bosne i Hercegovine ("Službeni glasnik BiH",broj :3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 16/09,93/09,

[84] Vidi Zakon o krivičnom postupku FBiH („Službene novine F BiH",broj: 35/03, 37/03, 56/03, 78/04, 38/05, 55/06, 27/07, 53,07, 09/09, 12/10,

[85] Vidi Zakon o krivičnom postupku RS („Službeni glasnik RS ",broj 50/03, 111/04, 115/04, 29/07, 68/07, 119/08),

U sadržaju odredaba člana 62. stav 3.[86] ZKP BiH, člana 76. st. 3.[87] ZKP FBiH, člana 62 stav 3.[88] ZKP BD BiH i člana 126. stav 3.[89] ZKP RS koji regulišu zapisniku o pretresanju određeno je da će se predmeti upotrijebljeni prilikom pretresanja kompjutera i sličnih uređaja za automatsku obradu podataka vratiti poslije pretresanja njihovim korisnicima, ako nisu potrebni za daljnje vođenje krivičnog postupka. Ova odredba je također, nedovoljno jasna, jer se na ovaj način ne zna koji to mogu biti predmeti upotrijebljeni prilikom pretresanja kompjutera i kada bi se ti predmeti trebali vratiti. Ponovno se vraćamo na termin pretresanje kompjutera. Da li se to odnosi na vizuelni pregled kompjutera prilikom njegovog izuzimanja ili se radi o pregledu baza podataka u samom kompjuteru.Sva ova pitanja ukazuju na neophodnost donošenja posebnih pravilnika i uputstava o načinu rada u ovoj oblasti.

Ako termin «pretresanje kompjutera» podrazumjeva i pregled sadržaja kompjutera, a pretpostaviti je da je to svrha pretresanja, onda se mora odrediti stručno lice koje će taj pregled izvršiti, odnosno dolazimo u fazu vještačenja sadržaja računara.

U cilju obezbjeđenja valjanosti dokaza, određeni vještak mora poštovati procedure koje su iznimno važne u ovom procesu dokazivanja. Osnovno pravilo je da se nikada ne vrši analiza direktno na izuzetom računaru. Naime, svako uključivanje računara za sobom povlači promjene podataka na njemu, a samim tim omogućava da se dokazuje neautentičnost dokaza.

Pregledom računara se može dokazati postojanje kompromitirajućih podataka, ali je to potrebno dovesti u vezu sa određenom ličnošću, da li je to uradio baš ovaj počinitelj, da li je taj računar korišten kao „kukavičije jaje“ i sl.... (primjer sa spam porukama za lijekove, kada je na stotine hiljada računara korišteno, bez znanja vlasnika, za dalje slanje neželjenih poruka).

Postupajući tužilac i sudija mora poznavati osnove ove vrste forenzike, kako bi mogao dati nalog u cilju dobijanja kvalitetnog dokaza. U nalogu za izuzimanje opreme koja će biti predmet forenzičkog dokazivanja, mora biti naznačeno šta se izuzima, na koji način se to izuzima, sa tačno datim nalogom šta treba da se utvrdi.

Prema odredbi člana 71.[90]ZKP BIH, člana 85[91]. ZKP FBIH, člana 71.[92] ZKP BD BIH i člana 135 [93]ZKP RS otvaranje i pregled privremeno oduzetih predmeta i dokumentacije vrši tužilac. Ovdje imamo i otvaranje i pregled privremeno oduzetog kompjutera, a to radi lice

[86] Vidi Zakon o krivičnom postupku Bosne i Hercegovine (“Službeni glasnik BiH”,broj :3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 16/09,93/09,

[87] Vidi Zakon o krivičnom postupku FBiH („Službene novine F BiH“,broj: 35/03, 37/03, 56/03, 78/04, 38/05, 55/06, 27/07, 53,07, 09/09, 12/10,

[88] Vidi Zakon o krivičnom postupku Brčko Distrikt BiH („Službeni glasnik BD BiH“,broj: 10/03, 48/04, 06/05, 06/05 (2), 12/07,14/07, 21/07,44/10.,

[89] Vidi Zakon o krivičnom postupku RS („Službeni glasnik RS “,broj 50/03, 111/04, 115/04, 29/07, 68/07, 119/08),

[90] Vidi Zakon o krivičnom postupku Bosne i Hercegovine (“Službeni glasnik BiH”,broj :3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 16/09,93/09,

[91] Vidi Zakon o krivičnom postupku FBiH („Službene novine F BiH“,broj: 35/03, 37/03, 56/03, 78/04, 38/05, 55/06, 27/07, 53,07, 09/09, 12/10,

[92] Vidi Zakon o krivičnom postupku Brčko Distrikt BiH („Službeni glasnik BD BiH“,broj: 10/03, 48/04, 06/05, 06/05 (2), 12/07,14/07, 21/07,44/10.,

[93] Vidi Zakon o krivičnom postupku RS („Službeni glasnik RS “,broj 50/03, 111/04, 115/04, 29/07, 68/07, 119/08),

koje je tužilac ili sud odredio. Da li se ne postupanje u skladu sa ovom odredbom može pravdati nestručnošću tužioca?

Slijedom navedenog i poodavno artikulisane potrebe sudija i tužilaca koje su pažljivo stipulirane u konceptu obuke o kibernetičkom krim inalu za sudije i tužioce koji je sastavni dio Projekta o kibernetičkom krimninalu i Lisabonske mreže koji vodi i sufinasira Vijeće Europe, Odjel za informatičko društvo i borbu protiv kriminala, je kocipiran i ovaj edukativni model.Njegov osnovni cilj da tužioci i pripadnici sagencija za sprovođenje zakona dobiju osnovna znanja o pitanjima vezanim za kibernetički kriminal i elektronske dokaze .Osnovna znanja u smislu ovog modela podrazumjevaju:međunarodne stabdarde i njihovu implementaciju u domaće zakonodavstvo (uključujući sudsku praksu), informaciopno komunikacijske tehnologije odnosno računare i računarske mreže sa Internetom kao mrežom mreža, tehničko-tehnološki i zakonski aspekt prikupljanja, čuvanja, korištenja i prezentacije aspekt elektonskih/digitalnih dokaza uključujući integrisani model digitalne forenzičke istrage.

2.4.6. Šta su informacijske i komunikacijske tehnologije?

Informacijska tehnologija (IT) je tehnologija koja koristi računala(hardware i software) za prikupljanje, obradu, pohranu, zaštitu i prijenos informacija. Terminu IT su pridružene komunikacijske tehnologije jer je da nas nezamisliv rad s računalom ako ono nije povezano u mrežu, tako da se govori o informacijskoj i komunikacijskoj tehnologiji (*engl. Information and Communications Technology - ICT).*

S obzirom na složenost pitanja koje je obrađeno kroz ovaj modul, daju se podaci o pojedinim elementima koji čine informacionu tehnologiju, kao što su:

2.4.6.1. Hrdver (Hardware)

Kompjuterski hardver podrazumijeva fizički opipljiv dio računara, odnosno komponente kompjuterskog sistema koje su obično smještene u centralnoj jedinici to jest kutiji kompjutera ili periferno-van centralne jedinice. Hardverske komponente tehnoloških modernih personalnih računarskih sistema su:

a). Kućište – Kutija u kojoj su smješteni osnovni uređaji neophodni za rad kompjutera
b). Napojna jedinica – Skup električnih uređaja koji napajaju kompjuter određenim naponima i jačinama struje
c). Procesor ili CPU – Srce kompjutera koji binarnim sistemom obrađuje instrukcije i upravlja ostalim komponentama sistema
d). RAM (Random Access Memory) memorija – Memorija u kojoj se pišu ili brišu podaci dok je sistem u funkciji. Ovo je nepostojana (volatile memory) vrsta memorije jer se gubitkom napajanja svi podaci smješteni u ovu vrstu memorije gube odnosno brišu.
e). ROM (Read Only Memory) memorija – Podrazumijeva manju količinu memorije koja služi samo za čitanje. Ovo je postojana (non-volatile memory) vrsta memorije smještena u ROM čipu od strane proizvođača te se ne može mijenjati.
f). Ulazno izlazne jedinice
g). Hard disk

- CD/DVD/DHDVD/BD uređaj/i – Uređaj/i za čitanje/pisanje izmjenjivih optičkih medija odnosno diskova pomoću lasera i optičkog sistema različitih brzina. Tu

spadaju Compact Disc ili CD, Digital Video Disc ili DVD, High-Definition/Density DVD ili HD DVD, Blue-ray ili BD
- Floppy disk uređaj – Uređaji za magnetno čitanje/pisanje podataka na floppy diskete veličine 5,25 ili 3,5 inča.
- Mrežna kartica -
- Zvučna kartica – Kompjuterska komponenta koja pretvara digitalne signale u zvuk, zvučne signale ili generiše govor na slušalicama ili zvučnicima.

h). Ulazne jedinice
- Tastatura
- Miš, tačped
- Skeneri
- Bar kod skeneri i slični čitači i senzori (RFID)
- Audio uređaji
- Web kamere
- Digitalne kamere
- Video kamere

i). Izlazne jedinice
- Monitor – Izlazni uređaj koji služi za vizuelni prikaz i komunikaciju i interakciju sa korisnicima
- Matična ploča – Skup štampanih elektronskih kola smještenih u ploči u koju se smještaju i/ili dodatno postavljaju sve ostale komponente sistema a u pojedinim slučajevima ploča može posjedovati integrisane hardverske komponente poput grafičke i/ili mrežne kartice i/ili drugih ulazno-izlaznih priključaka poput USB, Firewire, Thunderbolt, WiFi, Bluetooth, Infrared i drugih.
- Grafička kartica – Izlazni uređaj za pretvaranje digitalnih signala u sliku na monitoru, TV, projektoru ili drugom izlaznim uređajima koji posjeduju Video Graphics Array ili VGA, Digital Video Interface ili DVI, High-Definition Multimedia Interface ili HDMI i/ili druge priključke.
- Štampači
- Ploteri
- Tableti/grafičke table

j). Ostali uređaji za pohranu podataka: ZIP, Jaz,

Hardverski dio kompjutera može ali ne mora imati sve pomenute komponente. U zavisnosti od namjene kompjuterski sistemi su prilagođeni različitim potrebama, te prema obliku i veličini hardver mogu biti u obliku desktop-a sa horizontalnim kućištem, tower-a sa vertikalnim kućištem, laptopa, notebook-a, netbook-a, pocket-a ili džepnog kompjutera, tablet kompjutera poput iPad i Samsung Galaxy Tab.

2.4.6.2. Softver (Software)

Glavna uloga softvera je da prevede korisničke naredbe i zahtjeve u instrukcije poznate procesoru ili CPU, koji nakon izvršavanja instrukcija proizvode određenje rezultate za korisnika. Što znači da softver služi kao prevodilac između korisnika i njegovih zahtjeva i procesora. Po svojoj prirodi softver je veoma kompleksan i obrađuje veoma kompleksne operacije koje premošćuju dva nedostatka. Prvi je pretvaranje programskih jezika bliskih ljudskom (engleskom) govoru u obliku naredbi u mašinski jezik poznat procesoru kompjutera. Drugi nedostatak je procesiranje zahtjeva visokog nivoa kao što jedan običan

dokument ili izvještaj u niži nivo detalja koje obavljaju operacije sa pojedinostima pomenutog izvještaja. Što znači da zahtjevi ili naredbe postavljenje obrađivanje mogu da predstavljaju jedan klik mišem za računar to predstavlja veliku seriju instrukcija koje procesor mora da obradi.

Softver u biti predstavlja skup određenih programa pomoću kojih izvršava kompleksne operacije. Funkcioniše po potrebi kompjuterskog sistema i obično poziva programski kod sa hard diskova i smješta ga u osnovnu memoriju ili RAM i izvršava naredbe kojima produkuje određene korisničke rezultate čiji se izlaz obično prikazuje na monitoru, ili nekim drugim izlaznim uređajima poput štampača ili drugih izlaznih uređaja. Softver dijelimo na aplikativni i sistemski softver.

Aplikativni softver ili program ili popularno zvana aplikacija predstavlja unaprijed snimljeni set instrukcija koje reaguju u zavisnosti od korisničkih zahtjeva ili naredbi. Osnovni primjeri aplikativnog softvera su programi namijeni za finansijsko ili materijalno knjigovodstvo, trodimenzionalno projektovanje, procesiranje audio ili video zapisa, te programi slične prirode. U ovu vrstu takođe spadaju programi poput Microsoft Word, Microsoft Excel i drugi te se nabavljaju kako gotovi proizvodi na tržištu od raznih firmi.

Sistemski softver se sastoji od programa koji obavljaju slijedeće zadatke: podrška aplikativnog softvera pomoću različitih funkcija, alociranje odnosno doznačavanje određenih kompjuterskih resursa aplikativnom softveru, i upravljanje kompjuterskih resursima ili komponentama. Obični primjeri sistemskog softvera predstavljaju operativni sistemi poput Microsoft Windows-a, Mac OS X-a, Linux-a i drugih, zatim sistemi za upravljanje bazama podataka, antivirusni i drugi sigurnosni softveri. Namjena i upotreba sistemskog i aplikativnog softvera predstavlja njihovu osnovu razliku i u biti proizvođači softvera se koncentrišu oko svake grupe posebno prilikom izrade određenih softverskih paketa i kompjuterskih sistema.

2.4.6.3. Računarska mreža

Računarska mreža predstavlja dva ili više međusobno povezanih računara , perifernih uređaja i drugih resursa, s ciljem kvalitetnijeg, efikasnijeg i opertivnijeg korištenja informacija, podataka i raspoloživih resursa[94].Računarska mreža u širem smislu podratumjeva i ostale uređaje kao što su prespojnik (engl.Swich) ili usmjerenik (engl.router).Ti uređaji služe da bi povezali korisnike iste mreže ili korisnike različitih mreža.

2.4.6.3.1. Osnovne komponente računarske mreže

Iz definicije računarske mreže se da zaključiti da mrežu čine računari,periferni uređaji i veze između njih. U mrežama istog prioriteta (peer-to-peer),osnovne komponente su računari i komunikaciona oprema. Kod softverski orjentisanih mreža osnovne komponente su:

a).fajl server-obično je to računar s najvećom procesorskom snagom,velikom RAM memorijom i najvećim i najbržim hard diskovima;
b) radne stanice-računari čija je konfiguracija određena prema poslovima koji se na njima obavljaju;

[94] Vidi www.lecad.unze.ba/nastava/INFORMATIKA/ ,

c). Komunikaciona oprema-razvodna kutija (*hubs*), skretnice (*routers*), kablovi, adapteri, konektori, linijski pojačivači, primopredajnici (transceivers), itd.Ako se radi o bežičnom prenosu signala ,u jednom dijelu mreže za komunikaciju su potrebni još i radio prijemnici i antene.

2.4.6.3.2. Mrežni standardi/Standardi računarskih mreža

Pri projektovanju računarski mreža bitno je voditi računa o standardizaciji i odlučiti se za neki od mrežnih standarda.Organizacija IEEE (Institute of Electrical and Electronics Engineers) je stručna organizacija koja definiše standarde u vezi sa umrežavanjem.Tako da je standard IEEE 802.x[95] najrespektabilniji mrežni standard.

2.4.6.4. Vrsta računarskih mreža

Računarske mreže se uglavnom klasificira prema određenim kriterijima. odnosno karaktersitikama i funkcijama.Najznačajnija među brojnim klasifikacijama je prema kritrerijima kako slijedi:

- kriterij pokrivanja geografskog prostora;
- kriterij tituklara vlasništva nad mrežom;
- kriterij korištene tehnike prijenosa podataka;

2.4.6.4.1. Vrsta računarske mreže prema kriteriju pokrivanja geografskog prostora

Širina pokrivanja geografskog prostora je najčešći korišteni kriterij za grupisanje računarskim mreža.Prema ovom kriteriju ,mreže se dijela na:

- LAN (engl.Local Area Network)-mreže lokalnog područija ili samo lokalne mreže.Ove mreže uspostavljaju se na manjem geografskom prostoru ,koji obično odgovara prostotu na kojem je fizički locirano neko pravno livce ,nekiorganizacioni dio ili neka razmjerno zatvorena funkcionalna cjelina poslovnog sistema.Lokalne meže namjenjene su prvenstveno povezivanju radnih stanica (engl.workstation) opdnosno računara (obično osobnih računara) pomoću kojih zaposlenici obavljaju svaki svoj dio nekog zajedničkog posla.
- MAN (*Metropolitan Area Network*)-gradska mreža, ili računarske mreže koje pokrivaju teritoriju jednog grada.Mreže ovakve vrste pokrivaju radijus do oko 100 km.Rade sa velikom brzinom prenosa podataka (preko 100 Mbps) i mogu da penose i glasovne poruke.
- WAN(*Wide Area Netvork)*-računarska mreža đireg područija,kojeg pokrivaju geografska područija kao što je država,zajednica više država, ioli cijeli kontinent.Ov4e mreže sastoje se od računara raspoređenih na širem području ,kao što je kompleks zgrada nekog fakulteta ,industrijsko postrojenje ,grad,država i slično.Obično sadrži i neku vrstu udaljenih mrežnih mostova ili skretnica ,koji povezuju grupe čvorova telefonskim ili namjenskim linijama,što utiče na smanjenje opsega ovih mreža na LAN mreže.U WAN mreže spadaju:(a) CAN(*Campus Area Network*) mreža univerzitetskog kompleksa.Ova mreža povezuje čvorove pa i lokalne mreže pojedinih odsjeka,instituta,ili istraživačkih

[95] Vidi www.ieee802.org

labaratorija sa velikog broja udaljenih lokacija (b) DAN (*Departmental Area Network*) je mala mreža koja povezuje 20 do 30 čvorova,tako da mogu da se koriste zajednički resursi.Uobičajeno ih imaju:poreske i carinske uprave i druge državne službe uključujući i ministarstva(c) SWAN (Satelit Wide Area Network) je mreža širokog područija realizovana uz upotrebu satelita.

- GAN (*Global Area Network*)-računarska mreža koje prelaze granice država i pokrivaju teritorij više država ,a potencijalno i cijeli svijet.Do prije samo dvadest godina takva ideja se nerijtko smatrala utopijom ,neki gotovo da su je svrstavali u sferu znanstvene fantastike.međutim,ta je zamisao upravo nevjerovatno brzo postala stvarnost,što bjelodano svjedoči o izrazizoj visokoj stopi razvitka mrežne tehnologije.radi se o Internetu „mreži svih mreža“ ili „mreži nad mrežama“ kako se ponekad popularno naziva.
- WWAN(World Wide Area Network)-skup globalnih računarskih mreža koje će pokrivati cijeli svijet i objedinjavati mreže tipa MAN,WAN i GAN.

2.4.6.4.2. Vrsta računarski mreža prema kriteriju titulara vlasništva

S obzirom na način finansiranja izgradnje mreže i na to ko postaje nakon dovršene izgradnje njen vlasnik razlikujemo:

- Javne računarske mreže (eng.Public Network) koje grade državna tijela i agencije,a njihova izgradnja finansira se budžeta.Javnoj mreži u naćelu može pristupiti svako ko za tim ima potrebe, naravno,uz određenu naknadu za korištenje usluga.Sistem naknade za korištenje usluga računarske mreže naziva se mrežnom tarifom.
- Privtne računarske mreže grade i koriste privatne kompanije za svoje potrebe.Najčešće se radi o lokalnim mrežama ,ali nisu rijetki primjeri niti rasprostranjenih mreža u privatnom vlasništvu.Takve mreže,u pravilu,grade velike ,međunarodne kompanije i njihove asocijacije ,a najpoznatije su one u bankarstvu (primjer, mreža SWIFT),u vojnom sektoru (primjer mreža MILNET) i u zračnom prometu(primjer, mreža SITA),itd.

2.4.6.4.3. Vrsta računarskih mreža prema kriteriju korištene tehnike prijenosa podataka

U telekomunikacijama se primjenjujeu različite tehnike prijenosa podataka,odnosno informacija.Za svrhe prijenosa podataka u računarskim mrežama najefikasnijom se pokazala metoda komutacije paketa podataka (*engl.Packet Switching*).Uz njih se , ali u daleko manjoj mjeri, primjenjuju i tehnike komutacije vodova (*engl.Circuit Switching*) te komutacija poruka (*engl.Message Switching*). Bit se komutacije paketa podataka svodi na segmentiranje poruke (informacije) veće dužine.Takav dio poruke naziva se paketom podataka.Segmentiranje poruke u paketu podataka obavlja specijalizirani komunikacijski uređaj-uređaj za pripremu i analizu paketa(engl.Pavket Assembler/Disassembler ili Packet Adjusting Device-PAD),i to tako što djelovima izvorne poruke dodaje neke kontrolne(upravljačke) informacije. U konačnom obliku paket podataka sastoji se od tri dijela: (1) zaglavlje (engl.Header) (2) informacijsko tijelo (engl.Information Body) (3) začelje (engl.Flag).

2.4.6.4. Standardizacija prijenosa podataka u računarskim mrežama

Razlozi zbog kojih treba standardizirati prijenos podataka u računarskim mrežama su:

- Uslovi rada u mrežama različite arhitektire su razlišite pa su različite i metode upravljanja mrežama,
- Različiti računari funkcionišu na različite načine,
- Podaci se mogu iskazivati (formatizirati,kodirati) na razlišite načine,pa se mogu i različito tumačiti(interpretirati).

2.4.6.5. OSI referentni model

U traženje rješenja tih problema međunarodna organizacija za standarde (International Standard Organization, ISO) razvila je koncept tzv.otvorenih sistema(engl.Open System) kao sistema koji su otvoreni za komunikaciju prema svojoj okolini tj.prema ostalim sistemima.Da bi takvi sistemi mogli ostvariti komunikaciju i nesmetano razmjenjivati informacije sa svojom okolinom (ostali sistemi) moraju se pridržavati nekih standarda tj.opštih i zajedničkih pravila ponašanja u radu i komunikaciji.Skup takvih standarda predstavljen je tzv OSI (engl.Open Systems Interconnection) referentnim modelom.To je složen model,a čini ga Sedam slojeva(engl.Layer):fizički sloj, sloj veze, mrežni sloj, sloj prijenosa, sloj razgovora (sesije), prikaza i aplikacije.

2.4.6.6. Komunikacijski protokoli

Komunikacijski protokol je skup pravila za razmjenu informacija između dva uređaja na mreži koji uključuje sintaksu informacija, semantiku informacija te pravila za razmjenu informacija. Komunikacijski protokol možemo uporediti sa komunikacijom dva civilizirana sagovornika. Da bi uspješno razgovarali i razumjeli se treba da koriste isti jezi.Taj jezik koji koriste se sastoji od znakova jezika (sintaksa jezika) i značenja tih znakova(semantika jezika).Pored toga treba da postoje pravila komunikacije i razmjene informacije(jedan govori,a drugi sluša i obrnuto).Veoma slično i sa komunikacijom dva uređaja u računarskoj mreži, da bi mogli komunicirati moraju se koristiti isti protokol odnosno „ pričati istim jezikom“.U računarskim mrežama za uspješno korištenje usluga mreže najčežće je potrebno koristiti više protokola koji rade „zajedno“.Takav skup komunikacijskih protokmola koji omogučavaju komunikaciju između najmanje dva uređaja naziva se komunikacijska arhitektira.[96] Konkretizacija standarda za svaki sloj su tzv.komunikacijski protokoli(engl.Communication Protocol),koji predstavlja skup propisa o osobinama koje sistem mora imati da bi se mogao smatrati otvorenim.Zbog brojnih neslaganja među zainteresovanim stranama ,zbog sukoba interesa proizvođaća opreme ,pružatelja mrežnih usluga i korisnika ,a nerijetko i zbog pomanjkanja političke volje,još uvijek nisu razvijeni protokoli za sve nivoe OSI referentnog modela.

2.4.6.7. Uređaji za povezivanje mreža različitih arhitektura

Implementacijom OSI referentnog modela i odgovarajućih komunikacijskih protokola u obliku odgovarajućih komunikacijskih programa,omogućava se povezivanje dvaju ili više otvorenih sistema.Ako se pri tome radi o mrežnim sistemima različitih arhitektura ,na njihovim će se spojevima morati instalirati određeni posrednički ili spojni uređaji,koji će omogućiti nesmetan protok podataka među mrežama,ali istio tako i štiti svaku pojedinu

[96] Vidi www.carnet.hr

mrežu od neželjenih „posjeta“ izvana. Najčešće se radi o povezivanju lokalnih mreža međusobno ili o povezivanju lokalnih i rasprostranjenih mreža.Ovisno o karaktersitikama mreže,o zahtijevima prometa podataka i složenosti korištenih aplikacija, koristiti će se neki od slijedećih spojnih uređaja: (1) mostovi (2) usmjerenici (3) pristupnici.

2.4.6.7.1. Mrežni premosnik/most

Most(engl.Bridge) je uređaj koji povezuje računarske mreže na drugom sloju OSI referentnog modela.Ovaj spojni uređej ima memoriju u kojoj održava tablicu adresa računara koji pripadaju „njegovoj“ lokalnoj mreži.Kada iz okoline mreže naiđe neki niz paketa podataka ,most kontroliše odgovaraju li adrese odredišta navedene u paketima adresi ili adresama jednog ili računara u toj lokalnoj mreži.Ako je tako ,most izdvaja takve pakete iz niza nadolazećih paketa ,što se naziva postupkom filtriranja (engl.Filtering), i upučuje ih odredištu.

2.4.6.7.2. Mrežni usmjrenik

Usmjernik (engl.Router) je najvažniji od svih mrežnih uređaja.Usmjerenik je mrežni spojni uređaj koji ima saznanja o dostupnosti svih djelova mreže. Međutim, takvi su uređaji prilagođeni obavljanju funkcija mrežnog (trećeg) sloja OSI referentnog modela.Oni su zato specifični s obzirom na mrežni protokol, što znači da“poznaju“ samo protokol mreže čiji su sastavni dio.Usmjernici stoga mogu poslužiti kao svojevrsni odbrambeni („vatreni“) zid (engl.Firewall),koji „svoju“ mrežu štiti od paketa podataka generiranih u skladu s nekim njemu i mreži nepoznatim komunikacijskim protokolom.

2.4.6.7.3. Mrežni pristupnik/poveznik

Pristupnik ili poveznik[97] (*engl.Gateway*) je uređaj koji se koiristi kod priključivanja lokalnih mreža na neku od velikih rasprostranjenih mreža.Funkcija pristupnika je predstavljanje uređaja lokalne mreže prema rasprostranjenoj mreži na jedinstven (unificiran) način.On, dakle, pretvara pakete podataka formirane prema protokolu lokalne mreže u paketu koji odgovaraju protokolu rasprostranjene mreže i obrnuto.Taj postupak se naziva emulacijom(engl.Emulation)[98].

Pored navedenih mrežnih uređaja netreba zaboraviti nivrlo važne uređaje mrežne uređaje i njigbhove funkcije kako slijedi:(a) Repeater (ponavljač, obnavljač) b). HUB (koncetrator, zvjesdište) c). Switch (preklopnik, prespojnik) (d) Access point (pristupna tačka) (e) Firewall (vatrozid) (f) Modem (Modulator-Demodulator)

2.4.6.8. Internet

Internet je popularno zvana mreža svih mreža, što u biti i jeste. Internet je globalna kolekcija mreža koje su spojene sa TCP/IP. Neodvojivi dio interneta je World Wide Web (WWW) ili skraćeno web koji predstavlja skup programa, datoteka, i servisa kojima se može pristupiti preko interneta i standardnih protokola, kao sto su Hypertext Transfer Protocol (HTTP).

Internet je svjetska decentralizirana računarska informacijska mreža,sastavljena od velikog broja manjih međusobno povezanih računarskih mreža,koja omogućava prenos informacija

[97] Vidi www.informatika.bdzdo.com/s922.htm-Hrvatska,
[98] Vidi www.magabajt.org/rješnik/emulacija/

između računara koji čine mrežu. To je „mreža svih mreža“koja se sastoji od brojnih kučnih,poslovnih, akademskih, vladinih, nevladinih i drugih mreža koje međusobno razmjenjuju informacije i usluge kao što su elektronska pošta, prenos datoteka,chat,povezane stranice i dokumente world wide weba.

U samim početcima Internetom se služila ograničena i privilegirana grupa ljudi radi potrebe razmjene uglavnom naučnih informacija.Pojavom prvih Internet preglednika, korištenje Interneta i razmjena informacija je postalo vrlo jednostavno i široko dostupna.Ta je obezbijedilo nagli porast broja korisnika Intermneta, a time i porast broja informacija na Internetu.Nakon toga je uslijedio enormno brzi razvoj Internete do nivoa kakvog danas poznajemo.Opredmećena ideja otvorenosti,dostupnosti i fleksibilnosti su osigurale Internetu današnju poziciju. Danas Internet obuhvata širok spektar informacijskih resursa i usluga preko kojih se pretvorio u medij koji je do početka 21.vijeka uveo korjenite promjene na području informisanmja, komunikacija, trgovine, bankarstva, plaćanja, zabave i drugim područjima ljudskog djelovanja.

Međutim ,zajedno sa svim benefitima Internet je potaknuo i omogućio aktivnosti koje su štetne po društvo.Kriminalci su takođe u mogućnosti da pristupe i koriste Internet u svoju korist kako bi im olakšao život na jednoj strani i poslužio pri počinjenju krivičnih djela i otvorio mnoge mogućnosti na tom polju na drugoj strani .I ne samo to, Internet je generisao nekoliko novih krivičnih djela i prouzrokovao brojne promjene u načinu obavljanja postojećih krivičnih djela.

Internet je gotovo eliminirao potrebu fizičkog prisustva klijenta u banci prilikom otvaranja računa i obavljanja finansijskih transakcija i tako izložio bankarski sistem prema brojnim rizicima i nada sve nezakonitim aktivnostima pojedinaca i grupa.Kriminalci uz smanjeni rizik, sve više su u mogućnosti legitimiraju nezakonito stečen prihod koristeći blagodeti anonimnosti Interneta kroz kreiranje lažne identitete , zloupotrebljavajući ukradene identitete, krađa platnih kartica i sl..

Na temelju statistika brojnih zemalja koje su objedinili naučnici i brrojne međunarodne organizacije može se udstvrditi da su se značajno modificirale tipologije pranja novca na globalnoom nivou od pojave Interneta.Tako da se pranja novca dans uglavnom obavlja kroz internet i korespodentno bankarstvo,smart kartice,digitalnu gotovinu ,on-line kockarince,on-line aukcije i sl.Nažalost napredak i mogućnosti Interneta neprate brze promjene u sferi donošenja, primjene i provođenja zakona.Policija kao i pravosudni organi su reaktivni i duboko konzervativne institucije koje vrlo sporo reagiraju na b rze i revolucionarne promjene.Ako se ovome doda da su kriminalci već poodavno spoznalida moraju pratiti tehnološki razvoj te nerijetko prilikom osmišljavanja i realizacije složenih operacija pranja novca koje imaju transnacionalna obilježja koriste expertna znanja .,a experte iz raznih oblasti(finansijski menađeri, računovođe,informatičari,pravnici i sl) privlače enormionim zaradama.

“Internet” u izvornom obliku označava globalnu, svjetsku zbirku/kolekciju računarskih mreža povezanih na dogovornoj osnovi koje među sobom podatke razmjenjuju Internet protokolom. To je protokol iz trećeg sloja OSI modela čiji se podaci prenose bilo kojim protokolom drugog sloja. Zato je moguće povezivati raznorodne mreže. Posebno je važno da se jednako koristi za lokalne (LAN) kao i za globalne (WAN) mreže. Ta jednoobraznost istovjetna je i za programe i za ljude.

Podaci se u Internetu prenose IP datagramima, no korisnički programi uglavnom koriste User Datagram Protocol (UDP) ili Transport Control Protocol (TCP) čiji se podaci onda prenose IP datagramima. Na toj se, pak, osnovi gradi čitav niz specijaliziranih protokola poput: SMTP, SNMP,TELNET, FTP, HTTP i dr.

Svaki računar u Internetu ima jedinstvenu Internet adresu, koje se grupiraju u mrežne adrese određene klase. Ljudi koriste Internet imena koje u numeričke adrese pretvara Domain Name Service (DNS). Brojni čvorovi u Internetu spajaju dvije ili više mreža. Takvi se čvorovi zovu "gateway" i u njima se donosi odluka kojim putem proslijediti pojedini paket podataka. Odluka ovisi propusnosti i zagušenosti veza, cijeni prijenosa, vrsti paketa i sl. Taj se proces zove "routing", za razliku od procesa drugog OSI sloja koji koristi tehniku preklapanja paketa.

Internet, dakle, nije ni pravna osoba, ni tehnička infrastruktura, već samo dogovor.Internet nema vlasnika, pa ni upravno tijelo. Vlasništvo postoji samo nad pojedinim dijelovima Interneta, nad pojedinim mrežama koje ga čine. Njima pripadaju i međusobne veze za povezivanje mreža. Internet nema hijerarhiju, ni u tehnologiji, ni u infrastrukturi ni u organizaciji. Tako hijerarhije nema ni u pojedinim zemljama, pa nekoliko sasvim odvojenih mreža iz jedne zemlje može biti različitim putovima povezano drugim s mrežama koje su u Internetu. Obično se sve mreže unutar jedne zemlje međusobno povezuju, ali to je zbog smanjenja međunarodnih telekomunikacijskih troškova, a ne zbog toga što bi to Internet na bilo koji način od njih zahtijevao.

Kako računala povezana u Internet moraju imati jedinstvene adrese, a slično je i s nazivima koje koriste ljudi, nužna je neka središnja organizacija za koordinaciju. To su IANA (Internet Assigned Numbers Authority) i Internic (Network Information Center) koji izdaju adresne opsege organizacijama koje to od njih zatraže. Internet Activities bord (IAB) i Internet ???ngineering Task Force (IETF) okupljaju ljude koji i dalje razvijaju Internet. Zanimljivo je da ta najviša tijela u Internetu zapravo nitko ne postavlja i ne nadzire..

2.4.7. Cyber kriminal i digitalni dokazi

Korištenje informaciono komunikacione tehnologije u krimimnalne svrhe zbog svoje specifičnosti zahtijeva i posebnu metodologiju za vođenje kriminalističke istrage.Digitalni dokazi su osjetljivi,lako se brišu i mjenjaju,a time i kompromituju.Posebni forenzički alati omogučavaju povrat i analizu brisanih, skrivenih i privremenih datoteka.S obzirom na činjenicu

2.4.8. Procedure i principi prikupljanja digitalnih dokaza

Na zasjedanju Kompjuterskih specijalista (Internacionalna asocijacija kompjuterskih specijalista) u Portlandu-Oregon(1991),jedan od osnovnih zaključaka je bio da su digitalni dokazi jednake vrijednosti kao i opipljivi dokazi.Nakon toga 1996. godine propisane su procedure i opći principi koji se odnose na digitalne dokaze u cilju međunarodne razmjene ovih dokaza.

Osnovni principi su:

- ✓ u radu sa digitalnim dokazima se moraju primjenjivati striktne procedure i principi
- ✓ digitalni dokaz ne smije da bude izmijenjen prije, u toku uzimanja ili poslije uzimanja dokaza
- ✓ digitalnom dokazivanju može da pristupi samo dobro obučena osoba (sudski vještak – forenzičar)
- ✓ svaka aktivnost mora biti dobro i detaljno dokumentirana.

Razvili su se izvjesni principi digitalne forenzike, kao npr:

1. svaka aktivnost mora biti provedena na osnovu naloga suda
2. svi dokazi moraju biti potpuni i moraju dopunjavati jedan drugog – ne smije se isključiti ni jedan digitalni dokaz
3. princip čuvanja digitalnog dokaza ukazuje da se digitalni dokaz ne smije mijenjati ni po koju cijenu. To znači da se mora sačiniti forenzička kopija dokaza i izvršiti osiguranje medija od uništenja
4. mora se izvršiti tačna identifikacija medija koji se kontroliše
5. istraga se mora voditi poznatim metodama, poznatim alatima, alatima koji su licencirani i o kojima postoji dokumentacija, kako bi se eventualno moglo provjeravati kako rade
6. sačinjavanje konciznog izvještaja
7. prezentiranje sudu

2.4.9. Integrisani model digitalne istrage

Dok su digitalne fotrezničke istrage tek skoro postale uobičajene,fizičke istrage postoje već više stotina godina i iskustva iz njih se mogu primjeniti i na digitalni svijet kriminala.Integrisani model digitalne istrage u sebi sadrži istragu fizičke scene zločina(mjesto na kojem se zločin dogodio) sa istragama digitalne scene zločina s ciljem identifikacije osobe-a koje su odgovormne i za nedozvoljenu digitalnu aktivnost.

2.4.9.1. Forenzika

Forenzika je riječ nastala od latinskog pridjeva forensis ("pred forumom", odnosno, grubo prevedeno, "pred sudom")[99].

Forenzička nauka ili skraćeno forenzika je primjena različitih naučnih disciplina u svrhu rješavanja sudskih ili pravnih pitanja.

2.4.9.1.1. Digitalna forenzika

Digitalna forenzika je forenzička disciplina koja se bavi razvojem rješenja i softvera koji u službi forenzičkih ispitivanja (pribavljanja dokaza krivičnog djela).

Osnovna definicija digitalne forenzike je tehnološka, sistematska kontrola digitalnih nosilaca podataka i njihovog sadržaja u cilju prikupljanja dokaza krivičnog djela ili druge zloupotrebe za koje je digitalni uređaj korišćen. Iz ovoga proizilazi da se digitalna forenzika odnosi na sve

[99] Vidi http://sh.wikipedia.org/wiki/Forenzika

vrste elektronskih medija (CD, DVD, USB, mobilni telefoni i digitalni aparati i digitalne kamere i dr), provjera e-mail poruka, JPG snimaka i sl.

Iako u teoriji ima mnogo različitih pristupa, digitalnu forenziku možemo podijeliti na kompjutersku forenziku, mrežnu forenziku, forenziku baze podataka i forenziku mobilnih uređaja.

Digitalna forenzika se koristi kako bi se utvrdilo postojanje kaznenih predmeta (npr. kod optuživanja za dječju pornografiju, kod utvrđivanja postojanja terorističkih djela), ali i u parnicama, npr. kod korporativne špijunaže, kao i zloupotreba u radu zaposlenika. U inostranstvu su sve češći slučajevi provođenja dokazivanja putem digitalne forenzike u cilju utvrđivanja varanje supružnika.

Najbitnije je, koristeći priznate i poznate metode digitalne forenzike, dokazati postojanje radnji koje predstavljaju osnove za dalja postupanja pred pravosudnim organima.

Cilj digitalne forenzike jeste da se pronađu digitalni tragovi na osnovu kojih ćemo saznati šta, kada, sa kim, kako i zašto je neko nešto radio koristeći digitalni uređaj.

2.4.9.1.2. Digitalni dokaz

Digitalni dokazi su informacije pohranjene, primljene ili poslane sa elektronskog uređaja i prikupljene u istražnom postupku te kao takve imaju veliki značaj u procesu dokazivanje kriminalnog djela. Digitalni dokazi mogu poslužiti kao i dokazi prikupljeni klasičnim istražnim postupcima:

- Skriveni su, poput otisaka prstiju ili DNK dokaza.
- Dokazi ove prirode brzo i lako prelaze granice nadležnosti
- Podložni su izmjenama, oštećenjima, uništavanju
- Vremenski su osjetljivi

Digitalni dokazi mogu da sadrže i fizičke dokaze kao DNA, otisak prstiju, ili serologiju. Fizički dokazi trebaju da se zadrže zbog mogućeg pretraživanja[100].

2.4.9.2. Prijem i procesiranje forezničkog zahtijeva

Prema odredbi člana 289. ZKP FBIH, dokaz je orginalni dokumenat. Izuzetno, kao dokaz se može koristiti i ovjerena kopija originala, kao i kopija koja je potvrđena kao neizmijenjena u odnosu na original.

Iz ovoga proizilazi da je valjan dokaz samo ako se može izvršiti upoređivanjem sa originalom, a to znači da kopirani disk, samostalno nije dokazno sredstvo, ali kopirani disk koji se može uvijek uporediti sa originalnim diskom, sačinjavajući novu, identičnu kopiju, mora predstavljati valjano dokazno sredstvo.

Zbog toga, u forenzičkoj laboratoriji se rade kopije diskova, po sistemu „svaki bit (dio) se kopira“. To se najčešće radi koristeći programe ENCASE, Norton Ghost, Byte back, Autopsy

[100] Izvor: http://www.nij.gov/nij/pubs-sum/219941.htm, Electronic Crime Scene Investigation A Guide for First Responders, Second Edition by National Institute of Justice, April 2008

itd. EnCase Forensic, proizvod kompanije Guidance Software, je industrijski standard u digitalnoj forenzici i istrazi. Sistemima firme Guidance Software koristi se 90 posto svih američkih istražitelja, te niz vladinih i vojnih institucija

Tu je vrlo važno voditi računa da se tim kopiranjem ne izvrše promjene na originalu, te da se prilikom provjeravanja od strane npr. odbrane, dobiju isti podaci.

Prije samog kopiranja mora se izvršiti blokiranje rada računara, postavljanjem tzv. writer blokera.

Za sigurno podizanje računara, te kako bi se izbjegli neželjeni efekti pokretanja računara sa programom koji je na računaru, koriste se tzv. live CD-a koji imaju programe za podizanje i početak rada računara i onda se takvi programi koriste za normalan forenzički rad.

2.4.9.3. Upravljanje istragom

Kada se zahtjev za forenzičko ispitivanje odobri, kriteriji, prioriteti i dodjele zadataka ispitivanja bi trebala bi biti uspostavljeni i implementirani. Kriteriji mogu uključivati prirodu kriminala koji se istražuje, datum sudskog procesa, vremenski rokovi, potencijalne žrtve, pravni razlozi, nepostojana (volatile) priroda dokaza, i resursi na raspolaganju.

2.4.9.3.1. Rukovanje i zadržavanje dokaza

Potrebno je napraviti pravilnike za primanje, procesuiranje, dokumentaciju, i rukovanje dokaza kao i alati koji su korišteni za ispitivanje. Pravilnik treba da bude u skladu postojećim pravilnicima istražnog odjela. Ponekad kriteriji za rukovanje digitalnim dokazima i njihovo zadržavanje može biti iznad postojećih pravila istražnog odjela.

Vrlo je važno zapamtiti da druge forenzičke discipline mogu otkrivati ostale dokaze, poput otisaka prstiju na hard disku, vlasi kose ili vlakana na tastaturi i na ručno pisanim nazivima na diskovima ili štampanom materijalu. Za ovakve slučajeve, potrebno je imati propisane procedure koje određuju redoslijed i načine kako bi trebalo pristupiti ispitivanju dokaza, kako bi se izvukla potpuna vrijednost dokaza.

2.4.9.3.2. Procesno ispitivanje

Standardne Operativne Procedure (SOP) moraju biti uspostavljene za zadržavanje i procesuiranje digitalnih dokaza. SOP trebaju biti dovoljno uopštene da se odnose na osnovne korake u rutinama forenzičkih ispitivanja dok pružaju fleksibilnost za postupanje po jedinstvenim i nepredvidivim situacijama koje se mogu pojaviti.

2.4.9.3.3. Razvijanje tehničkih procedura

Uspostavljanje procedura treba da definiše tehnički proces za ispitivanje dokaza. Procedure je potrebno testirati prije njihove implementacije kako bi istražni rezultati bili validni i nezavisno reprodukovani. Koraci u razvoju i tačnost procedura treba da se dokumentuje i uključi:

- Definiše zadatak ili problem
- Predloži moguće rješenje

- Testira svako rješenje na poznatu kontrolu uzorka
- Ispitati rezultate testa
- Finalizirati procedure

Prilikom razvijanja procedura ni u kojem slučaju se ne smije koristiti originalni dokaz[101].

2.4.9.3.4. Ispitivanje dokaza

2.4.9.3.4.1. Princip

Digitalni dokaz je potrebno detaljno ispitati u skladu sa obimom i ciljevima istrage čime bi se odredili slijedeći koraci u istrazi.

2.4.9.3.4.2. Procedura

Provesti detaljno ispitivanje počevši od istražnog naloga ili drugih pravnih odobrenja, detalja istražnog slučaja, prirode hardvera i softvera, dostupnih potencijalnih dokaza, i okolnosti pod kojim se oduzeti dokaz treba ispitati.

2.4.9.3.5. Proučavanje istražnog slučaja

- Razmotriti zahtjev od nadležnog tužitelja ili ovlaštene službene osobe

    - Definisati potrebne pravne dozvole za izvršenje forenzičkog zahtjeva
    - Uvjeriti se u kompletnost zahtjeva za saradnju
    - Kompletirati dokumentaciju posjedovanja ili primopredaje dokaza.

- Konsultovati sa tužiocem odgovornim za istragu oko istražnog slučaja i upoznati ga ili šta forenzičko osoblje može ili ne može otkriti. Prilikom razgovora sa istražiteljima o činjenicama istražnog slučaja, treba obratiti pažnju na slijedeće:

    - Utvrditi da li uraditi druga forenzička ispitivanja nad dokazima (poput DNK analize, otisaka prstiju, tragova alata, tragova, i spornih dokumenta).
    - Utvrditi mogućnosti kretanja istrage ka drugim načinima istrage kako bi se obezbijedili dodatni digitalni dokazi (poput zahtjeva za dodatne informacije od strane internet servis provajdera (ISP), kako bi se identifikovale daljinske lokacije za pohranu podataka, nabavke e-maila).
    - Razmotriti važnost perifernih komponenti za istragu. Na primjer, istražni slučajevi poput falsifikovanja ili prevare razmotriti ostale uređaje koji ne spadaju u kompjutersku opremu, poput laminatora, neispunjenih/čistih kreditnih kartica, papira za čekove,skenera i štampača. U istražnim slučajevima dječija pornografije pregledati digitalne kamere.
    - Odrediti potencijalni dokaz koji se traži (primjeri fotografije, tablične podatke (spreadsheets), dokumente, baze podataka, finansijske podatke.
    - Odrediti dodatne informacije vezanih na istražni slučaj (kao dodatna imena (aliases), e-mail računi, e-mail adrese, korišteni ISP, imena, konfiguracija mreže i korisnika, sistemski zapisnici (logs), lozinke, korisnička imena). Ove informacije

[101] Izvor: http://www.nij.gov/nij/pubs-sum/199408.htm, Forensic Examination of Digital Evidence: A Guide for Law Enforcement by National Institute of Justice, April 2004

mogu se dobiti kroz intervjue i razgovore sa sistemskim administratorima, korisnicima, ili radnicima.
- Ispitati nivo vještina upletenih korisnika kompjutera. Tehnike korištene od strane vještih korisnika za skrivanje ili uništavanje dokaza mogu biti sofisticirane (kao šifrovanje (encryption), zamke, steganografija).
- Odrediti prioritet i redoslijed kojim se dokazi moraju ispitivati.
- Odrediti da li će biti potrebno dodatno osoblje.
- Odrediti opremu koja će biti potrebna.

Ispitivanje može otkriti dokaze koji se odnose na kriminalne aktivnost (kao pranje novca povezano sa narkotičkim aktivnostima).

2.4.9.3.6. Razmatranje lica mjesta

Slijedeći materijal ne obezbjeđuje kompletnu informaciju za ispitivanje digitalnih dokaza, nego je generalni vodič za istražne službe koje ispituju digitalne dokaze na licu mjesta.

Razmotriti bezbjednost i zaštitu osoblja na licu mjesta. Uvijek se pobrinuti da je lice mjesta pravilno obezbijeđeno prije i tokom istraživanja.

U pojedinim slučajevima, istražitelj može biti jedina osoba koja ima priliku da na licu mjesta uradi slijedeće:

- Identifikuje broj i tip kompjutera
- Utvrdi da li je prisutna mreža
- Ispita i intervjuiše sistemske administratore i korisnike
- Identifikuje i dokumentuje tipove i veličine medija, uključujući izmjenjive medije. Dokumentovati mjesta ili lokacije sa kojeg se mediji uzimaju.
- Identifikovati pohrane podataka na licu mjesta i/ili udaljenim kompjuterskim lokacijama.
- Identifikovati vlasništvo softvera
- Utvrditi generalno stanje na licu mjesta
- Odrediti operativne sisteme

Odrediti ako je neophodan kontakt eksternih resursa, po potrebi. Uspostaviti i posjedovati telefonsku listu vezanih za resurse.

2.4.9.3.7. Procesuiranje istražnog mjesta

Pregledati dokaze radi utvrđivanja mjesta istrage. Prednost dati ispitivanju u kontrolisanoj okolini, poput forenzičkog radnog prostora ili laboratorije. Kada okolnosti nalažu ispitivanje na istražnom mjestu, pokušati obezbijediti kontrolisanu okolinu. Prilikom utvrđivanja razmotriti:
- Vrijeme koje je potrebno da bi se ispitivanje kompletiralo
- Pitanja logistike i osoblja u slučaju dužeg zadržavanja
- Prikladnost opreme, resursa, medija, treninzi, i iskustvo za ispitivanje istražnog mjesta

2.4.9.3.8. Pravne okolnosti

- Odrediti granice ovlaštenja za ispitivanje
- Razmotriti moguće situacije koje se odnose na ostale zakone, statute, pravilnike, i procedure.

Ako mjesto na kojem se dokaz nalazi nije naznačeno u dozvoli za istragu, utvrditi dodatne pravne procese koji mogu biti potrebni za nastavak istrage (dozvola za istragu, forme za dodatna odobrenja).

2.4.3.9. Ispitivanje dokaza

- Napraviti prioritet nad dokazima (npr. distribuciju CD-ova prije korisnički kreiranih CD-ova)
    - Mjesto gdje je dokaz pronađen
    - Stabilnost medija koji se ispituje
    - Odrediti način dokumentovanja dokaza (npr. fotografisanje, skice, bilješke)
    - Utvrditi mjesto za skladištenje zbog elektromagnetne interferencije
    - Utvrditi stanje dokaza rezultirano od pakovanja, transporta, i skladištenja
    - Utvrditi potrebu za neprekidno napajanje električnom energijom za baterijske uređaje

Okvirne procedure su bazirane na osnovu opšte prihvaćene prakse[102]. Posebno konsultovati agencije i tražiti savjete, ako je potrebno, prije početka ispitivanja. Stvarna istraga može zahtijevati alternativne korake pored ovdje nabrojanih. Ispravno ispitivanje je temelj za ostale procedure.

2.4.3.10. Pribavljanje dokaza

2.4.3.10.1. Princip

Digitalni dokazi, po svojoj prirodi, je lomljiv i može se izmijeniti, oštetiti, ili uništiti nestručnim rukovanjem ili ispitivanjem. Zbog ovih razloga posebne korake je potrebno preduzeti kako bi se sačuvao ovaj top dokaza. Pogrešno pristupanje može uzrokovati neupotrebljivost ili dovesti do pogrešnog zaključka.

2.4.3.10.2. Procedure

Preuzeti originalne digitalne dokaze na način koji štiti i zadržava dokaze, uključujući osnovne korake:

- Osigurati digitalni dokaz u skladu sa službenim pravilnikom. U slučaju nepostojanja službenog pravilnika poslužiti se drugim procedurama ili pravilnicima.
- Dokumentovati konfiguraciju hardvera i softvera na sistemu kojim se vrši ispitivanje
- Provjeriti ispravnost kompjuterskog sistema pomoću kojeg se vrši ispitivanje, uključujući hardver i softver
- Rastaviti kućište kompjutera koji se ispituje kako bi se omogućio fizički pristup uređajima za pohranu podataka

[102] Izvor: http://www.nij.gov/nij/pubs-sum/199408.htm, Forensic Examination of Digital Evidence: A Guide for Law Enforcement by National Institute of Justice, April 2004

- Pobrinuti se da je oprema zaštićena od statičkog elektriciteta i magnetnih polja

- Identifikovati uređaje za pohranu podataka koje treba izvaditi. Ovi uređaji mogu biti interni, eksterni ili oboje.
- Dokumentovati interne uređaje i hardversku konfiguraciju
  - Stanje uređaja (npr. Proizvođač, model, geometriju, veličinu, spojene pinove pomoću džampera, mjesto, priključak uređaja
  - Interne komponente (npr. zvučna kartica, video kartica, mrežna kartica, uključujući MAC (Media Access Control) adresu, PCMCIA (personal computer memory card international association) karticu/e).

- Isključiti uređaje za pohranu podataka (korištenjem kabla za napajanje ili kabla za podatke sa zadnjeg dijela uređaja ili sa matične ploče) kako bi se spriječilo uništenje, oštećenje, ili izmjena podataka.
- Očitati informacije o konfiguraciji sa sistema koji se ispituje kroz kontrolirano butanje (boot)
  - Uraditi kontrolisano butanje za očitavanje CMOS/BIOS informacija i testirati funkcionalnost
    - Sekvenca butanja (ove radnje mogu značiti izmjenu BIOSa kako bi utvrdilo butanje sistema sa floppy-ja ili CD-ROM uređaja)
    - Vrijeme i datum
    - BIOS lozinke
  - Uraditi drugo kontrolisanje butanje radi testiranja kompjuterske funkcionalnosti i forenzičkog diska za butanje
    - Potvrditi da su strujni i kabl za podatke ispravno spojeni na floppy ili CD-ROM uređaj, i potvrditi još jednom da su strujni i kabl za podatke sa uređaja za pohranu podataka odvojeni
    - Ubaciti forenzički disk za butanje u floppy ili CD-ROM uređaj. Butati kompjuter i potvrditi da li kompjuter vrši butanje pomoću forenzičkog diska za butanje.
  - Ponovo spojiti uređaje za pohranu podataka i uraditi treće kontrolisano butanje kako bi se očitale informacije o konfiguracijama uređaja za pohranu podataka u CMOS/BIOSu.
    - Potvrditi da se forenzički disk za butanje nalazi u floppy ili CD-ROM uređaju kako bi se spriječilo butanje kompjutera sa uređaja za pohranu podataka.
    - Informacije o konfiguracijama uređaja za pohranu podataka uključuje LBA (logical block addressing), veličina diska, cilindri, glave, i sektori (CHS), ili auto-detekcija
  - Isključiti sistem
  - Kada se ukaže prilika, izvaditi uređaje za pohranu podataka koji se ispituju i pristupiti pribavljanju dokaza koristeći sistemom za ispitivanje. Prilikom spajanja uređaja sa kojeg se pribavljaju dokazi na sistem za ispitivanje, konfigurisati uređaj kako bi bio prepoznat
- Izvanredne okolnosti, uključujući slijedeće, mogu uticati na promjenu odluke o vađenju uređaja sa kojeg se pribavljaju dokazi sa sistema koji se ispituje:
  - RAID (redundant array of inexpensive disks). Vađenje diskova i ispitivanje neće pomoći dobijanju upotrebljivih rezultata.
  - Laptop sistemi. Pristup sistemskom uređaju može biti otežan ili može postati neupotrebljiv ako se skine sa originalnog sistema.

  - Hardverska zavisnost (za nasljedne (legacy) sisteme). Stariji uređaji mogu bit neupotrebljivi na novim sistemima.
  - Dostupnost opreme. Istraživačko osoblje nema pristup potrebnoj opremi.
- Mrežna pohrana podataka. Ukazana potreba za korištenje mrežne opreme da bi se pristupilo podacima.

Kada se koristi oduzeti kompjuter za prikupljanje dokaza, priključiti uređaj za pohranu podataka sa kojeg se prikupljaju dokazi i priključiti uređaj za pohranu podataka koji se ispituju (npr. hard disk, uređaj za traku (tape drive), CD-RW, MO (magnetno-optički)).

- Potvrditi da je uređaj za pohranu podataka za ispitivanje forenzički čist kada se prikupljaju dokazi.

Zaštitu od snimanja je potrebno inicirati, ako je dostupan, radi zadržavanja i zaštite originalnih dokaza.

Istraživačko osoblje treba da razmotri važnost dokaza koji se ispituju prije prikupljanja dokaza (npr. izvođenje nezavisne CRC (independent cyclic redundancy check) provjere, hashing). Zavisno od izabranog metoda za prikupljanje, ovaj proces je moguće da je već kompletiran.

- Ako se koristi hardverska zaštita za snimanje:
  - Instalisati uređaj za zaštitu snimanja
  - Butati sistem sa kontrolisanim operativnim sistemom za ispitivanje
- Ako se koristi softverska zaštita:
  - Butati sistem sa kontrolisanim operativnim sistemom za ispitivanje
  - Aktivirati zaštitu snimanja
- Provjeriti geometriju svih uređaja za pohranjivanje podataka i utvrditi da li se poklapa sa cijelim diskovnim prostorom, uključujući host-zaštićene dijelove sa podacima. (npr. za uređaje suprotne od host sistema, da li podaci poput particionih tabela odgovaraju fizičkoj geometriji uređaja).
- Zabilježiti elektronski serijski broj uređaja i druge korisnički-dostupne, host vezane, podatke.
- Prebaciti dokaze koji se ispituju na uređaj za pohranu podataka u istražnom sistemu korištenjem odgovarajućeg softverskih ili hardverskih alata poput:
- Samostalni softver za dupliranje
- Forenzički komplet softvera za analizu
- Namijenjenih hardverskih uređaja
- Verifikovati uspješnost preuzimanja poređenjem poznatih vrijednosti originala i kopije ili poređenjem sektor-po-sektor originala sa kopijom[103].

Kopiranje precizne kopije diska kod nas se generalno naziva “gostovanje” po popularnom Norton Ghost programu. U pitanju je zabluda vezana za preciznost kojom Nortonova aplikacija kopira podatke. Naime u forenzičke svrhe neophodna je identična kopija diska. Identična kopija podrazumijeva identičan raspored i sadržaj klastera (eng. cluster) na disku, čak i oni koji nemaju nikakav sadržaj moraju se vjerodostojno prenijeti na novi disk. Prva stvar koju moramo znati je da je nephodno imati čist disk kao destinaciju za duplikat. Čist disk podrazumjeva onaj disk čiji je cjelokupan sadržaj ispisan nulama. Potpuna je zabluda da je to fabrički novi disk. Takav, novi disk u pravilu nije čisti disk. Naime,u procesu testiranja

[103] Izvor: http://www.nij.gov/nij/pubs-sum/199408.htm, Forensic Examination of Digital Evidence: A Guide for Law Enforcement by National Institute of Justice, April 2004

fabrike upisuju nasumične bitove u pojedine sektore ne bi li na taj način testirali sam kvalitet medija kao i ispravnost tzv. translacionog algoritma (ovaj algoritam se odnosi na prevođenje logičkih (LBA) u fizičke (CHS) adrese prilikom smještanja i čitanja podataka). Dakle, čak i novi diskovi moraju biti podvrgnuti čišćenju/uništavanju podataka prije nego što se krene sa pravljenjem precizne kopije.

Drugi problem se javlja u načinu kopiranja podataka. Da bi postigli određene performanse, svi moderni diskovi će podatke koji im se serviraju upisivati redom. Međutim za forezničare je najbitnije očuvanje redoslijeda i rasporeda podataka i zato je nephodno korištenje bitstream aplikacija. Kopija sačinjena na opisani način je identična originalu i fizički i logički.

2.4.3.11. Ispitivanje dokaza

2.4.3.11.1. Princip

Prilikom ispitivanja digitalnog dokaza koriste se opšti forenzički principi. Različiti tipovi istražnih slučajeva i mediji mogu zahtijevati drugačije metode ispitivanja. Istražno osoblje koje provodi ispitivanje nad digitalnim dokazima mora biti trenirano za ove svrhe.

2.4.3.11.2. Procedure

Provesti ispitivanje nad podacima koji su prikupljeni koristeći pomoć prihvaćenih forenzičkih procedura. Po mogućnosti, ispitivanje ne bi trebalo vršiti na originalnim dokazima.

Slijedeće izlaganje se koristi za izdvajanje i analizu digitalnih dokaza. Izdvajanje se odnosi na proces prikupljanja podataka sa medija. Analiza se odnosni na interpretaciju prikupljenih podataka i postavljanje u logički i čitljiv format (npr. Kako su dospjeli tamo, odakle su potekli, i šta to znači?). Ponuđeni koncepti su namijenjeni da pomognu istražnom osoblju u razvijanju pravilnika, procedura i struktuiranja ispitivanja digitalnih dokaza. Pomenuti koncepti nisu namijenjeni da obuhvate i raspoznaju sve niti trebaju biti razlogom neiskorištavanja drugih tehnika u istragama. Na istražnom osoblju je da donese odluku i izvrši selekciju odgovarajućeg načina.

Prilikom izvođenja ispitivanja dokaza, razmotriti korištenje slijedećih koraka:

2.4.3.11.3. Korak 1 – Pripremanje

Pripremiti radni/radne direktorije na odvojenom mediju gdje se smještaju datoteke i podaci koje je potrebno izdvojiti.

2.4.3.11.4. Korak 2 – Izdvajanje

Kako je pojašnjeno ispod, postoje dva različita tipa izdvajanja, fizičko i logičko. Fizičko izdvajanje pronalazi i izdvaja podatke cijelog fizičkog uređaja bez obzira na sistem zapisivanja (file system). Logičko izdvajanje pronalazi i izdvaja datoteke i podatke na osnovu instalisanog operativnog sistema, sistema zapisivanja, i/ili aplikacija.

2.4.3.12. Fizičko izdvajanje

Ovim postupkom pristupa se izdvajanju podataka sa uređaja na fizičkom nivou bez obzira na sistem zapisivanja koji je zastupljen na uređaju. Ovaj tip može uključivati slijedeće metode: pretraživanje ključnih riječi, pretraživanje podataka na osnovu sadržaja (file carving), i izdvajanje particione tabele i neiskorištenog prostora na fizičkom uređaju.

- Pretraživanjem ključnih riječi na fizičkom uređaju može pomoći istražnom osoblju da izdvoji podatke koje operativni sistem i sistem zapisivanja ne registruju.
- Pretraživanje podataka na osnovu sadržaja (file carving) izvodi se pomoću alata koji pretražuju fizički uređaj i mogu pomoći pronalaženje i izdvajanje korisnih datoteka i podataka koje operativni sistem i sistem zapisivanja ne registruju.
- Pretraživanjem strukture particija može se identifikovati sistem zapisivanja i utvrditi da li cijela fizička veličina uređaja odgovara veličini uređaja.

2.4.3.13. Logičko izdvajanje

Ovim postupkom pristupa se izdvajanju podataka sa uređaja na osnovu sistema zapisivanja (file system), kojih može biti jedan ili više na uređaju, koji mogu uključivati dijelove aktivnih datoteka, izbrisanih datoteka, ostataka praznog prostora u klasterima (file slack), i neokupiranog datotečnog prostora. Ovi koraci mogu uključivati:

- Izdvajanje informacija iz sistema zapisivanja koji otkrivaju direktorijsku strukturu, atribute datoteka, imena datoteka, datume i vremena, veličinu datoteka, i lokaciju datoteka.
- Redukciju podataka zbog identifikacije i eliminacije poznatih datoteka kroz komparaciju dobijenu kalkulacijom hash vrijednosti prema autentičnim hash vrijednostima.
- Izdvajanje fajlova ključnih za istragu metodama baziranih na imenu datoteka, ekstenzijama, zaglavlju datoteke, sadržaju datoteke, i lokaciji na uređaju.
- Vraćanje izbrisanih datoteka
- Izdvajanje lozinkom zaštićenim, šifrovanih (encrypted), i kompresovanih podataka.
- Izdvajanje ostataka praznog prostora u klasterima
- Izdvajanje neokupiranog prostora

2.4.3.13.1. Korak 3 – Analiza i izdvajanje podataka

Analiza je proces interpretacije izdvojenih podataka za utvrđivanje važnosti za istražni slučaj. Pojedini primjeri analize koji se mogu izvršiti uključuju vremenski raspon, sakrivanje podataka, aplikacije i datoteke, vlasništvo i posjed. Analiza može uključivati provjeru zahtjeva za ispitivanje dokaza, pravnu dozvolu za istraživanje digitalnih dokaza, nadležne osobe za istragu, i/ili analitičara nadležnih za istragu.

2.4.3.14. Vremenski raspon analize

Vremenski raspon može se iskoristiti za određivanje slijeda pojedinih događaja na kompjuterskom sistemu, koji se mogu iskoristiti kao dio koji se odnosi na korištenje kompjutera od strane pojedinih osoba u vremenu kada se desio događaj koji se istražuje. Postoje dva metoda koji se mogu iskoristiti:

- Pregledanje vremena i datuma datoteka sadržanih u meta podacima sistema zapisivanja (npr. zadnja modifikovana datoteka, poslednja datoteka kojoj je pristupano, kreirana, promijenjen status) koji povezuju datoteke koje se traže i spadaju u vremenski raspon koji se istražuje. Primjer ove analize bio bi korištenje zadnjeg modifikovanog datuma i vremena za određivanje kada je sadržaj datoteke zadnji put promijenjen.
- Pregledanje zabilješki (log) sistema i aplikacija ako postoje koje uključuje zabilješke greški (log errors), zabilješke konekcija (connection logs), bezbjedonosne zabilješke (security logs), i slično. Primjer, ispitivanje bezbjedonosnih zabilješki može otkriti korištenje kombinacije korisničkog imena sa lozinkom za prijavu i ulaz u sistem.

Napomena
Uzeti u obzir razlike datuma i vremena svaki kompjuter prikazuje u BIOSu.

2.4.3.15. Analiza skrivenih podataka

Podaci mogu biti skriveni na kompjuterskom sistemu. Analiza skrivenih podataka se može iskoristiti za otkrivanje i povrat takvih podataka i uključuje poznavanje, vlasništvo, ili namjenu. Metode koje se mogu koristiti su:

- Povezivanje zaglavlja datoteka odgovarajućom ekstenzijom datoteka radi identifikacije ako su različite. Postojanje istih ukazuje da je korisnik namjerno sakrio podatke.
- Dobijanje pristupa za sve lozinkom zaštićene, šifrovane (encrypted), i kompresovane datoteke, koje mogu ukazivati na pokušaj skrivanja podataka od neautorizovanih korisnika. Sama lozinka može biti važna koliko i sadržaj same datoteke.
- Steganografija - Informacije skrivene u pisanju (kada se na jedan tekst ili sliku koja je vidljiva, prikači još jedan tekst ili slika koja nije vidljiva, bez ovlaštenog pristupa)
- Dobijanje pristupa za zaštićeni host prostor ili HPA (host-protected area). Postojanje korisnički kreiranih podataka u HPA prostoru može ukazivati na pokušaj skrivanja podataka.

2.4.3.16. Analiza datoteka i aplikacija

Mnogi programi i datoteke koji se pronađu mogu sadržati informacije koje se odnose na istragu i obezbijediti uvid u mogućnosti sistema i znanje koje korisnik posjeduje. Rezultati ove analize mogu ukazati dodatne korake koje treba preduzeti prilikom procesa izdvajanja i analize. Pojedini primjeri uključuju:

- Pregledanje imena datoteka vezano za istragu i sličnosti
- Ispitivanje sadržaja datoteka
- Identifikacije broja i tipa od operativnog/ih sistema
- Povezanost datoteka i instaliranih aplikacija
- Utvrditi povezanost između datoteka. Primjer, povezivanje internet istorije sa keširanim (cache) datotekama i e-mail datoteka sa e-mail prilozima
- Identifikovati poznate tipove datoteka kako bi se utvrdio njihov doprinos u istrazi.
- Ispitivanje osnovne/ih korisničke/ih lokacije za pohranu podataka vezanih za aplikacije i strukturu za datoteke (file structure) na uređaju kako bi se utvrdilo ako su datoteke smještene u svoje osnovnu/e ili alternativnu/e lokaciju/e.
- Ispitivanje korisničkih konfiguracija i podešavanja (user-configuration settings)

- Analiziranje meta podataka (metadata) datoteka, odnosno sadržaja datoteka kreiranih od strane korisnika koje imaju dodatne podatke osim podataka koji se prikazuju korisnicima i koji su obično kreiraju od strane aplikacija od kojih potiču. Primjer su datoteke kreirane aplikacijama za procesuiranje riječi koje mogu uključivati podatke o autoru, vrijeme zadnje izvršene promjene, broj koji pokazuje koliko je puta izmijenjena datoteka, i gdje je datoteka štampana ili snimljena.

2.4.3.17. Vlasništvo i posjedovanje

U pojedinim slučajevima važno je identifikovati osobu/e koje su kreirale, vršile promjene, ili pristupale datoteci. Takođe je važno utvrditi vlasništvo i posjedovanje znanja za podatke koji se istražuju. Elementi posjedovanja znanja mogu se bazirati na analizi koja je gore opisana, uključujući jedan ili više slijedećih faktora:

- Stavljanje datoteke na kompjuter u određeno vrijeme i datum mogu pomoći u određivanju vlasništva i posjedovanja (vremenski raspon analize)
- Datoteke koje se traže mogu biti locirane u nestandardnim mjestima (na primjer korisnički kreiranom direktoriju pod imenom " dječija pornografija") (analiza datoteka i aplikacija)
- Samo ime datoteke može biti od važnosti za istragu i može upućivati na sam sadržaj datoteke (analiza datoteka i aplikacija)
- Skriveni podaci mogu upućivati na namjerno skrivanje kako bi se izbjegla detekcija (analiza skrivenih podataka)
- Sadržaj datoteke može uključivati vlasništvo ili posjedovanje koje se odnosi na pojedinog korisnika (analiza datoteka i aplikacija)

2.4.3.17.1. Korak 4 – Zaključak

Sami rezultati prikupljeni pomoću bilo kojeg od pomenutih koraka može biti nedovoljno da bi se izvukao zaključak. Gledano u cjelini, povezanosti među pojedinačnim rezultatima pomažu da se kompletira cijela slika. Kao zadnji korak istražnog procesa, treba uzeti u obzir rezultate ispitivanja i analize u cijelosti[104].

2.4.3.18. Dokumentovanje i izvještavanje

2.4.3.18.1. Princip

Istraživačko osoblje je odgovorno za kompletiranje i tačno izvještavanje pronalazaka, rezultata analize i ispitivanja dokaza. Dokumentovanje je popratni proces istraživanja i vrlo je važno zapisivati korake koji se preduzimaju tokom istraživanja digitalnih dokaza.

2.4.3.18.2. Procedura

Svu dokumentaciju treba kompletirati, sa tačnošću, i iscrpno. Izvještaj sa rezultatima treba pisati namjenski za publiku koja ce čitati ili slušati.

2.4.3.19. Istražiteljske bilješke

[104] Izvor: http://www.nij.gov/nij/pubs-sum/219941.htm, Electronic Crime Scene Investigation A Guide for First Responders, Second Edition by National Institute of Justice, April 2008

Dokumentacija treba da prati istraživanje sa zadržanim bilješkama koje su u skladu sa pravilima istraživačkog odjela. Slijedeća je lista uopštenih razmatranja koja mogu pomoći osoblju koje istražuje kroz cijeli proces dokumentovanja:

- Zabilježiti konsultacije sa osobom nadležnom za istragu i/ili tužiocem
- Čuvati kopiju naloga ili dozvole za istragu zajedno sa ostalim zabilješkama
- Čuvati inicijalni zahtjev za podršku zajedno sa ostalim istražnim zabilješkama
- Čuvati kopiju dokumentacije posjedovanja
- Praviti detaljne zabilješke koje omogućuju kompletnu duplikaciju poduzetih radnji
- Zabilješke uključuju datume, vremena, opise i rezultate radnji koje su preduzete
- Dokumentovati svaki neregularnost na koju se naiđe, kao i radnje koje su preduzete zbog neregularnosti prilikom istraživanja
- Uključiti dodatne informacije, kao što je mrežna topologija, lista autorizovanih korisnika, korisničke saglasnosti, i/ili lozinke
- Dokumentovati promjene napravljene na sistemu ili mreži ili na osnovu zakonskih smjernica ili od istražnog osoblja
- Dokumentovati operativni sistem i relevantnu verziju softvera i trenutno instalisane zakrpe (patches)
- Dokumentovati informacije koje se prikupe na istražnom licu mjesta u slučaju daljinske pohrane podataka, daljinski korisnički pristup, i rezervne kopije sa lica mjesta.

Tokom procesa ispitivanja, moguće je pronaći informacije o dokazima koji su od posebnog značaja, ali koje su van grupe trenutnog pravnog ovlaštenja. Dokumentovati ove informacije i obavijestiti nadležno istražno osoblje zato što informacije mogu zahtijevati dodatna ovlaštenja za pretraživanja.

2.4.3.20. Istražni izvještaj (Examiner's report)

Slijedi pregled uputstva za pripremanje izvještaja koji će se predati nadležnom istražnom osoblju, tužiocu, ili drugima. Slijedeći su uopšteni prijedlozi dok pravilnik istražnog odjela može diktirati izgled i specifičnosti, kao što su redoslijed i sadržaj. Izvještaj može uključivati:

- Podaci o istražnoj službi
- Oznaka istražnog slučaja ili broj zahtjeva
- Istražno osoblje
- Podatke o podnosiocu
- Datum prijema
- Datum izvještavanja
- Opisna lista uređaja koji su predani za istragu, uključujući serijski broj, proizvođača, i model
- Podatke i potpis istražnog osoblja
- Kratki opis i koraci preduzeti tokom istraživanja, poput pretraga stringova, pretraga grafičkih slika, i vraćanje izbrisanih datoteka
- Rezultati / zaključci

2.4.3.21. Kratak pregled rezultata istrage

Slijedi kratki pregled rezultata istražnih radnji na uređajima predanim za analizu. Svi izlistani rezultati u pregledu također trebaju da budu sadržani u dijelu izvještaja sa detaljnim rezultatima istrage.

2.4.3.22. Detaljni rezultati istrage

Ovaj dio opisuje veće detalje rezultata istraživanja i mogu uključivati:

- Pojedine datoteke koje se odnose na zahtjev
- Druge datoteke, uključujući izbrisane datoteke, koji podržavaju rezultate istrage
- Pretraživanje stringova, ključnih riječi, i tekstualnih stringova
- Internet-vezani dokazi, poput analize web sajt saobraćaja, chat zabilješke (logs), keš datoteke, e-mail, i aktivnosti vezane za nove grupe (news group)
- Analiza grafičkih slika
- Indikatori o vlasništvu, koji mogu uključivati programsku registraciju podataka
- Analiza podataka
- Opis relevantnih programa na uređajima koji su istraživani
- Tehnike koje su korištene za skrivanje ili maskiranje podataka, poput šifrovanja (encyption), steganografija, sakriveni atributi, sakrivene particije, i anomalije u imenovanju datoteka

2.4.3.23. Riječnik

Riječnik može biti uključen u izvještaj kako bi pomogao čitaocu u razumijevanju tehničkih riječi koje su se koristile. Koristiti opšte prihvaćeni izvor za definicije termina i uključiti odgovarajuće reference[105].

2.4.3.24. Rukovanje digitalnim dokazima na licu mjesta

Rukovanje digitalnim dokazima na licu mjesta izvršenja kriminalnog djela je potrebno pristupiti na poseban način. U pojedinim slučajevima potrebno je obezbijediti potrebne preduslove u prikupljanju, zadržavanju, i transportu digitalnih dokaza. Istražni organi pristigli na lice mjesta prilikom prikupljanju dokaza moraju:

- Prepoznati, identifikovati, oduzeti, i osigurati sve digitalne dokaze na licu mjesta
- Dokumentovati lice mjesta sa tačnom lokacijom svakog pronađenog uređaja
- Prikupiti, označiti, oduzeti i zadržati digitalni dokaz
- Zapakovati i bezbjedno transportovati digitalni dokaze

Takođe prije bilo kakve istrage potrebno:
- Obezbijediti dozvole za istražne radnje i oduzimanje dokaza
- Obezbijeđeno i dokumentovano lice mjesta
- Stručno istražno osoblje koristi odgovarajuću zaštitnu opremu

[105] Izvor: http://www.nij.gov/nij/pubs-sum/199408.htm, Forensic Examination of Digital Evidence: A Guide for Law Enforcement by National Institute of Justice, April 2004

Istražni organima bez odgovarajućeg treninga i vještina se ne preporučuje pristupanju sadržaja ili informacijama na kompjuteru ili drugih elektronskih uređaja osim da dokumentuju ono što vide na ekranu monitora. Ne pritiskati tipke ili dugmad miša[106].

2.4.3.25. Elektronski uređaji-vrste opis potencijalnih dokaza

Elektronski uređaji ili samo uređaji, pronađeni na licu mjesta predstavljaju izvor potencijalnih dokaza koji se mogu koristiti u dokazivanju izvršenja krivičnih djela u sudskim procesima. Svaki pronađeni elektronski uređaj mora biti pravilno identifikovan, kao i podaci koji mogu biti od istražne vrijednosti. Bilo da se radi o internim komponentama ili eksternim odnosno perifernim dijelovima kompjuterskog sistema istima se mora pristupiti sa posebnom pažnjom. Pojedini uređaju zahtijevaju interno ili eksterno električno napajanje da bi zadržali podatke u memoriji.

2.4.3.26. Računarski sistemi

Računarski sistem ili računar je informacioni sistem koji se sastoji od hardvera i softvera koji vrše obradu podataka i koji uključuje:

- Kućište koje sadrži elektronska kola, mikroprocesore, hard disk, memoriju, i ostale priključke
- Monitor ili drugi uređaj sa ekranom
- Tastaturu
- Miš ili drugu vrstu pokazivača
- Periferne ili spojene eksterne uređaje i komponente

Današnji računarski sistemi, zavisno od svrhe, se proizvode u različitim formama i oblicima i njihova fizička veličina u mnogome varira. računarski sistemi mogu biti dio stalaže poput serverskih računarski sistema (rack), desktop sa horizontalnim kućištem, tower sa vertikalnim kućištem, mainframe sistemi. Takođe računarski sistem mogu sadržavati periferne uređaje kako što su štampači, ruteri, switch-evi, skeneri i drugi.

Potencijalni dokazi koji se mogu naći u kompjuterskom sistemu i njegovim komponentama su od izuzetne važnosti za istrage. Sastavni hardver i softver sa podacima može sadržavati dokumente, slike, e-mailove, istoriju internet surfanja, zapisnike chat-ova, liste prijatelja, finansijske informacije, podatke o događajima kao i vremenima pojedinih dešavanja koje mogu poslužiti u identifikaciji kriminalnih djela i mogu služiti kao potencijalni dokazi.

2.4.3.26.1. Otvoreni i zatvoreni računarski sistemi

Sve elektronske uređaje i sisteme možemo svrstati u dvije grupe: zatvoreni i otvoreni sistem zavisno od prirode njihovog korištenja.

U grupu zatvorenog sistema spadaju svi uređaji koji nikada nisu bili spojeni na internet, te je uređaj bio u upotrebi u izoliranoj i/ili kontrolisanom okruženju i/ili zatvorenoj mreži koja je takodje zatvoreni ili izolirani sistem ili skup više manjih sistema koji su zatvoreni.

[106] Izvor: http://www.nij.gov/nij/pubs-sum/219941.htm, Electronic Crime Scene Investigation A Guide for First Responders, Second Edition by National Institute of Justice, April 2008

Pod otvorenim sistemom podrazumijevamo bilo koji sistem, bez obzira na njegovu veličinu, koji ima internet konekciju, koja može biti direktna (javni internet kafei ili konekcija na javnom mjestu) ili indirektna (konekcija preko USB memorije koji je prethodno bio nakačen na internet). Bez obzira na formu ili korake, spajanja na internet mijenja zatvoreni sistem u otvoreni.

2.4.3.27. Uređaji za pohranjivanje podataka

Uređaji koji služe za pohranu podataka, se u mnogome razlikuju po tipu, veličini, opisu i svrsi, te načinu pohranjivanja podataka. Podaci smješteni na uređajima za pohranjivanje podataka su od izuzetne važnosti jer mogu sadržavati digitalne dokaze koje se mogu koristiti u istražnim i sudskim postupcima.

2.4.3.28. Hard diskovi

Hard diskovi ili samo diskovi su uređaji za koji služe za pohranu podataka koji imaju eksterno napajanje i čiji su osnovni dijelovi: štampana ploča, keš (cache) ili privremena interna memorija, spojevi za napajanje, te interne magnetske ploče (platters) izrađene od stakla, keramike ili metala i služe za smještanje podataka.

Po veličini razlikujemo 2.5 ili 3.5 inča hard diskove, ali njihova veličina može varirati, također po mjestu ugradnje u sisteme razlikujemo interne i eksterne hard diskove.

Interni hard diskovi se napajaju od strane kompjuterskog sistema. Po vrsti priključka na kompjuterski sistem možemo podijeliti na slijedeće tipove hard diskova:

- IDE ili Parallel ATA (PATA) hard diskovi:
- IDE 40-pinski, ATA – 3.5 inča
- IDE 44-pinski – 2.5 inča
- IDE 80-pinski – 3.5 inča
- PATA – 2.5 i 3.5 inča
- SATA (Serijski ATA) hard diskovi:
- SATA II (Serijski ATA druge generacije)
- SCSI hard diskovi:
- SCSI IDC 50-pinski
- SCSI HD 68-pinski
- SSD hard diskovi

Eksterni hard diskovi su interni diskovi smješteni u kućišta standardne veličine hard diska i služe kao dodatak za pohranjivanje podataka odnosno proširenje kapaciteta memorije kompjuterskog sistema. Eksterni hard diskovi su uređaji tehnički prilagođeni i pogodni za prenosivost i bolju zaštitu od podložnih oštećenja zbog kućišta. Napajaju se pomoću eksternog napajanja ili preko priključnih komponenata poput USB priključka. Eksterne diskove po vrsti priključaka možemo razlikovati:

- Universal Serial Bus - USB 1.0/USB 2.0/USB3.0
- Firewire 400/Firewire 800
- Ethernet ili uređaji za mrežnu pohranu podataka
- WiFi

2.4.3.29. Izmjenjivi mediji

Izmjenjivi mediji predstavljaju medij za pohranjivanje podataka na kojem se informacije smještaju na tanku kružnu magnetnu površinu koja je obložena plastičnom ambalažom radi zaštite ili je u obliku optičkih diskova različitih prečnika, gdje se podaci snimaju u slojevima koristeći lasersku tehnologiju i optička leća. Za čitanje ili snimanje izmjenjivih medija kompjuterski sistemi moraju posjedovati uređaje koji odgovaraju vrsti izmjenjivih medija. Postoje različiti kapaciteti, koji u poređenju sa današnjim hard diskovima pohranjuju manje podataka. Ova vrsta medija se koristi za snimanje, arhiviranje, transfer i transport podataka kao i za druge informacije. Pomažu korisnicima podjelu podataka, informacija, aplikacija i alata između različitih kompjutera i ostalih uređaja.

Primjeri izmjenjivih medija sa odgovarajućim uređajima koji ih mogu čitati:
- Floppy diskete / Floppy uređaj
- Superdisk LS-120 / Superdisk LS-120 uređaj
- Zip diskete / Zip uređaj
- Jazz diskete / Jazz uređaj
- CD – Compact Disc / CD-ROM, DVD ili BD uređaj
- DVD – Digital Versatile Disc / DVD ili BD uređaj
- BD – Blu-ray Disc / Blue-ray uređaj

Postoje različite forme ovakvih uređaja te po mjestu mogu biti interni ili eksterni, dok uređaji koji čitaju i snimaju podatke mogu biti u formi kućanskih aparata ili drugih uređaja.

2.4.3.30. Memorijski stikovi(Thumb drives/keychains/memory stick/flwsh drives)

Memorijski stikovi su mali, laki i izmjenjivi uređaji za pohranjivanje podataka sa USB priključkom. Ova vrsta uređaja se još naziva i flash uređaji koje je lako sakriti i nositi. Mogu se naći kao sastavni dio nečega ili prerušeni u obliku ručnog sata, džepnog višenamjenskog alata poput džepnih švajcarskih vojnih nožića, privjesaka za ključeve, kao i dio drugih vrsta uređaja.

2.4.3.31. Memorijske kartice

Memorijske kartice su mali uređaji za pohranjivanje podataka najčešće korištene na digitalnim kamerama, kompjuterima, mobilnim telefonima, digitalnim muzičkim plejerima, personalnim digitalnim asistent (PDA) uređajima, konzolama za video igre, ručnim i drugim elektronskim uređajima.

Čitanje ili snimanje podataka na memorijske kartice se ostvaruje putem samog uređaja u koji je postavljena i koji obično imaju ugrađen USB priključak, te se može vršiti čitanje pomoću USB kablova. Pored ovog načina moguće je čitati ili snimati podatke pomoću posebno namijenjenih USB čitača jednih ili više vrsta kartica. Najpoznatije vrste memorijskih kartica su:
- Smart Media kartice
- MultiMediaCard (MMC) kartice
- SD (Secure Digital) kartice ili SDHC (Secure Digital High Capacity)
- Mini SD kartice
- Miniature Card kartice

- Micro (Micro) SD kartice
- CF (Compact Flash) kartice I/II/III/IV
- MicroDrive (MD) kartice
- xD-Picture memorijska kartica
- Memory Stick, Memory Stick PRO/PRO-HG/Duo/Micro (M2)/XC

Uređaji za pohranjivanje podataka poput hard diskova, eksternih hard diskova, izmjenjivih medija, memorijskih stikova i memorijskih kartica mogu sadržavati informacije poput e-mailova, istorije otvorenih internet stranica, zapisnike sa internet chat sesija ili liste prijatelja, fotografije, slike, baze podataka, finansijsku dokumentaciju, ili zapisnike događanja na sistemima koji mogu biti značajni dokazi prilikom istražnih radnji ili sudskih procesa.

2.4.3.32. Ručni uređaj(Handheld devices)

Ručni uređaji su uređaji koji omogućuju snimanje i prenosivost podataka i koji omogućuju komunikaciju, digitalnu fotografiju, posjeduju navigacione sisteme, zabavu, snimanje podataka, i upravljanje ličnim informacijama.

Ručni uređaji poput mobilnih telefona, smart telefona, PDA uređaja, digitalnih multimedijalnih (audio i video) uređaja, pejdžera, digitalnih kamera, i GPS uređaja, koji primaju signale sistema globalnog pozicioniranja koji mogu da sadrže softverske aplikacije, podatke, i informacije poput dokumenata, e-mailova, istorije otvorenih internet stranica, zapisnike sa internet chat sesija ili liste prijatelja, fotografije, slike, baze podataka, finansijsku dokumentaciju, ili zapisnike događanja na sistemima koji mogu biti značajni dokazi prilikom istražnih radnji ili sudskih procesa.

Vrlo je važno napomenuti da:

- Podaci ili digitalni dokazi mogu biti izgubljeni ako se uređaj ne održava pod napajanjem električnom energijom.
- Podaci ili digitalni dokazi na pojedinim uređajima poput mobilnog ili smart telefona mogu biti presnimljeni ili izbrisani ako uređaj ostane aktivan.
- U slučaju da je mobilni ili smart telefon izgubljen ili ukraden, softver koji posjeduju ovakvi telefoni može se daljinski aktivirati i uzrokovati kvar čime uređaj i podaci postaju neupotrebljivi. Ovaj softver može da uzrokuje slične rezultate ako se aktivira na uređajima koji su oduzeli istražni organi, te je potrebno poduzeti sve mjere kako bi se spriječio gubitak podataka na oduzetim uređajima.

2.4.3.32. Periferni uređaji

Periferni uređaji predstavljaju opremu koja može biti spojena na kompjuter ili kompjuterske sisteme radi unapređenja korisničkog pristupa i proširenja funkcija kompjutera.
Neki od perifernih uređaja su:

- Tastatura i miš
- Mikrofon
- USB i FireWire hubovi
- Web kamere
- Čitač memorijskih kartica
- VoiP uređaji

- Štampači
- Skeneri

Sami uređaji uključujući funkcije koje obavljaju ili pružaju kao i njihova namjena čine potencijalni dokaz. Informacije o upotrebi koji su pohranjeni na uređaje se također smatraju dokazima, primjer su primljeni i pozivni telefonski ili fax brojevi, zadnji skenirani, faxirani ili štampani dokumenti, i informacije o namjeni za koju je korišten uređaj. Dodatno ovakvi uređaji mogu biti izvor otisaka prstiju, DNK, i drugih pokazatelja.

2.4.3.33. Ostali izvori potencijalnih digitalnih dokaza

Pred nabrojanih, istražni organi treba da uzmu u obzir i druge elemente potencijalnih dokaza zatečenih na licu mjesta koji su povezani sa digitalnim informacijama, poput elektronskih uređaja, opreme, softvera, hardvera, i drugih tehnologija koji mogu funkcionisati nezavisno ili odvojeno, zajednički, ili kao dodatak kompjuterskim sistemima. Ovakvi uređaji mogu se koristiti za bolji korisnički pristup za proširenje funkcionalnosti kompjuterskog sistema, samog uređaja, ili ostale opreme.

Primjeri ovakvih uređaja su:

- Trake za snimanje podataka
- Oprema za osmatranje
- Digitalne kamere
- Video kamere
- Digitalni audio snimači
- Digitalni video snimači
- MP3 Plejeri
- Satelitski audio, video risiveri i satelitske kartice
- Konzole za video igre
- Set slušalica sa mikrofonom namijenjenih za chat
- Tastatura, mis i video razdjelnik (KDM switch)
- GPS risiver
- Čitač SIM kartica
- Čitač otisaka prstiju
- Uputstva za upotrebu, priručnici i ostale reference

Potencijalni dokazi su sami uređaji, namjena ili svrha korištenja, funkcionalnost i mogućnosti, i bilo koje podešavanje ili druge informacije koje može da sadrži kao potencijalni dokaz.

2.4.3.34. Računarska mreža

Računarska mreža se sastoji od dva ili više kompjutera povezanih kablovima za prenos podataka ili bežičnim putem koji dijele ili mogu dijeliti resurse i podatke. računarska mreže često uključuju štampače, druge periferne uređaje, i uređaje za usmjeravanje poput habova, svičeva i rutera.

Primjeri uređaja koje koriste računarska mreže su:

- Mrežni hub
- Mrežna kartica za laptop
- Ethernet kabl
- Internet modemi
- Mrežni svič sa uređajima za napajanje
- Uređaji za bežično umrežavanje
- Bežični mrežni serveri
- Bežične kartice i uređaji
- Bežične kartice za PC kompjutere
- Bežični USB uređaji
- Direkcione antene za mrežne kartice

Potencijalni dokazi vezani za umrežene računare i spojene uređaje samo posjedovanje može predstavljati dokaz koji je koristan u istrazi ili suđenju. Podatke koje sadrže mogu predstavljati dokaze i mogu uključivati softver, dokumente, fotografije, slikovne podatke, e-mail poruke sa dodacima, baze podataka, finansijske informacije, istoriju otvorenih internet stranica, zapisničke (log) podatke, zapisnike događaja an sistemu i chat sesija, listu prijatelja, i podatke pohranjene na eksterne uređaje. Funkcije uređaja, mogućnosti, i bilo koja identifikaciona informacija koja se odnosi na kompjuterski sistem, komponente i spojevi, uključujući internet protokol (IP) i adrese lokalne mreže (LAN) korištene sa računare i ostalim uređajima, podešavanja za slanje, i MAC (media access cards) kartice ili adresa NIC (Network Interface Card) mrežnih kartica mogu takođe biti korisni dokazi[107].

2.4.3.35. Alati i oprema za istrage

U većini slučajeva, uređaji koji sadrže digitalne dokaze prilikom istražnih radnji mogu se oduzeti koristeći standardne alate i materijale. Pored toga potrebno je obratiti pažnju prilikom prikupljanja, pakiranja ili skladištenja digitalnih uređaja kako bi se izbjegla promjene, oštećenja, ili uništili digitalni dokazi. Izbjegavati koristiti alate koji mogu proizvesti ili emitirati statički elektricitet ili magnetno polje jer isti mogu oštetiti ili uništiti dokaze.

Ako kompleksnost elektronike na licu mjesta odvijanja kriminalnih radnji prelazi znanje i ekspertizu pojedinih članova istražne službe potrebno je zatražiti pomoć od strane stručnjaka koji posjeduju napredniju opremu i treninge u prikupljanju digitalnih dokaza.

2.4.3.35.1. Alati i materijali koji se koriste za prikupljanje digitalnih dokaza

Kao dodatak alatima za procesiranje lica mjesta kriminalnih radnji preporučeni su slijedeći predmeti i alati koji pomažu istražne radnje i prikupljanje digitalnih dokaza:
- Kamere (foto i video)
- Kartonske kutije
- Bilježnice
- Rukavice
- Zapisnici inventure

[107] Izvor: http://www.nij.gov/nij/pubs-sum/219941.htm, Electronic Crime Scene Investigation A Guide for First Responders, Second Edition by National Institute of Justice, April 2008

- Samoljepljiva traka za obilježavanje dokaza
- Papirne vrećice za pakovanje dokaze
- Traka za obilježavanje istražnog lica mjesta
- Antistatičke vrećice
- Permanentni markeri
- Antimagnetni alati

Kao dodatak ovim alatima spadaju i materijali za zaštitu od frekvencija poput faradejevih izolacionih vrećica, aluminijske folije za pakovanje mobilnih telefona, smart telefona, i drugih uređaja mobilne komunikacije koji se oduzmu prilikom istražnih radnji.

Pakovanjem u vrećice za zaštitu od frekvencija sprečava se dopiranje radio frekvencija do telefona, primanja poziva, primanja poruka i drugih komunikacijskih signala koji mogu promijeniti dokaze[108].

2.4.3.36. Obezbjeđenje i ispitivanje lica mjesta

Prije poduzimanja bilo kakvih istražnih radnji nad dokazima digitalne prirode na licu mjesta potrebno je izvršiti fizičko obezbjeđivanje i osiguranje istražnog lica mjesta u skladu sa postojećim pravilnicima i procedurama istražnih organa. Kada su svi pomenuti preduslovi zadovoljeni pristupa se identifikaciji i procesu obezbjeđenja integriteta i očuvanja svih potencijalnih dokaza uključujući klasične tradicionalne kao i digitalne dokaze koje je potrebno zadržati. Digitalni dokazi koji se nalaze na kompjuterskim sistemima i drugim elektronskim uređajima vrlo lako mogu biti izmijenjeni, izbrisani, ili oštećeni tako da se mora obratiti posebna pažnja. Nakon identifikacije pristupa se dokumentovanju, fotografisanju, i osiguranju digitalnih dokaza u što kraćem vremenu na licu mjesta.
Prilikom izvršenja istražnih radnji nad dokazima digitalne prirode potrebno je zadovoljiti slijedeće uslove:

- Sve istražne radnje koje je potrebno poduzeti na licu mjesta moraju da budu u skladu sa pravilnicima i procedurama istražnih organa
- Izvršiti obezbjeđivanje svih elektronskih uređaja u što kraćem vremenskom roku, uključujući lične i mobilne uređaje
- Obezbijediti lice mjesta i zabraniti pristup neovlaštenim licima
- Odbiti bilo kakvu tehničku pomoć od neovlaštenih lica
- Odstraniti sva neovlaštena lica sa istražnog mjesta i neposredne blizine uređaja koji mogu poslužiti kao dokazi
- Pobrinuti se da lice mjesta sa elektronskim uređajima bude nepromijenjeno
- U slučaju da su elektronski uređaji isključeni pobrinuti se da ostanu u tom stanju i ne uključivati iste

Kompjuterske komponente poput tastature, miša, izmjenjivih medija ili bilo kojih drugih predmeta koji sadrže skrivene dokaze poput DNK, ili druge fizičke dokaze koje je potrebno sačuvati. Sve istražne aktivnosti preduzete na licu mjesta ne smiju dokaze fizičke prirode i promijeniti njihovu originalnost dokaza prilikom procesa dokumentovanja.

U slučaju da je prilikom izvođenja istražnih radnji na licu mjesta teško odrediti da li kompjuterski sistem uključen potrebno je preduzeti slijedeće korake:

[108] Izvor: http://www.nij.gov/nij/pubs-sum/219941.htm, Electronic Crime Scene Investigation A Guide for First Responders, Second Edition by National Institute of Justice, April 2008

- Osmatrati i slušati za bilo koje naznake aktivnosti kompjuterskog sistema. Pratiti zvučne znakove ventilatora, rotirajućih uređaja, ili aktivnosti LED dioda koje pokazuju da je sistem uključen.
- Provjeriti uređaj(e) za prikaz i tražiti znakove koji indiciraju uništavanje digitalnih dokaza. Tražiti riječi poput "format," "delete," "copy," "move," "wipe," "cut," "remove."
- Provjeriti znakove koji ukazuju da se kompjuterskom sistemu pristupa daljinski pomoću drugog kompjuterskog sistema ili uređaja
- Provjeriti znakove aktivnosti ili moguće komunikacije sa drugim kompjuterskim sistemima ili korisnicima putem programa i prozora instantnih poruka ili chat prostorija.
- Provjeriti aktivnosti na svim priključenim kamerama ili web kamerama i utvrditi da li su aktivne

Tehnološki razvoj u polju informacionih tehnologija omogućuje povezivanje više uređaja i dijeljenje internih resursa mreže kao i povezivanje istih na internet. Osoblje koje pristupa prikupljanju digitalnih dokaza treba da bude upoznato sa mogućnostima i potencijalnim mjestima za digitalne dokaze koje sadrži većina uređaja kao što su telefon, razni kućni aparati, digitalni uređaji koji imaju mogućnost pohrane podataka, kao i motornih vozila.

2.4.3.37. Preliminarni intervjui i ispitivanje

Prilikom obrade lica mjesta istražni organi su obavezni izvršiti identifikaciju svih lica koja su zatečena u momentu početka istrage te dokumentovati njihove tačne fizičke lokacije. Zatim je hitno potrebno zabraniti pristup kompjuterskim sistemima ili drugim elektronskim uređajima. U skladu sa pravilnicima i procedurama nadležnih istražnih organa potrebno je izvršiti obradu i prikupiti što više informacija od osoba zatečenih na licu mjesta uključujući slijedeće informacije:

- Imena svih korisnika kompjuterskih sistema i uređaja
- Sve kompjuterske sisteme i korisničke informacije vezane za internet
- Sva korisnička imena koja se koriste za prijavu i imena korisničkih računa? (account names)
- Svrhe upotrebe kompjuterskog sistema i uređaja
- Sve lozinke
- Sve korištene automatske aplikacije
- Tip internet pristupa
- Uređaje za pohranu podataka koji trenutno nisu u pogonu
- Ime internet servis provajdera(ISP)
- Sve email račune (? termin email accounts?)
- Zaštita mjere koja se koriste
- Informacije o Web e-mail računu
- Ograničenja za pristup podacima koja se koriste
- Sva imena koja za programe instant poruka
- Softver ili uređaji koji se koristi za uništavanje
- MySpace, Facebook, ili drugi online web stranica za druženje
- Druge relevantne informacije[109]

[109] Izvor: http://www.nij.gov/nij/pubs-sum/219941.htm, Electronic Crime Scene Investigation A Guide for First Responders, Second Edition by National Institute of Justice, April 2008

2.4.3.38. Dokumentovanje lica istražnog mjesta

Dokumentovanje lica mjesta i njegova obrada se mora provoditi u skladu sa postojećim zakonima, pravilnicima i procedurama nadležnih i istražnih organa. Proces dokumentovanja ne smije izvršiti ni po kojem osnovu izvršiti povredu istih. Dokumentovanjem lica mjesta se kreira dokument o izvršenoj istrazi i prikupljenim dokazima. Jedan takav dokument sadrži tačne podatke o lokaciji, zatečeno stanje, trenutno stanje sistema u pogonu, sistemski uslovi, mediji za pohranu podataka, uređaji vezani za bežično umrežavanje, mobilni telefoni, napredni smart telefoni, PDA uređaji, internet i mrežni pristup i drugi elektronski uređaji. Istražno osoblje mora posebnu pažnju posvetiti uređajima koji nisu u neposrednoj blizini kompjutera ili drugih elektronskih uređaja.

Prilikom procesa dokumentovanja ovlašteno istražno osoblje mora prikupiti informacije poput serijskih brojeva i drugih specifikacija. U slučaju prostornih ili drugih ograničenja kada je nemoguće izvršiti ovaj proces bez fizičkog pomjeranja uređaja dozvoljeno je pomjeranje kompjuterskog sistema ili drugog elektronskog uređaja tek nakon isključivanja iz pogona i potpunog prestanka rada uređaja. Svako pomjeranje kompjuterskog sistema ili drugog elektronskog uređaja za vrijeme rada može oštetiti uređaj te oštetiti digitalne dokaze koje sadrži.

Dokumentovanje zatečenog stanja potrebno obaviti detaljno. Uređaji koji mogu poslužiti procesu dokumentovanja su video uređaji, fotografisanje, zapisnici i skice koji mogu pomoći da se rekreira lice mjesta po potrebi nadležnih istražnih organa. Sve aktivnosti i procesi koji se odvijaju na uređajima za prikaz je potrebno detaljno dokumentovati.

Proces dokumentovanja lica mjesta treba da obuhvati cijelu lokaciju, uključujući tip lokacije, okružnu lokaciju, fizičku lokaciju i pozicije kompjuterskih sistema, komponenti, i periferne opreme, kao i drugih elektronskih uređaja. Proces dokumentovanja može obuhvatiti više lokacija te je potrebno dokumentovati sve fizičke povezanosti prema i od kompjuterskih sistema i drugih uređaja.

Takođe je neophodno obuhvatiti bežične mrežne tačke (wireless access points) kojima je moguće pristupiti i povezati kompjuterske sisteme i druge uređaje jedne sa drugim ili na internet. Postojanje mreže i bežičnih mrežnih tačaka može ukazati da postoje dodatni digitalni dokazi koji nisu prikupljeni na licu mjesta.

U slučaju kada istražni organi nisu u mogućnosti prikupiti i dokumentovati sve digitalne dokaze na licu mjesto zbog postojanja otežanih okolnosti koje nisu ovdje opisane. Takođe pojedine okolnosti koje su predviđene zakonom, pravilnicima, i procedurama mogu se ispriječiti i izuzimanje i izvršenje istražnih radnji. U takvim slučajevima istražni organi su obavezni dokumentovati uslove zbog kojih su spriječeni kao i zatečeno stanje i okolnosti lica mjesta.

2.4.3.39. Prikupljanje dokaza na licu istražnog mjesta

Da bi se započeo bilo kakav proces u vezi prikupljanja dokaza potrebno je obezbijediti potrebne dozvole od strane nadležnih organa. Osoblje istražnih organa mora biti upoznato sa postojećim pravilnicima i procedurama koji se moraju pridržavati prilikom istražnih radnji kao i predmeta izuzimanja i prikupljanja dokaza. U slučaju nepredviđenih situacija osoblje mora imati informacije kome da se obrati i ko je nadležan za pomenutu istragu.

Rukovanjem digitalnih dokaza se mora posvetiti posebna pažnja da bi se zadržali integritet fizičkih uređaja kao i podaci koje sadrže. Pojedini digitalni dokazi zahtijevaju posebne tehnike vezane za prikupljanje, pakiranje i transport. Podaci koji su pohranjeni vrlo lako se mogu oštetiti izlaganjem elektromagnetnom polju kojeg generiše statički elektricitet, magneti, radio odašiljači i drugi uređaji. Kompjuterski sistemi koji koriste šifrovanje (encryption) kao zaštitu podataka na uređajima za pohranjivanje ili na drugim elektronskim uređajima u slučaju nestručnog isključivanja iz pogona i gašenja tokom prikupljanja dokaza podatke koje sadrži mogu biti uništeni. Komunikacijski uređaji poput mobilnih telefona, smart telefona, PDA uređaja ili pejdžera moraju biti osigurani i zaštićeni od primanja ili odašiljanja podataka kada se identificiraju i prikupe kao dokaz.

2.4.3.40. Računari ,komponente i ostali uređaji

Da bi se spriječila bilo kakva promjena digitalnog dokaza prilikom izuzimanja potrebno je da istražno osoblje obrati pažnju na:

- Dokumentovati bilo kakvu aktivnost na kompjuterskom sistemu, komponentama, i uređajima
- Potvrditi stanje kompjuterskog sistema. Obratiti pažnju na aktivnosti LED lampica, rad ventilatora, kao i drugih znakova koji ukazuju da je sistem uključen i u pogonu. Ako je tačno nemoguće odrediti stanje iz navedenih aktivnosti, potrebno je obratiti pažnju na monitor da bi se utvrdilo da li je sistem u pogonu, van pogona, ili u modu štednju električne energije (sleep mode).

2.4.3.41. Razmatranje situacije

Nakon utvrđivanja stanja aktivnosti kompjuterskog sistema potrebno je koristiti slijedeće korake:

a). SITUACIJA 1: Monitor uključen i prikazuje program, aplikaciju, radni dokument, sliku, e-mail, ili internet stranicu na ekranu**.**

1. Fotografisati ekran i dokumentovati informacije koje se nalaze na ekranu
2. Preći na korak "Ako je kompjuter uključen i u pogonu"

b). SITUACIJA 2: Monitor uključen i skrin sejver (screen saver) ili slika su prikazani na ekranu.

1. Lagano pomjeriti miša ili drugi uređaj za pokazivanje i interakciju sa kompjuterskim sistemom bez pritiskanja dugmadi ili rotacionog točkića. Aktivni ekran će se promijeniti na login ekran spreman za ukucavanje korisničkih podataka, radni dokument, ili se aktivira drugi uređaj za prikaz.
2. Fotografisati ekran i dokumentovati informacije koje se nalaze na ekranu
3. Preći na korak "Ako je kompjuter uključen i u pogonu"

SITUACIJA 3: Monitor uključen ali ekran je bez slike i izgleda kao da je ugašen**.**

1. Lagano pomjeriti miša ili drugi uređaj za pokazivanje i interakciju sa kompjuterskim sistemom bez pritiskanja dugmadi ili rotacionog točkića. Izgled ekrana će se promijeniti

sa praznog crnog ekrana na login ekran spreman za ukucavanje korisničkih podataka, radni dokument, ili se aktivira drugi uređaj za prikaz. Posmatrati promjene na ekranu.
2. Fotografisati ekran i dokumentovati informacije koje se nalaze na ekranu
3. Preći na korak "Ako je kompjuter uključen i u pogonu"

SITUACIJA 4a: Monitor isključen a ekran bez slike.

1. Ako je prekidač paljenja monitora u poziciji koja pokazuje da je isključen, pritisnuti dugme za paljenje i uključiti monitor. Izgled ekrana će se promijeniti sa praznog na login ekran spreman za ukucavanje korisničkih podataka, radni dokument, ili se aktivira drugi uređaj za prikaz. Posmatrati promjene na ekranu.
2. Fotografisati ekran i dokumentovati informacije koje se nalaze na ekranu
3. Preći na korak "Ako je kompjuter uključen i u pogonu"

SITUACIJA 4b: Monitor uključen a ekran bez slike.

1. Ako je prekidač paljenja monitora u poziciji koja pokazuje da je isključen, pritisnuti dugme za paljenje i uključiti monitor. Izgled slike na ekranu se ne mijenja i dalje je bez slike. Posmatrati promjene na ekranu.
2. Fotografisati prazan ekran
3. Preći na korak "Ako je kompjuter isključen i van pogona"

SITUACIJA 5: Monitor uključen a ekran bez slike.

1. Lagano pomjeriti miša ili drugi uređaj za pokazivanje i interakciju sa kompjuterskim sistemom bez pritiskanja dugmadi ili rotacionog točkića zatim čekati reakciju sistema.
2. U slučaju da se slika na ekranu ne mijenja i dalje se ne prikazuje slika provjeriti da li se monitor napaja električnom energijom. Ako ekran i dalje bude bez slike, provjeriti da li je kućište kompjuterskog sistema pokazuje znake aktivnosti pomoću LED lampica, pratiti zvuk ventilatora ili drugih znakova koji ukazuju da je kompjuterski sistem uključen.
3. Ako je ekran i dalje bez slike i kućište kompjuterskog sistema ne pokazuje znakove da je sistem uključen i u pogonu, preći na korak "Ako je kompjuterski sistem isključen".

2.4.3.42. Ako je kompjuterski sistem isključen

2.4.3.42.1. Prikupljanje digitalnih dokaza sa kompjuterskih sistema tipa desktop-a, tower-a, i mini računara

Za kompjuterske sisteme poput desktop-a, tower-a, i mini kompjutera preduzeti slijedeće korake:
1. Dokumentovati, fotografisati, i skicirati cijelu mrežu kablova, žičanih spojeva, i druge uređaje koji su spojeni na kompjuterski sistem.
2. Pojedinačno označiti sve kablove i žičane spojeve uključujući spojeve svih dodatnih perifernih uređaja spojenih na kompjuterski sistem.
3. Fotografisati označene kablove, žičane spojeve kompjuterskog sistema kao i označene spojeve dodatnih perifernih uređaja.
4. Otkačiti kabel za napajanje kompjuterskog sistema električnom energijom iz zidne utičnice ili produžnog kabla ili UPS uređaja za neprekidno napajanje i sačuvati ga.
5. Isključiti i sačuvati sve ostale kablove i žičane spojeve sa kompjuterskog sistema zatim dokumentovati kablove i žičane spojeve dodatnih uređaja.

6. Zalijepiti samoljepljivu traku preko otvora floppy uređaja ako je instalisan na kompjuterskom sistemu.
7. Po potrebi ladice CD/DVD/BD ili sličnog uređaja vratiti unutar uređaja. Pregledati dali se u ladici nalazi medij ako je moguće zatim samoljepljivom trakom zalijepiti zatvorenu ladicu kako bi se spriječilo otvaranje.
8. Zalijepiti samoljepljivu traku preko prekidača za paljenje kompjuterskog sistema.
9. Zapisati ime proizvođača, model, serijske broj(eve), i druge oznake ako postoje na kompjuterskom sistemu.
10. Sačiniti listu kompjuterskog sistema uključujući sve kablove, žičane spojeve i dodatne uređaje koristeći nadležna uputstva i pravilnike službe istražnog organa.
11. Izvršiti pakovanje svih prikupljenih dokaza po instrukcijama pravilnika istražnog organa i preduzeti sve preventivne mjere da ne bi došlo do oštećenja ili izmjene dokaza tokom transporta i skladištenja.

2.4.3.42.2. Prikupljanje digitalnih dokaza sa kompjuterskih sistema tipa laptopa, notebook-a ili netbook-a

Za kompjuterske sisteme poput laptopa, notebook-a ili netbook-a preduzeti slijedeće korake:
1. Dokumentovati, fotografisati, i skicirati cijelu mrežu kablova, žičanih spojeva, i druge uređaje koji su spojeni na kompjuterski sistem.
2. Pojedinačno označiti sve kablove i žičane spojeve uključujući spojeve svih dodatnih perifernih uređaja spojenih na kompjuterski sistem.
3. Fotografisati označene kablove, žičane spojeve kompjuterskog sistema kao i označene spojeve dodatnih perifernih uređaja.
4. Otkačiti kabel za napajanje kompjuterskog sistema električnom energijom iz zidne utičnice ili produžnog kabla ili UPS uređaja za neprekidno napajanje i sačuvati ih. Odvojiti bateriju i sačuvati je zajedno sa ostalim prikupljenim baterijama ako postoje.
   Isključiti i sačuvati sve ostale kablove i žičane spojeve sa kompjuterskog sistema zatim dokumentovati kablove i žičane spojeve dodatnih uređaja.
5. Zalijepiti samoljepljivu traku preko otvora floppy uređaja ako je instalisan na kompjuterskom sistemu.
6. Po potrebi ladice CD/DVD/BD ili sličnog uređaja vratiti unutar uređaja. Pregledati dali se u ladici nalazi medij ako je moguće zatim samoljepljivom trakom zalijepiti zatvorenu ladicu kako bi se spriječilo otvaranje.
7. Zalijepiti samoljepljivu traku preko prekidača za paljenje kompjuterskog sistema.
8. Zapisati ime proizvođača, model, serijske broj(eve), i druge oznake ako postoje na kompjuterskom sistemu.
9. Sačiniti listu kompjuterskog sistema uključujući sve kablove, žičane spojeve i dodatne uređaje koristeći nadležna uputstva i pravilnike službe istražnog organa.
10. Izvršiti pakovanje svih prikupljenih dokaza po instrukcijama pravilnika istražnog organa i preduzeti sve preventivne mjere da ne bi došlo do oštećenja ili izmjene dokaza tokom transporta i skladištenja.

2.4.3.43. . Ako je kompjuterski sistem uključen

Tokom izvođenja istražnih radnji najbolja i najbezbjednija opcija prilikom izuzimanja kompjuterskog sistema je isključenje kompjuterskog sistema sa napajanja električnom energijom. U slučaju da je digitalni dokaz vidljiv na ekranu monitora potrebne su dodatne istrage i dokumentovanje od strane ovlaštenog osoblja prije isključenja sistema sa napajanja.

Hitno isključenje je preporučljivo u slijedećim situacijama:

- Informacije ili aktivnosti na ekranu monitora ukazuju na brisanje (delete) ili presnimavanje novih podataka preko starih (overwriting)
- Informacije ili aktivnosti na ekranu monitora ukazuju na uništavanje podataka na uređajima za pohranu.
- Isključenjem kompjuterskog sistema na kojem je instalisan Microsoft(R) Windows(R) operativni sistem sačuvat će se informacije o zadnjem korisniku prijavljenog na sistem, poput tačnog vremena, zadnjih korištenih dokumenata, komandi kao i druge informacije.

Isključenje kompjuterskog sistema sa napajanja električne mreže nije preporučljivo u slijedećim situacijama:

- Podaci prikazani na ekranu monitora predstavljaju potencijalne digitalne dokaze. U ovakvim situacijama potrebna stručna pomoć ovlaštenog osoblja istražnih organa.
- Postoje pokazatelji koji ukazuju da se koriste ili se odvijaju slijedeće aktivnosti:
- Chat sobe
- Otvoreni tekstualni dokumenti
- Pregledi pohranjenih podataka na udaljenoj fizičkoj lokaciji odnosno na drugim serverima
- Programi instantnih poruka
- Dječija pornografija
- Šverc (neovlašteni promet)
- Finansijske dokumente
- Zaštita podataka
- Opšte ilegalne aktivnosti

Vršenje istražnih radni i prikupljanje digitalnih dokaza kompjuterskih sistema kao sto su serveri ili grupe umreženih kompjuterskih sistema moraju se vršiti od strane treniranog i ovlaštenog osoblja koje ima iskustva sa sličnim kompjuterskim i mrežnim sistemima. Velika grupa umreženih i kompleksnih kompjuterskih sistema zahtijeva poseban pristup i način obrade.

2.4.3.44. . Dodatni dokazi u drugim obliku

Lice mjesta izvođenja kriminalnih radnji u većini slučajeva može sadržati i ostale vrste dokaza ili materijale i predmete koji mogu ukazivati ili pomoći istražnim organima u pronalaženju i rasvjetljavanju kriminalnog djela. Pronađeni predmeti, zapisnici, papiri, ostaci papira sa rukopisima, zapisane lozinke, adrese, prazni listovi dnevnika koji sadrže utisnute tragove pisanja, knjige, softver, hardver, uputstva, literatura, označeni datumi, kalendari, tekst ili grafički materijal štampan sa kompjuterskog sistema. Ove vrste dokaza takodje treba dokumentovati i sačuvati u skladu sa pravilima i procedurama istražnih organa.

2.4.3.45. . Ostala elektronika i periferni uređaji kao potencijalni dokazi

Lice mjesta kriminalnih radnji može sadržavati dodatnu elektroniku i periferne uređaje koji mogu pomoći istražne radnje kao i služiti potencijalni dokazi i biti od posebnog značaja vezanih za istragu. Osim u hitnim slučajevima takve uređaje nije preporučljivo uključivati ili koristiti i pristupati informacijama. Ako hitnosti nalaže takvo postupanje i zahtijeva hitan pristup informacijama onda svaka aktivnost mora biti dokumentovana. Nestručno rukovanje kao i informacije koje sadrži mogu biti izgubljene odnosno oštećene. Slijedeći navedeni

primjeri predstavljaju elektronske uređaje, komponente, i periferijske koji mogu poslužiti kao digitalni dokaz:

- Audio snimači
- GPS uređaji
- Uređaji sa automatskom sekretaricom
- Kompjuterski čipovi
- Pejdžeri
- Telefoni uključujući bežične telefone
- Uređaji za kopiranje
- Mobilni telefoni
- Hard disk duplikatori
- Fax uređaji
- Štampači
- Multifunkcijski uređaji (štampači, skeneri, kopir i fax uređaji)
- Uređaji za pristup bežičnog umrežavanje (Wireless access points)
- Uređaji vezani za napajanje laptopa kao i dodatni uređaji
- Smart kartice (smart cards)
- Video rekorderi (VCRs)
- Skeneri
- Telefoni i uređaji koji pokazuju korisnički pozivajući broj
- PCMCIA memorijske kartice
- Mobilni Digitalni Asistent uređaji (PDAs)

Ovakvi uređaji zahtijevaju stručno rukovanje kako bi se sačuvao integritet informacija koje mogu poslužiti kao digitalni dokazi. Preporučljivo je da ovim uređajima rukuje isključivo stručno i trenirano osoblje u prikupljanju dokaza. Ako postoje punjači za napajanje električnom energijom pomenutih uređaja, kablovi, žičani spojevi, kao i njihove dodatne ili periferijske komponente potrebno ih je također sačuvati zajedno sa uređajima.

2.4.3.46. Kompjuterski sistemi u poslovnom okruženju

Poslovna okruženja često imaju komplikovane konfiguracije više mrežno povezanih kompjuterskih sistema, servera, mrežnih uređaja, ili kombinacije istih. Obezbjeđivanje lica mjesta i prikupljanje digitalnih dokaza u ovakvim okruženjima predstavlja dodatne izazove naročito za ovlaštena lica koja pristupaju obradi. Svako nestručno isključivanje sistema može rezulturati gubitkom podataka, gubitkom dokaza, kao i izazvati potencijalne odgovornosti istražnih organa. U pojedinim slučajevima istražnim organima različiti operativni sistemi ili posebne hardverske ili softverske konfiguracije mogu predstavljati dodatne izazove jer zahtijevaju posebne procedure za isključivanje[110].

2.4.3.47. Pakiranje,transport i skladištenje prikupljenih dokaza

Digitalni dokazi sa kompjuterskim sistemima i elektronskim uređajima na kojima su pohranjeni su lomljivi i osjetljivi na ekstremne temperature, vlažnost, fizičke udare, statički elektricitet i magnetna polja.

[110] Izvor: www.nij.gov/nij/pubs-sum/219941.htm, Electronic Crime Scene Investigation A Guide for First Responders, Second Edition by National Institute of Justice, April 2008

Istražni organi moraju preduzeti sve mjere i predostrožnosti prilikom dokumentovanja, fotografisanja, pakiranja, transporta, i skladištenja digitalnih dokaza da bi se izbjeglo promjena, oštećenje, ili uništavanje podataka.

2.4.3.48. Procedure pakiranja

Sve aktivnosti koje se preduzimaju po osnovama identifikacije, prikupljanja, pakiranja, transporta, i skladištenja digitalnih dokaza se mora pažljivo dokumentovati. Prilikom pakiranja digitalnih dokaza za transport, potrebno je:

- Pobrinuti se da prikupljeni digitalni dokazi su pravilno dokumentovani, označeni, markirani, fotografisani, ili snimljeni video uređajima, skicirani, izvršena inventura prije pakiranja. Svi spojeni uređaji takođe trebaju biti označeni za što lakše sastavljanje sistema po potrebi.
- Takođe voditi računa o tome da digitalni dokazi mogu sadržavati skrivene tragove, otiske ili druge dokaze biološke prirode za koje je potrebno preduzeti posebne korake da bi se sačuvali. Snimanje ili fotografisanje digitalnih dokaza se mora izvesti prije procesiranja dokaza u vezi skrivenih tragova, otisaka ili drugih dokaza biološke prirode.
- Zapakovati sve digitalne dokaze pomoću antistatičke ambalaže. Samo papirne vrećice i koverte, kartonske kutije, i antistatički kontejneri bi se trebali koristiti za pakiranje digitalnih dokaza. Plastični materijali se ne bi trebali koristiti za prikupljanje digitalnih dokaza zbog toga što plastika može proizvesti ili prenijeti statički elektricitet i omogućiti pojavu vlažnosti i kondenzacije koji mogu uništiti dokaze.
- Zapakovati sve digitalne dokaze na način koji sprečava savijanje, grebanje, kao i druge vrste deformacija.
- Označiti sve kontejnere koji su se koristili za pakiranje i smještaj digitalnih dokaza.
- Mobilne telefone i smart telefone ostaviti uključene ili isključene zavisno od stanja u kojem su pronađeni.
- Mobilne i smart telefone zapakovati ambalažu izrađenu od materijala koji blokiraju signal kao što su Faradejeve izolacione vreće (faraday isolation bags), materijal za zaštitu od radio frekvencija, ili aluminijsku foliju koja sprečavaju primanje ili slanje poruka sa uređaja. U slučaju vađenja ili nepravilnog pakiranja iz zaštitne ambalaže, uređaj može slati ili primati podatke ili poruke ako prime signal u zoni komuniciranja.
- Prikupiti sve uređaje za napajanje, adaptere za elektronske uređaje koje se oduzimaju prilikom istražnih radnji

2.4.3.49. Transportne procedure

Prilikom transporta digitalnih dokaza potrebno je:

- Držati uređaje dalje od magnetnog polja koje proizvode radio odašiljači, magneti u zvučnicima, svjetla opasnosti koji se postavljaju pomoću magneta. Drugi potencijalni izvori na koje treba obratiti pažnju su grijači sjedišta ili slični uređaji koji proizvode statički elektricitet.
- Izbjegavati od držanja digitalnih dokaza u vozilima na duži period vremena. Toplota, hladnoća, i vlažnost mogu oštetiti ili uništiti digitalne dokaze.
- Obezbijediti sva pakovanja u kojima se nalaze prikupljeni kompjuterski i elektronski uređaji tokom transporta kako bi se spriječila oštećenja izazvana udarom ili vibracijama.
- Dokumentovati transport digitalnih dokaza i zadržati spisak svih preuzimanja ili promjene nosioca posjedovanja svih dokaza koji se transportuju.

2.4.3.50. Procedure skladištenja

Za skladištenje digitalnih dokaza potrebno je:

- Obezbijediti da je izvršena inventura nad digitalnim dokazima u skladu sa pravilnikom istražnih organa
- Prostor u koji se smještaju digitalni dokazi bude bezbjedan, klimatski kontrolisan i da lokaciju koja ne podliježe ekstremnim temperaturama ili vlažnosti.
- Pobrinuti se da digitalni dokazi nisu izloženi magnetnom polju, vlažnosti, prašini, vibracijama ili bilo kojem drugom elementu koji ga može oštetiti ili uništiti.

Važni potencijalni digitalni dokazi mogu uključivati datume, vremena, i stanja sistemskih konfiguracija koja mogu biti izgubljena zbog predugog skladištenja ili zbog pražnjenja baterija ili drugih izvora punjenja koji čuvaju pomenute informacije. Po potrebi informisati nadležna lica istražnih organa koji upravljaju digitalnim dokazima da elektronski uređaji zahtijevaju pregled ili druge aktivnosti u vezi zaštite podataka koji su pohranjeni na njima.
U slučaju da je više od jednog kompjuterskog sistema oduzet kao dokaz prilikom istražnih radnji, sve kompjuterske sisteme, kablove, i uređaje koji su spojeni na njih moraju se označiti samoljepljivim naljepnicama kako bi omogućili ponovno sastavljanje u slučaju potrebe[111].

2.4.3.51. Elektronski kriminal i kategorisanje digitalnih dokaza

Lista elektronskog kriminala prikazana ispod nije konačna lista svih mogućih oblika kriminalnih djela ali omogućava lakše raspoznavanje i identifikaciju izvor potencijalnih digitalnih dokaza po kategorijama kriminalnih djela. U zavisnosti od kompleksnosti lica mjesta i situacije koja je zatečena pristup često zahtijeva prisustvo više stručnih i ovlaštenih lica istražnog organa.

U zavisnosti od zatečene situacije okolnosti, nevidljivi tragovi, ili biološki dokazi poput otisaka prstiju, DNK može da bude jednako važna za istragu i može se nalaziti na kompjuterskim sistemima ili drugim digitalnim uređajima. Ovakve situacije zahtijevaju praćenje aktivnosti i pravila istražnog organa za pristup i način oduzimanja takvih uređaja. Sve aktivnosti koje bi mogle dovesti do oštećenja i koja su povezana sa procesima analiziranja za otkrivanja tragova, nevidljivih tragova, bioloških i drugih dokaza trebaju sačekati dok se ne završi otkrivanje, ispitivanje i analiza digitalnih dokaza.

Službeno lice koje se prvo našlo licu mjesta treba da obrati pažnju i prikuplja slijedeće informacije:

- Kratki pregled o kriminalnom djelu
- Lozinke za uređaje koji se oduzimaju
- Kontakt informacije i nadležnost vezane za istražne radnje
- Rane izvještaje i dokumentaciju
- Listu ključnih riječi
- Listu kriminalnih aktivnosti
- Informacije o osumnjičenim licima uključujući nadimke

[111] Izvor: www.nij.gov/nij/pubs-sum/219941.htm, Electronic Crime Scene Investigation A Guide for First Responders, Second Edition by National Institute of Justice, April 2008

2.4.3.51.1. Zloupotrebljavanje i iskorištavanje djece

Potencijalni digitalni dokazi vezani za istrage zloupotrebljavanje ili iskorištavanja djece uključuju:

- Kompjuteri
- Skeneri
- Mobilni komunikacioni uređaji
- Video, foto kamere i mediji
- Kalendari ili dnevnici
- Softver za digitalne kamere
- Informacije o internet aktivnostima
- Softver za pregledanje i uređivanje fotografija
- Štampani e-mailovi, bilješke, pisma i mape
- Štampane fotografije ili slike
- Bilješke ili zapisnici chat sesija
- Web kamere i mikrofoni
- Kompjuterske igre
- Štampači i kopirni uređaji
- Informacije skrivene u pisanju (steganografy)
- Izmjenjive medije
- Eksterne uređaje za pohranjivanje podataka
- Video kasete
- Konzole za video igre, igre, i proširenja
- Reference za korisnički kreirane foldere imena datoteka pod kojima su sačuvane slike

2.4.3.51.2. Upadi u kompjuterski sistem

Prikupljanje potencijalnih digitalnih dokaza o upadima u kompjuterske sisteme uključuje:

- Kompjutere
- Mrežni uređaje, rutere, svičeve (switches)
- Ručne mobilne uređaje
- Antene
- Prenosive medije
- Eksterne uređaje za pohranu podataka
- Web kamere
- Oprema za bežična umrežavanja
- Kontakt liste i adresare
- Liste adresa internet protokola
- Liste ili podatke o korištenim softverima za upad
- Zabilješke i zapisnike internet chat sesija
- Štampane e-mailove, zabilješke ili pisma
- Štampani kompjuterski programski kod
- Izvršne programe (executable programs)
- Liste kompjutera kojima se pristupalo
- Zabilješke i zapisnike internet aktivnosti
- Korisnička imena i lozinke

2.4.3.51.3. Falsifikovanje/krivotvorenje/Counterfeiting

Potencijalni digitalni dokazi u istražnim radnjama falsifikovanja uključuje:
- Kompjutere
- Ručne mobilne uređaje
- PDA uređaje ili adresare
- Informacije vezane za internet aktivnosti
- Informacije vezane za čekove, valute, i slično
- Izmjenjive medije i eksterne uređaje za pohranu podataka
- Čitači magnetne trake kreditnih kartica
- Online softveri za bankarstvo
- Kalendari
- Reprodukcije potpisa
- Informacije o klijentima ili podatke o kreditnim karticama
- Lažne isprave
- Štampane e-mailove, zabilješke i pisma
- Lažne forme za finansijske transakcije
- Informacije o finansijskim podacima
- Štampane baze podataka

2.4.3.51.4. Istraživanje ubistva

Potencijalni digitalni dokazi prilikom istraživanja ubistva uključuje:
- Kompjutere
- Račune za internet servise
- Izmjenjive medije
- Eksterne uređaje za pohranu podataka
- Uređaje za mobilnu komunikaciju
- PDA uređaje
- Adresare i kontakt informacije
- Liste telefonskih poziva
- Ručno pisane materijale i dnevnike
- Medicinsku dokumentaciju
- Štampane e-mailove, zabilješke, i pisma
- Finansijsku ili imovinsku dokumentaciju
- Zadnje štampane materijale
- Informacije vezane za pravnu dokumentaciju
- Informacije vezane za internet aktivnosti
- Softvere za ostavštinu ili reference

2.4.3.51.5. . Porodično naselje, prijetnje i iznude/ucjene

Potencijalni digitalni dokazi vezani za domaće nasilje, prijetnje, i iznude uključuje:
- Kompjutere
- Izmjenjive medije
- Korisnička imena i račune
- Eksterne uređaje za pohranu podataka
- Uređaje za mobilnu komunikaciju

- Liste telefonskih poziva
- PDA uređaje ili adresare
- Finansijsku ili imovinsku dokumentaciju
- Ručno pisani materijali i dnevnike
- Informacije vezane za internet aktivnosti
- Štampane e-mailove, zabilješke i pisma
- Pravne dokumente
- Uređaje za prikazivanje broja pozivaoca

2.4.3.51.6. Email prijetnje,uznemiravanje i praćenje

Potencijalni digitalni dokazi vezani za e-mail prijetnje, uznemiravanje, i praćenje uključuje:
- Kompjutere
- Ručne mobilne uređaje
- PDA uređaje ili adresare
- Liste telefonskih poziva
- Dnevnike ili zapisnike o nadgledanju
- Dokaze o istraživanju podataka o žrtvama
- E-mailove, zabilješke, i pisma
- Finansijsku ili imovinsku dokumentaciju
- Štampane fotografije ili slike
- Pravne dokumente
- Informacije o internet aktivnostima
- Štampane mape

2.4.3.51.7. Kockanje/klađenje

Potencijalni digitalni dokazi o istraživanjima kockanja uključuje:
- Kompjutere
- Izmjenjive medije
- PDA uređaje, adresare, ili kontakt liste
- Eksterne uređaje za pohranjivanje podataka
- Baze podataka o klijentima i učesnicima kockanja
- Informacije o internet aktivnostima
- Elektronske transfere novca
- Softver za online bankarstvo
- Kalendare
- Sportsku kockarsku statistiku
- Informacije o klijentima i kreditnim karticama
- Finansijsku imovinsku dokumentaciju
- Štampane e-mailove, zabilješke i pisma
- Reference za sajtove za online kockanje

2.4.3.51.8. Krađa identiteta

Potencijalni digitalni dokazi o krađi identiteta uključuje:
- Kompjutere
- Mobilne uređaje

- Dokumentaciju za online kupovinu
- Izmjenjive medije
- Eksterne uređaje za pohranjivanje podataka
- PDA uređaje, adresare, kontakt liste
- Softver za online bankarstvo
- Informacije o internet aktivnostima
- Finansijsku imovinsku dokumentaciju
- Elektronske transfere novca
- Laminatore
- Kalendare ili dnevnike
- Falsifikovana dokumenta ili lažne isprave
- Informacije o žrtvama i kreditnim karticama
- Kopije potpisa
- Štampane e-mailove, zabilješke i pisma
- Fotografije za lična dokumenta
- Kartice za unovčavanje čekova
- Skenere

2.4.3.51.9. Narkotici

Potencijalni digitalni dokazi kod istrage o narkoticima uključuje:
- Kompjutere
- Ručne mobilne uređaje
- Izmjenjive medije
- Eksterne uređaje za pohranjivanje podataka
- PDA uređaje, adresare, kontakt liste
- Falsifikovana dokumenta
- Baze podataka
- Informacije o internet aktivnostima
- Potvrde za prijemu lijekova
- Neispunjene recepte za lijekove
- Štampane e-mailove, zabilješke i pisma
- Finansijsku imovinsku dokumentaciju
- GPS uređaje

2.4.3.51.10. Online prevare ekonomske prirode

Potencijalni digitalni dokazi vezani za online prevare ekonomske prirode uključuje:
- Kompjutere
- Izmjenjive medije
- Uređaje za mobilnu komunikaciju
- Eksterne uređaje za pohranjivanje podataka
- Online aukcije i podatke o računima
- Baze podataka
- PDA uređaje, adresare, liste kontakata
- Štampane e-mailove, zabilješke i pisma
- Kalendare ili dnevnike
- Finansijsku imovinsku dokumentaciju

- Softveri za računovodstva ili finansijske podatke
- Fotografije i slike u štampanom i digitalnom obliku
- Zapisnike ili bilješke od chat sesija
- Informacije vezane za internet aktivnosti
- Kreditne informacije od klijenata
- Informacije online bankarstva
- Liste sa brojevima kreditnih kartica
- Telefonske brojeve i liste poziva
- Čitače magnetne trake kreditnih kartica
- Obračune vezne za kreditne kartice ili račune
- Štampače, kopire, i skenere

2.4.3.51.11. Prostitucija

Potencijalni digitalni dokazi vezani za istrage prostitucije uključuje:
- Kompjutere
- Ručne mobilne uređaje
- Izmjenjive medije
- Eksterne uređaje za pohranjivanje podataka
- Adresare i liste klijenata
- Baze podataka i zabilješke vezane za klijente
- Kalendare i rasporede sastanka
- Falsifikovane dokumente
- Informacije vezane za internet aktivnosti
- Finansijsku imovinsku dokumentaciju
- Štampane e-mailove, zabilješke i pisma
- Informacije vezane web stranicu
- Medicinsku dokumentaciju
- Web kamere

2.4.3.51.12. Piratstvo softverom

Potencijalni digitalni dokazi vezani za piratstvo softverom uključuje:
- Kompjuterske sisteme
- Ručne mobilne uređaje
- Izmjenjive medije
- Eksterni uređaji za pohranjivanje podataka
- Informacije vezane za chat sesije
- Informacije vezane za skidanje zaštite sa softvera (cracking software)
- Štampani e-mailovi, zabilješke i pisma
- Reference za zaštićeni softver
- Falsifikovani softverski certifikati
- Liste sa kodovima za aktiviranje softvera
- Informacije vezane za internet aktivnosti
- Softveri za dupliciranje i materijali za pakiranje

2.4.3.51.13. Telekomunikacijske prevare

Potencijalni digitalni dokazi vezani za telekomunikacijske prevare uključuje:
- Kompjutere
- Ručne mobilne uređaje
- Izmjenjive medije
- Eksterne uređaje za pohranjivanje podataka
- Softver i kablove za programiranje telefona
- Više telefonskih uređaja
- Čitače SIM kartica (Subscriber Identity Module)
- Hakerske kutije i kablovi
- Liste i baze podataka o klijentima
- Ukradene telefone
- Štampane e-mailove, zabilješke i pisma
- Finansijsku imovinsku dokumentacija
- Informacije vezane za internet aktivnosti
- Uputstva za programiranje telefona
- EPROM snimače (Erasable programmable read-only memory burner)

2.4.3.51.14. Terorizam

Potencijalni digitalni dokazi vezani za terorizam uključuje:
- Kompjutere
- Ručne mobilne uređaje
- Izmjenjive medije
- Eksterne uređaje za pohranjivanje podataka
- Komunikacijske uređaje
- Mrežne komponente, rutere, svičeve (switches)
- VoIP (Voice over Internet Protocol) uređaje
- GPS uređaje
- Informacije vezane za internet aktivnosti
- Informacije vezane za steganografiju-informacije skrivene u pisanju (steganography)
- Štampane e-mailove, zabilješke i pisma[112]

[112] Izvor: http://www.nij.gov/nij/pubs-sum/219941.htm, Electronic Crime Scene Investigation A Guide for First Responders, Second Edition by National Institute of Justice, April 2008

3. PRANJE NOVCA

3.1. Uvod

Ogroman napredak u razvoju informacionih tehnologija, korištenje interneta, jeftini informatički resursi (mogućnost nabavke personalnog računara od strane pojedinca, zakup i usluge internet provajdinga), kao i ostvarivanje dugogodišnjeg sna ”kupovina i plaćanje iz doma” preko mreže, uz posjedovanje platne kartice za plaćanje elektronskim novcem, stvorili su i preduslove da se u glavama pojedinaca i grupa stvori ideja za zloupotrebu istih u svrhu pranja novca.

Ovakvo definisano okruženje kao jednu od bitnih determinanti ima i ekspanziju zloupotrebe informaciono-komunikacionih tehnologija do neslućenih granica. Zbog toga, ali svakako ne samo zato, pranje novca prerasta od usko nacionalnog i eventualnog regionalnog u primarni problem regionalne i globalne sigurnosti. Koji će najvjerovatnije biti u fokusu svjetske politike i tokom prvih dekada 21.vijeka. Trendovi međunarodne trgovine, tokovi novca i kapitala, kretanje ljudi, dobivaju nove pojavne oblike i gube neke od ograničenja. Nastaju nove mogućnosti, ali i još nepoznati rizici koje nije moguće sagledati do kraja. Pranje novca kao kriminalna djelatnost jedno je od najštetnijih krivičnih djela. Stepen organizacije koji to djelo karakterizira, sofisticiranost i raznolikost načina njegovog izvođenja te njegov međunarodni karakter i činjenica da je najveći broj krivičnih djela organiziranog kriminala karakteriziran imovinskom koriśću kao osnovnim motivom, pri čemu je pranje novca prateće kazneno djelo, nedvojbeno to djelo čini jednim od najopasnijih krivičnih djela današnjice, kojeg prevencija i otkrivanje zahtijevaju iznimnu osposobljenost, ekipiranost i predanost organa za prevenciju i provođenje zakona, njihovu organiziranost, znanje raznolikih područja i koordinaciju pojedinih područja djelovanja. Sadržajem ovog edukativnog modela nastojalo se prikazati osnovne karakteristike tog kaznenog djela u vezi sa *cyber* crime, njegovi (do sada poznati) najčešći pojavni oblici do i nakon Interneta kao, postojeća međunarodna i domaća pravna regulativa Posebna pažnja je posvećena je procesnom pitanju sticanje, čuvanja i upotrebe dokazivanja preko digitalnih dokaza, osobito s obzirom na međunarodne trendove u tom smislu.

3.2. Pojam i karakteristike pranja novca

Između mnogobrojnih definicija ovog pojma , koje pretendiraju biti sveobuhvatne (pri čemu to bjelodano nije nijedna), smatramo da najbolje oslikava prirodu stvari ona koja pojam pranja novca najkvalitetnije definira danas važeća Direktiva 2005/60/EZ o sprječavanju korištenja financijskog sustava u svrhu pranja novca i financiranja terorizma, kao: prikrivanje prave prirode, izvora novca, pretvorbu i prijenos imovine u smislu prikrivanja njenog protuzakonitog porijekla, odnosno nabavu, posjedovanje ili upotrebu imovine proizašle iz kaznenog djela. Jednako tako, podrazumijeva i sudjelovanje, povezanost, pokušaj pomaganja, poticanja te omogućavanje izvršenja bilo koje od *supra* navedenih radnji.

Iz odredaba Direktive 2005/60/EZ vidljiv je odmak od tradicionalnog poimanja pranja novca kao „pretvorbe prljavog u čisti novac“, „pranja novca od trgovine drogom“ ili „prikrivanje prljavog novca“ (elastično ili preusko definirano). Moderna informaciono-komunikacijska tehnologija, alternativni načini pranja novca putem nefinancijskog sektora i nepresušna mašta kriminalaca mogli bi pomoći pri formuliranju moderne definicije pranja novca koja bi govorila u prilog tome da se pranje novca javlja prilikom provođenja *bilo koje* transakcije ili

odnosa koji obuhvaća sve oblike imovine ili imovinske koristi, u materijalnom ili nematerijalnom obliku, a koja proizlazi iz nezakonitog djelovanja.

„ Brojni udžbenici koji se bave pranjem novca tvrde da postoje četri zajednička faktora za sve takve operacije .Prvi polazi od činjenice da nema potrebe za pranjem ako svako zna čije su pare kad one izađu iz mašine za pranje.Dakle, prvo pravilo je da vlasništvo i porijeklo moraju biti sakriveni.Drugi faktor, podrazumjeva da novac mora promjeniti oblik.Niko ne pere novac da bi od tri miliona dolara u apoenima od 20 dolara na kraju dobio tri miliona dolara u apoenima od 20 dolara.Zato se gotovina pretvara u sredstva na bankovnim računima, skupe slike, luksuzne vile, automobile, zemljište, čekove.....Američke vlasti su prije nekoliko godina utvrdile,recimo,da su pare prane preko računa otvorenih na ime Merlin Monro, Zeka Rodžer, Me Vest, Abraham Linkoln.....Promjena oblika, kad je riječ o ogromnim iznosima gotovine, znači i smanjenje obima. Jer, suprotno opštem uvjerenju, dva miliona dolara ne mogu stati u aktn-tašnu:dva miliona dolara u novčanicama od 20 dolara je gomila visoka bar tri metra. Treći, trag koji ostaje iza novca mora biti nejasan. Cilj čitave operacije je propao ako neko može ući u trag parama od početka do kraja. Zato se ona sprovodi kroz bezbroj bankarskih računa, preko lažnih banaka i lažnih kompanija. Recimo ,otvorite firmu ili banku na Holandskim Antilima i tamo položite svoj ilegalno zarađeni novac. Uz pomoć dobrih veza, prebacite pare u Roterdam, na račun brodske kompanije registrovane u Panami sa sjedištem na Kipru. Ona ih pošiljke u Singapur, na račun osiguravajućeg društva registrovanog u Lihtenštajnu sa sjedištem na Ajsl of Main (Isle of Men), odakle pare idu na račun građevinske kompanije registrovane u Hongkongu koji radi u Monaku, a ima račun u Los Anđelesu. I tako bar četrdeset puta. Ako ste spretni i brzi cijeli posao možete obaviti za manje od sata. I na kraju (četvrti), ma kroz kakve i ma kroz koliko operacija novac prolazio pri pranju,nad njim uvijek treba imati kontrolu. Svi ljudi umiješani u posao znaju da je riječ o prljavim parama i da njihov vlasnik malo šta može učiniti ako ih ukradu. Koliko je opasno ne poštovati ovo pravilo uvjerila su se četiri Mađara početkom 1992.godine.Sa 2,6 miliona njemačkih maraka u rukama ušli su jednog dana u glavnu zgradu čuvene švajcarske banke Kredi Svis,na Paradeplacu u Cirihu, gdje su imali zakazan sastanak. U velikom mermernom holu prišli su im dvojica muškaraca koji su se predstavili kao službenici banke. Dok je jedan sa koferima punim para otišao u sobu da ih prebroji, drugi Mađare pozvao na kafu. Pošto se onaj prvi nije pojavljivao ovaj drugi je otišao „da provjeri gdje je“i više se nije vratio. Nedjelju dana kasnije isto se proveo i jedan kanadski biznismen koji je opet u Kredi Svis na Parade place-došao sa torbom u kojoj je bilo 2,5 miliona dolara u švajcarskim francima. Banka se sprovela istragu i utvrdila da niko iz nje nije bio umješan i ostalo je nejasno kako je sve bilo moguće. Pokazalo se, ipak, da i nad lopovima ima lopova“.[113]

Pranje novca je zapravo proces, a ne pojedinačan čin, pri kojem se koriste mnoge tehnike, a može se teoretski podijeliti u tri faze.

3.3. Faze pranja novca

Bez obzira koje korake kriminalci poduzimaju pri operacijama pranja novca, većina shema pranja novca uključuje neke ili sve od tri klasične faze. Svaka knjiga ili priručnik o pranju novca počinju sa opisom tri faze, zatim opisuju svaku od faza ponaosob tako da je faza plasmana uvijek popraćena fazom uslojavanjem nakon kojeg slijedi neizbježna faza integracije. Međutim, linearno razmišljanje može biti veoma varljivo. Na primjer, nezakonito

[113]Mr. Dragan Đurđević,dokotorant na Fakultetu civilne odbrane u Beogradu,Pranje novca i zlopotreba informacionih tehnologija, Ziteh,Beograd, 2010.(www.singipedia.com ,08.02.2012.,23,58)

stečen novac može se miješati s legalnim novcem prije ulaganja u finansijski sistem (npr. sa gotovinom kockarnica, restorana, barova, fitnes klubova,taksi službi i sl.). Pored, navedenog moguće je i da nelegalno stečen novac nikad ne uđe u legalne tokove finansijskog sistema i da se kreće kroz razne modele paralelnog/podzemnog bankarskog sistema odnosno alternativnog sistema doznaka kao što hawala/hundi[114], crno devizno tržište pezosa[115] ili fei cien[116]. Međutim, u potpunosti razumjeti proces pranje novca može se samo ako se prethodno temeljito savladaju njegove osnovne tri faze .

Svrha pranja novca je da se smanji ili potpuno isključi rizik od otkrivanja, praćenja i oduzimanja protupravno stečenih sredstava ili imovine i kazne za počinitelje krivičnih djela. U svim slučajevima kada kriminalci posjeduju protivpravno stečena sredstva suočavaju se sa činjenicom kako da protivpravno stečena sredstva nesmetano koriste, a da pri tome ne ostave nikakav trag koji bi mogao da ukaže na njihovu kriminalnu djelatnost. Da bi ostvarili svoje ciljeve kriminalci pristupaju realizaciji pranja novca koristeći različite načine pranja novca koji se mogu kobinovati u manje ili više složene šeme pranja novca.

Osnovu većine identificiranih šema pranja novca, u različitim varijacijama, čine tri faze pranja novca poznate kao plasman (polaganje), pokrivanje (uslojavanje) i integracija (prožimanje).

[114] Havala/hundi je alternativni sistem doznaka koji je nastao u južnoj Aziji,ali je danas raširen svuda po svijetu slijedeći emigrantske tokove iz tog regiona. Hawala je tradicionalni metod kretanja sredstava povezan sa kretanjem prihoda od legalnog poslovanja, kao i kretanja prihoda od narkotika, krijumčarenja i kršenja carinskih i akciznih propisa. Sistem funkcionira preko pojedinačnih hawala operatera koji prikupljaju sredstva na jednom kraju operacije do drugih koji ta sredstva distribuiraju na kraj. Klijent dolazi do operatera u jednoj zemlji i zahtijeva da mu se sredstva prebace u drugu zemlju. Operater skupa u kontakt sa drugim operaterom telefonom ili faksom u naznačenoj zemlji i daje nalog za isplatu dostavljene sume umanjene za proviziju. Ove transakcije obavljaju se u oba smjera. U slučaju kada računi pojedinačnih operatera nisu izravnati, oni se poravnavaju recipročnim doznakama, manipulacijama sa fakturama, krijumčarenjem zlata i dijamanata, fizičkim kretanjem novca ili preko komercijalnih bankarskih sistema. Operateri se najčešće bave i nekom legalnom aktivnošću što omogućava veći stepen prikrivenosti operacija.

[115] Ovaj altrenativni sistem doznaka je nastao u Latinskoj Americi, kao paralelni finansijski sistem za podršku legitimnoj trgovini i krijumčarenju između Sjeverne i Južne Amerike. Njegov razvoj je bila reakcija na nemogućnost finansijskih sistema da pruže pouzdane i pravovremene transfere sredstava i odgovarajući obim zamjene deviznih sredstava. Danas se ovaj sistem najčešće koristi za protok sredstava od trgovine narkoticima. Sistem funkcioniše tako što trgovac narkoticima koji posjeduje sredstva od nelegalne prodaje narkotika angažuje brokera koji je vlasnik određenog pravnog lica. Broker stupa u kontakt sa partnerom, najčešće u Kolumbiji da stavi na raspolaganje određena sredstva u pezosima naznačenom klijentu. Tokovi novca se uravnotežuju kada broker prodaje dolare Kolumbijskim trgovcima koji namjeravaju da uvezu robu u Kolumbiju izbjegavanjem plaćanja carina i akciza. Ovi uvoznici plaćaju pezosima u Kolumbiji licu koje broker naznači, a broker plaća dobavljačima kolumbijskog partnera. Broker se koristi različitim šemama da bi izvršio plaćanje robe kolumbijskih trgovaca, na primjer može preko struktuiranih transakcija deponovati sredstva u finansijski sistem SAD-a ili prebaciti sredstva u neki od ofšor finansijskih centara.

[116] Fei cien je alternativna mreža doznaka poznata kao kineski ili istočnoazijski sistem, nastale su na dalekom istoku, proširile su se po svijetu poput hawake sistema ,slijedeći tokove emigracije. Danas se ovaj sistem koristi prije svega za legitimne svrhe privrednih subjekata i emigranata, ali i organizovanih kriminalnih grupa. Sistem funkcioniše tako što klijent dolazi do pružaoca usluga koji se bavi nekim legalnim poslovanjem,to lice vodi poslove u zemlji gdje se želi poslati novac. Specijalni davalac ove vrste usluga kontaktira svoju poslovnu ispostavu u toj zemlji i daje nalog za isplatu sredstava umanjenu za proviziju. Ove agencije ne vode obimnu evidenciju o transakcijama, ne zahtijevaju identifikaciju klijenta i ne podnose nadležnim organima izvještaj o sumnjivim transakcijama. Međusobna potraživanja između davalaca ovih usluga sravnjavaju se na sličan način kao i kod hawala sistema.

3.3.1. Prva faza – plasman/polaganje (placement).

Riječ je o uslovno prvom dijelu procesa, kad se nezakonito stečena sredstva, a to je najčešće gotov novac stečen kriminalnim aktivnostima, mijenjaju u lakše prenosiv i manje sumnjiv oblik i ubacuju u finansijski sistem ili se koriste kao sredstvo plaćanja pri nabavi različitih vrijednosti. Zapravo, bitno je da se kriminalnim putem stečena sredstva ubacuju u zakonite poslovne tokove. To je istovremeno krucijalna i najvažnija faza za detekciju prljavog novca, budući da je u ovoj fazi najlakše otkriti prirodu i porijeklo sredstava.U kriminalnim poslovima uobičajeno se i u pravilu koristi gotovina, dakako upravo zato da bi se izbjeglo identificiranje subjekata koji sudjeluju u takvom poslu.Dakle, takav novac nemože biti upotrijebljen a da se ne otkriju počinitelji nedopuštene aktivnosti kojima su novčana sredstva nastala, pri čemu gotovina u visokim iznosima izaziva pažnju i sumnju, pa se nastoji što prije iz tog oblika pretvoriti u drugi, prikladniji za daljnju uporabu. Iz rakursa počinitelja to je najteža i najrizičnija faza, budući da su prema propisima većine zemalja banke i druge finansijske institucije dužne prijaviti svaku veću transakciju.

Napomena edukatoru:

Kao ilustraciju tvrdnje da je gotovina u visokim iznosima količinski pozamašna I da ju je teško konvertovati u prenosiv I manje uočljiv oblik, koristiti podatak Ministarstva pravosuđa SAD da je jedan milion US dolara u apoenima od 5 US dolara teži 440 funti ili 199,58 kilograma (jedna funta je teška 0,4536 kilograma),u apoenima od 10 US dolara teži 220 funti ili 99,79 kilograma,u apoenima od 20 US dolara teži 110 funti ili 49,89 kilograma I u apoenima od 100 Us dolara teži 22 funte ili 9,98 kilograma.

Metode koje se koriste za plasman /polaganje gotovine u finansijski sistem su brojne, pored jednostavnog polaganja gotovine na račune u zakonu prilagođenim iznosima u obzir dolaze, plasman u trgovine nakitom i drugim dragocjenostima, kasina, konjske trke, aukcije kao I pretvaranje gotovine u čekove, putničke čekove i sl. Metod i njegova sofisticiranost su uglavnom prilagođen profilu zločinačke organizacije i važećoj legislativi protiv pranja novca koja se primjenjuje na teritoriju koji pokriva zločinačka organizacija.

3.3.2. Druga faza – uslojavanja/pokrivanje (layering).

U ovom dijelu procesa nastoji se često vrlo brojnim transakcijama prikriti pravo porijeklo sredstava, pa i prvog imatelja novca, sa svrhom da se zametne trag izvoru i dobije prividan dojam anonimnosti. Kad se ta faza promatra odvojeno od prve, uočljivo je daje riječ o nizu često pojedinačno legitimnih transakcija, koje, međutim, imaju ilegalan cilj: odvojiti sredstva od nezakonitog izvora. Najčešće korištene tehnike u toj su fazi: krijumčarenje valute, mijenjanje valute, doznake sredstava, korištenje *shell* poduzeća, korištenje osiguravajućih društava, korištenje *box office* i rezidentne pošte, korištenje uvozno-izvoznih poduzeća, manipulacije računima, manipulacije garancijama, obveznicama i vrijednosnim papirima, korištenje igraonica, poslovanje preko *off shore* zona, off shore i korespodentne banke te određene gotovinske kupovine. Ta se faza često sastoji od nekoliko transfera između banaka, između različitih računa otvorenih na različita imena brojnih osoba u različitim zemljama, kupovine vrijednih predmeta I sl. Možda je ključ uspješne operacije raslojavanja ako transakcije prelaze nekoliko nacionalnih jurisdikcija elektronskim putem i kroz više banaka i različitih korporativnih struktura.Prije su ove operacije radili pripadnici zločinačkih organizacija, međutim kako su tehnike sprečavanja pranja novca i provođenja zakona postajale sofisticiranije i efikasnije ,kriminalne organizacije su za ovaj sve zahtijevniji posao

počinjali angažirati eksperte iz raznih profesija: računovođe, advokate, bankare, brokere i investicijske savjetnike, finansijske menadžere. Nevjerovatne zarade su bile i ostale mamac za angažman eksperata .

3.3.3. Treća faza- integracije/prožimanja (integration).

U toj fazi akteri integriraju svoja sredstva u ekonomiju i financijski sistem i miješaju ih sa legitimnim sredstvima. Time se otežava detekcija pravog izvora novca, što i jest cilj cjelokupne akcije otkrivanja. Ovdje akteri donose odluke o reinvestiranju takvog "prljavog" novca u reproduktivni ciklus kriminalne djelatnosti ili pak u zakonito investiranje odnosno poslovanje koje se odvija sukladno važećim zakonima. Dakako, dio sredstava troši se na raznovrsnu (osobnu) potrošnju počinitelja kojom se oni nastoje statusno legitimirati društvu,ali zbog tih vanjskih manifestacija postaju meta tajnih i javnih aktivnosti agencija za provođenje zakona I tužilaštva.

Napomena edukatoru.

U nastavku se, radi stjecanja predstave o pojavnom obliku i složenosti takve operacije, izložiti jedan od najpoznatijih slučajeva pranja novca iz kasnih 1980-ih i ranih 1990-ih godina.
Harvardski obrazovan ekonomist Franklin Jurado osmislio i izveo je operaciju pranja novca za kolumbijskog narkobosa Josea Santacruza-Londona. Bila je to vrlo složena shema. U najjednostavnijem obliku izvedena je na sljedeći način:

Polaganje/Plasman:

Jurado je položio gotovinu od prodaje droge u SAD na račune otvorene u panamskim bankama (evidentno, koristeći se beziznimnom primjenom bankarske tajne u toj državi).

Uslojavanje/Prikrivanje:

Potom je prebacio novac iz Paname na više od 100 bankovnih računa u 68 banaka u devet država Europe, uvijek u doznakama ispod 10.000,00 $ da izbjegne sumnju. Bankovni računi su otvoreni na izmišljena imena i imena ljubavnica Santacruza-Londona i imena članova obitelji. Jurado je zatim osnovao lažne firme u Europi kako bi dokumentirao novac kao legalni prihod.

Integracija/Prožimanje:

Plan je bio poslati novac u Kolumbiju, gdje bi ga Santacrz-Londono upotrijebio za financiranje svojih mnogobrojnih zakonitih poslova. Ali, Jurado je otkriven I uhvaćen.
U cjelini Jurado je usmjerio 36 milijuna $ narkonovca kroz zakonite financijske ustanove. Juradova shema otkrivena je kad je banka u Monaku propala, a naknadna revizija otkrila mnoge račune koji su omogućili praćenje i povezivanje s Juradom. U isto vrijeme, Juradov susjed u Luxembourgu se žalio zbog buke, jer je Jurado imao stroj za brojenje novca koji je radio čitave noći. Lokalne vlasti započele su istragu, pa ga je sud u Luxembourgu odmah

proglasio krivim zbog pranja novca. Kad je kazna u Luxembourgu odslužena, sud u SAD također ga je proglasio krivim te je osuđen na sedam i pol godina zatvoru[117].

3.4. Slabe tačke u procesu pranja novca

Pranje novca kao proces ima svoje tzv. slabe točke, odnosno faze u kojima ga je lakše otkriti, a to su:

a. ulazak gotovine u financijski sistem (ujedno za perače novca najranjiviji za otkrivanje, budući da podrazumijeva velike svote gotovine koje je iznimno teško zakonito položiti na bankovni račun)
b. prebacivanje (doznake) u financijski sistem i iz njega (većina država propisala je obvezno dojavljivanje vlastima sumnjivih transakcija, što zasigurno predstavlja moćno oružje u borbi protiv pranja novca)
c. prekogranično kretanje gotovine (perač novca izlaže se riziku da bude otkriven prilikom policijske i carinske kontrole na prijelazu državne granice).

Iz iznesenog se primjera vidi da se, kad su vlasti sposobne prekinuti shemu pranja, to višestruko se isplati, vodi brojnim uhićenjima, oduzimanju prljavog novca i imovine, a ponekad i razbijanju kriminalne operacije. Međutim, većina shema pranja novca ostane neprimijećena, a velike operacije imaju ozbiljne posljedice na društveno i ekonomsko stanje.

3.5. *Cyber* kriminal i pranje novca

Kao što smo već naveli *cyber crime* podrazumijeva kriminal "koji se odnosi na bilo koji oblik kriminala koji se može izvršiti sa kompjuterskim sistemom i mrežom, u kompjuterskom sistemu i mreži ili protiv kompjuterskih sistema i mreža". Da bi razumjeli *cyber crime* u užem i širem smislu i njegove ekonomske posljedice kontekstu pranja novca potrebno je prvo razumjeti *cyber* bankarstvo, *cyber* plaćanje, *cyber* trgovinu.

3.6. Elektronsko bankarstvo

Stalne tehnološke inovacije i međusobno tržišno natjecanje postojećih bankovnih organizacija, kao i nove organizacije koje su stupile na tržište učinile su dostupnim širi asortiman bankarskih proizvoda i usluga. Inovacije su posebno dostupne stanovništvu, preduzećima odnosno privrednim društvima preko elektronskih distribucijskih kanala.

Razvoj novih tehnologija što uključuje elektronsko poslovanje[118] i elektronsko bankarstvo[119] otvara nove mogućnosti prevara i pranja novca. Jednostavnim elektronskim transferom novca iz jedne u drugu banku elektronski prenos novca postaje jedna od najčešćih načina

---

[117] Sanja Katušić-Jergović, sutkinja Županijskog suda u Velikoj Gorici, Pranje novca (Pojam, karakteristike, pravna regulativa i praktični problemi) UDK 343.341, 343.359, Stručni članak, 2007.godine, strana 625-626.(www.pravo.unizg.hr, 08.02.2012.,23,43)

[118] Pod elektronskim poslovanjem ,u smislu ovog modela, se podrazumijevaju sve aktivnosti koje poduzimaju pravne ili fizičke osobe radi razmjene dobara ili usluga, koristeći pritom računala i suvremene informacijske i komunikacijske tehnologije.

[119] Elektronsko bankarstvo (engl. electronic banking, njem. elektronische Abwicklung von Bankgeschäften) predstavlja upotrebu bankarskih usluga i izvođenje bankarskih transakcija koje obavlja sama stranka, vlasnik računa i komitent banke, posredstvom osobnih računala ili terminala s lokacija s kojih je moguć pristup telekomunikacijskoj mreži za prijenos podataka. Preuzeto iz Leko, V., (1998), Rječnik bankarstva, Masmedia, Zagreb.

prebacivanja velikih iznosa novca po cijelom svijetu, što ujedno implicira korisnu metodu druge faze pranja novca-oplemenjivanje.

Na taj se način „prljavi novac“ putem bankarskog ili financijskog sistema elektronski premješta globalnim bankarskim sistemom, u svrhu prikrivanja njegovog pravog izvora. Richards navodi okvirnu procjenu koja ukazuje da se 80% ukupnih poslovnih transakcija odvija elektronskim transferima s računa stranke na račune drugih korisnika, iz čega proizlazi da je elektronsko poslovanje krvotok globalne trgovine.[120] Prepoznajući potrebu za saradnjom između država i privatnog gospodarstva u suzbijanju *cyber* kriminala te potrebu za zaštitom legitimnih interesa prilikom korištenja i razvitka informatičkih tehnologija, a s time u vezi i vođenja zajedničke kaznene politike usmjerene zaštiti društva od *cyber* kriminala,, Bosna i Hercegovina je 2006. godine ratificirala Konvenciju o kibernetičkom kriminalu.[121]

3.6.1. Definicija i obuhvat elektronskog bankarstva

Elektronsko bankarstvo predstavlja poslovanje kreditnih institucija pomoću telekomunikacijske mreže, a uključuje sve proizvode i usluge dostupne strankama tim putem te poslove koje kreditna institucija obavlja u svoje ime i za svoj račun koristeći se navedenim distribucijskim kanalom. Karakterizira ga nepostojanje ličnog kontakta (fizičke prisutnosti stranke pri obavljanju transakcija) i teritorijalnih ograničenja (poslovanje s inostranstvom) te brzina kojom se odvijaju ove vrste transakcija. Elektronsko bankarstvo uklanja još jednog posrednika pri obavljanju poslova pranja novca zbog čega više nije potrebno tražiti korumpiranog bankara i plaćati mu nužnu proviziju. Stalne tehnološke inovacije i sve veća konkurencija na tržištu omogućili su ubrzan razvoj postojećih i novih bankarskih proizvoda i usluga što otvara nove poslovne mogućnosti za banke i njihove klijente.[122] U tom se smislu može promatrati i značaj elektronskog bankarstva kao neposredna ponuda novih i tradicionalnih proizvoda i usluga putem elektronskih interaktivnih komunikacijskih kanala.

3.6.2. Podjela elektronskog bankarstva

Elektronsko bankarstvo možemo podijeliti u tri grupe: (1) informativno: pružanje informacija klijentu, (2) komunikacijsko: interakcija banke i klijenta, (3) transakcijsko: provođenje konkretnih transakcija.

3.6.3. Distributivna mreža elektronskog bankarstva

Distributivna mreža elektronskog bankarstva podrazumijeva razvoj i primjenu: a) Pos terminala, b) Kućnog bankarstva, c) SMS bankarstva, d) Internet bankarstva d) Bankomate.

---

[120] Vidjeti više u Richards, J., (1998), Transnational Criminal Organizations, Cybercrime, and Money Laundering: A Handbook for Law Enforcement Officers, Auditors and Financial Investigators, CRC Press LLC, Florida.

121 Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu („Službeni glasnik BiH“,broj 6/06-Međunarodni ugovori“).

[122] Uzimajući u obzir da se od prodaje 1 kg čistog heroina generira i do 230 kg novčanica ili podatak da 20 dolara teži 1 gram, odnosno transakcija od 1.000.000 dolara (50.000 novčanica) otprilike 50 kg, jasno je da će dilerima droge elektronsko poslovanje predstavljati manji rizik prebacivanja novaca iz jedne u drugu zemlju nego fizički prijenos novca preko granice. Vidjeti više Grabbe, J., O., (1995), The End of Ordinary Money, Part II: Money Laundering, Electronic Cash, and Cryptological Anonymity, http://www.aci.net/kalliste/homepage.html.

3.6.3.1. Pos terminali

Putem Pos sistema odvija se bezgotovinski način plaćanja. U posljednje vrijeme se sve više koristi Eft Pos sistem koji omogućava elektronski transfer novčanih sredstava na mjestu prodaje. Da bi se to realiziralo, neophodno je direktno povezati elektronske registar kase (terminale) sa informatičkom mrežom u bankama. Sistem se primjenjuje provlačenjem platne kartice kroz terminal koji očitava magnetnu traku platne kartice, tako da se unošenjem iznosa finansijske transakcije provjerava na licu mjesta stanje na tekućem računu vlasnika kartice. Na osnovu provjerenog stanja šalje se Pos terminalu povratna informacija, na osnovu koje se štampa račun i to po pravilu u duplikatu. Jedan primjerak računa ostaje davaocu usluge, dok drugi primjerak ostaje korisniku platne kartice.

3.6.3.2. Telefonsko (kućno) bankarstvo

Telefonsko bankarstvo predstavlja direktno korištenje bankarskih usluga od kuće putem telefonske mreže. Primjenom ovog sistema klijent se lišava potrebe odlaska na šalter banke, kao i potrebe pismenog komuniciranja tehnologija kućnog bankarstva zasniva se na "pozivnim centrima" kojima se pristupa preko određenih šifri kucanih preko tastature. Pozivom na određeni telefonski broj pristupa se telefonskom servisu, te se nakon identifikacije, unošenjem PIN broja (lične kreirane lozinke) otvara meni koji preko govornog automata usmjerava korisnika telefonskog bankarstva do željene sluge. Da bi se mogla primijeniti govorna tehnologija neophodno je da se telefonski aparat poveže sa hardverskim dodatkom (preko telefonske mreže) kako bi e numerički podaci mogli pretvoriti u govorni signal računar govori).

3.6.3.3. SMS bankarstvo

SMS bankarstvo počiva na korištenju mobilnog telefona funkciji izvršavanja bankarskih transakcija. Uslov da bi e koristilo SMS bankarstvo jeste da korisnik bankarskih sluga popuni posebnu pristupnicu, u kojoj navodi podatke o tekućem računu i broju mobilnog telefona sa kojeg će izvršavati transakcije. Da bi klijent mogao da koristi bankarske usluge neophodno je da na broj servisnog centra pošalje SMS poruku koja će sadržati šifru vezanu za upit. Korisnik SMS bankarstva može u svakom momentu, u vremenu od 24 sata da: a) provjeri stanje na tekućem računu, b) da ima uvida u podatke o posljednjim bankarskim transakcijama, c) obavlja platne transakcije. Sistem sigurnosti SMS bankarstva je zasnovan na povezanosti broja mobilnog telefona i transakcionog računa, kao i navedenih brojeva tekućih računa u korist kojih se može izvršiti plaćanje

3.6.3.4. Internet bankarstvo

Preokret u razvoju Interneta nastaje u posljednjoj deceniji XX stoljeća, kada je primjena interneta izašla iz akademskog kruga i kada je izvršena komercijalizacija mreže interneta povezivanjem miliona računara u svijetu. internet bankarstvo predstavlja najrasprostranjeniji oblik elektronskog bankarstva. Korištenjem internet bankarstva pruža se mogućnost klijentima banke da preko personalnih računara, komuniciraju sa svojim tekućim računom.

Banke su veoma brzo shvatile da nije dovoljno da imaju samo Internet prezentacije koje dobro vizuelno izgledaju. Danas se postavljaju dodatni zahtjevi da prezentacije moraju da pruže i nešto više, da budu interaktivne, multimedijalne i da omogućavaju kompletno poslovanje direktno na Internetu. Zbog toga su banke u svoje Internet poslovanje uvele niz

inovacija (virtualne poslovnice, specijalne finansijsko-softverske programe koji brinu o budžetu klijenata, ulaganjima...). Ipak i pored spomenutih inovacija ponuda bankarskih proizvoda i usluga je gotovo uniformna. Bankarsko poslovanje na Internetu je brzo, efikasno i ekonomično. Otvaranje računa u Internet bankama je potpuno besplatno. Provizije za plaćanje računa elektronskim putem su minimalne ili u većini Internet banaka potpuno besplatne. Ostale provizije za Internet bankarske proizvode i usluge su identične ili manje od provizija u takozvanom tradicionalnom (filijalnom) bankarstvu. Plaćanje računa preko Interneta elektronskim novcem ili pametnim karticama (Smart Cards) je nova aktivnost koju Internet banke omogućavaju svojim klijentima. Internet bankarstvo ima niz prednosti u odnosu na takozvano tradicionalno (filijalno) poslovanje banaka. Prijelaz s direktnog šalterskog načina poslovanja na elektronski omogućio je anonimne transakcije kojima se sve teže ulazi u trag. Internet pruža nove mogućnosti pranja novca preko elektronskog poslovanja. Internet nosi veliki stepen rizika jer se elektronskim putem transakcije obavljaju lakše i brže, pri čemu je teško identificirati klijenta

.

Glavni ograničavajući faktori, koji uslovljavaju pristanak potrošača na ovu vrstu tehnologije, su sigurnost i privatnost. Sa tehničke tačke gledišta, ovaj problem su neke banke već riješile, ali ostaje činjenica da je ponašanje potrošača vođeno prije potrošačkom percepcijom nego tehničkim činjenicama. Neprihvaćanje da se bankarske transakcije obavljaju preko Interneta postoji prije svega iz straha da ključne finansijske informacije budu otkrivene. Jasno su vidljive razlike između Internet bankarstva i on-line bankarstva. Osnovna razlika je u ugradnji specijalnih softverskih programa, koji ograničavaju korisnika na obavljanje usluga isključivo sa računarom u koji je ugrađen odgovarajući softver.

3.6.3.4.1. Prednosti internet bankarstva

Prednosti internet bankarstva se uglavnom ogledaju u slijedećem: (1) niži troškovi realizacije naloga za plaćanje (2) viši prihodi, odnosno manje učešće rashoda u ostvarenim prihodima Korištenjem internet bankarstva (3) iskorištenje radnog vremena (internet bankarstvo je neprekidno na usluzi svojim klijentima, 24 časa dnevno, 365 dana u godini)(4) realizacija transakcija putem personalnog računara (nema administrativne formalnosti i ne odlazi se u banku)(5) pristup elektronskoj banci sa bilo kog računara u setu (ukoliko je računar sa modemom priključen na internet) (6) održavanje zaštite internet sistema preko banke uz obavljanje on line bankarskih transakcija.

3.6.3.4.2. Nedostaci internet bankarstva

Nedostaci internet bankarstva se odnose na neadekvatnu zakonsku regulativu u ovoj oblasti i nepostojanju savršenog sistema zaštite i sigurnosti u elektronskom poslovanju. Najveća prepreka masovne primjene internet bankarstva je neizgrađeno povjerenje između korisnika elektronske usluge i računara.

U internet bankarstvu se primjenjuje sistem kripto zaštite pod nazivom SET (Secure Electronic Transaction) projektovan od strane Visa, Master card, IBM kompanija. SET sistem predstavlja garanta za kupca, prodavca, banku i klijenta, da su svi učesnici u elektronskoj transakciji autentični. Što se tiče domicilnog bankarstva, kod nas je još uvijek široko rasprostranjena PC kompjuterska tehnologija. Preduslovi brže primjene internet bankarstva kod nas se odnose na: a) praćenje savremene elektronske tehnologije, b) razvoj novih bankarskih proizvoda,c) prilagođavanje organizacije i poslovanja banaka novim medijima i sl.

3.6.3.5. Bankomati

Bankomat predstavlja pojednostavljeni terminal koji služi za unos podataka sa dva ulazna i četiri izlazna uređaja. Bankomat je povezan sa centralnim računom preko modema ili iznajmljene linije. Bankomati se mogu koristiti za: a) podizanje gotovine, b) polaganje depozita, c) transfer sredstava sa računa na račun, d) uplate na račune, d) naručivanje i primanje izvještaja, f) korištenje kredita u granicama određenog limita.

Primjenom bankomata, banke mogu omogućiti klijentima da koriste usluge van radnog vremena banke, van prostorija i lokacije banke. Na ovaj način se bankama otvara mogućnost da kontinuirano pružaju svoje usluge bez postojanja mreže filijala i ekspozitura.

3.6.3.6. Zabrinutosti u vezi sa sprečavanjem pranja novca koje donosi cyber kriminal

Bez obzira na oblik kriminala, uzimajući u obzir i one u nastajanju kao što su *cyberporn*, *cybertheft* i *cyberstalking*, karakteristike koje imaju kompjuterski sistemi i kompjuterske mreže (brzina, sigurnost, efikasnost, racionalnost, anonimnost itd.) čine ih atraktivnim i za korištenje u nelegitimne svrhe kao što je pranje novca. Zbog toga su brojni međunarodni autoriteti već relativno dugo izražavaju zabrinutos i potrebu rješavanja najmanje tri pitanja. Prvo,djelotvornost postojećih zahtijeva za obaveznim izvještavanjem o sumnjivim transakcijama koje po svojoj prirodi obuvataju aktivnosti (s posebno velikom vjerovatnoćom) povezane sa pranjem novca ili finansiranjem terorizma, posebno složene i neobične velike elektronske transakcije i sve neobične uzorke takvih transakcije koje nemaju očitu privrednu ili vidljivu zakonitu svrhu. Drugo, sadašnji analitički i istražni alati i tehnike počivaju na pretpostavci da kriminalne organizacije moraju bar neki dio transakcije provesti preko nekog od posrednika(obveznika sprečavanja pranja novca) i oslanjaju se pri tome na efikasnost principa upoznaj svog klijenta koji je sastavni dio programa prevencije operativnih i reputacijskih rizika (identifikaciju klijenta, prihvatljivost klijenta, praćenje poslovanja klijenta i valoriziranje intenziteta rizičnosti) svake finansijske investicije. Međutim *cyber* bankarstvo iz kuće/stana i *cyber* sistem plaćanja gotovo da nemaju *face to face* transakcije što analitičke i istražne alate i princip upoznaj svog klijenta čini manje primjenjivim i efikasnim. Treće, većina *cyber* bankarstva i *cyber* sistema plaćanja djeluju u svijetu i sa više valuta tako da svakog trenutka prelaze tradicionalne fizičke nacionalne granice i njihove jurisdikcije što značajno umanjuje mogućnosti za efikasno i efektivno suprotstavljanje *cyber* kriminalu i pranju novca na nacionalnom nivou.

Jedan od brojnih međunarodnih napora koji se u posljednje vrijeme čine da bi se *cyber* kriminal stavio pod kontrolu I spriječiili novi incidenti je uspostava sigurne globalna mreža CyberSchengen[123] čiji je vlasnik Taransvar[124], nevladina organizacija iz Norveške. Globalna mreža CyberShengen se bavi istraživanjem svih incidenata inficiranih računala unutar CyberShengena tako da će sabračaj kroz sporedni ulaz biti detaljno ispitani.

3.6.4. Elektronsko bankarstvo u BiH

Brz razvitak informacijske i komunikacijske tehnologije u posljednjem je desetljeću dvadesetog stoljeća imao izuzetno velik utjecaj na ekonomiju, gospodarstvo i bankarski

[123] Vidi www.cybnershengen.com ,22.01.2012.,13,52.
[124] Vidi www.cybnershengen.com ,22.01.2012.,13,54

sustav. Globalizacija, kao ključni element početka ovog stoljeća, najvjernije pokazuje novi sistem pravila ponašanja koja donosi elektronska komunikacija, mrežno povezivanje i pristup podacima putem Interneta. „Bitni faktor za razvoj novih usluga je velika brzina protoka informacija kroz različite platforme“. BiH sa kašnjenjem i uglavnom zaslugama banki kćerki čije su majke iz država članica Evropske unije, slijedi primjere drugih zemalja i pruža priliku elektronskom poslovanju, a samim time i elektronskom bankarstvu.

Prema podacima koje je bh. javnosti saopštila CBBIH, 28 banaka u BiH pruža usluge elektronskog bankarstva. Također, 33.000 fizičkih osoba je u 2009.godini koristilo usluge elektronskog bankarstva, a u 2010. godini je to učinilo 48.545 osoba. U isto vrijeme broj pravnih osoba koje koriste elektronsko bankarstvo je gotovo identičan,jer je te usluge u 2009.godini koristilo 19.000,a u 20190.godini 19.257 pravnih lica. U saopštenju CB BIH pored navedenog navodi da je primjetno nastojanje banaka u BiH da povećaju broj ATM i POS uređaja što je rezultiralo da je u 2010. godini instalirano 1.098 ATM uređaja i 17.834 POS terminala[125].

Informacijska i komunikacijska infrastruktura ima posebni značaj za napredak poslovanja jer omogućava pristup udaljenim tržištima, smanjenje troškova poslovanja, povećanje brzine poslovnih transakcija, kontakt s korisnicima i personalizaciju usluga. Tehnologija, informacije i znanje postali su odlučujući faktori za konkurentnost pravnih lica u svim sektorima privrede, ali i za konkurentnost cijelih nacija.

Primjena informacijske tehnologije u svim aspektima bankarskog poslovanja stvorila je određenu ovisnost o informacijskoj tehnologiji kao sastavnom djelu upravljanja bankom u cjelini. Pritom je potrebno posebnu pažnju obratiti na upravljanje rizikom[126] koji proizlazi iz korištenja informacijskog sustava kako bi poslovanje banke bilo sigurno.

Globalizacija financijskih usluga zajedno s rastućim nivoom financijske tehnologije čine aktivnosti banaka u BiH a time i njihove profile rizika sve složenijima. Razvoj bankovnih praksa upućuje na to da, osim kreditnoga, kamatnoga ,tržišnoga, reputacijskog i operativni rizik[127] također može biti vrlo značajan. Kao jedan od primjera operativnog rizika svakako je rast elektronskog poslovanja koji nosi sa sobom potencijalne rizike, unutrašnje i vanjske prevare i pitanja sigurnosti sistema, koji još nisu u potpunosti razrađeni. Operativni rizik se razlikuje od ostalih navedenih rizika u tome što se on ne preuzima direktno, u zamjenu za očekivanu dobit, već je prisutan u uobičajenom toku obavljanja aktivnosti. Zbog njegovog značaja banke trebaju utvrditi i procijeniti operativni rizik u svim značajnim proizvodima, aktivnostima, procesima i sistemima. Također, trebaju osigurati da prije uvođenja novih procesa i sistem takav rizik bude podvrgnut adekvatnim postupcima procjenjivanja.

[125] http://www.seebiz.net/finansije/bankarstvo-i-osiguranje/cbbih,23.01.2012.godine 13,49;

[126] Na osnovi obavljene procjene rizika banka će, između ostalog, odrediti adekvatne kriptografske metode čija će primjena smanjiti rizik od narušavanja temeljnih načela informacijskog sustava. Kriptografske metode predstavljaju jednu vrstu logičkih kontrola kojima se dodatno osigurava zaštita informacija i smanjuje rizik od narušavanja temeljnih načela informacijskog stava. Kriptografija se najčešće upotrebljava za enkripciju (šifriranje podataka), elektronsko potpisivanje, očuvanje integriteta podataka i utvrđivanje autentičnosti korisnika (verifikacija stranke).

[127] Baselski odbor za nadzor banaka definirao je operativni rizik kao „rizik od gubitaka koji nastaje zbog neprimjerenih ili neuspješnih unutarnjih procesa, ljudi ili sustava ili zbog vanjskih događaja“. Vidjeti više u Baselski odbor za nadzor banaka, (2011.), Dobre prakse za upravljanje operativnim rizikom i nadzor nad njim, Banka za međunarodne namire.

Internet je u BiH, uslovno rečeno, svima dostupan jer je globalan po svojoj prirodi. Prema podacima Regulatorne agencije za komunikacije u 2010.godini u BiH je evidentirano 522.364 internet pretplatnika i po procjeni dva miliona internet korisnika,te je stopa korištenja interneta u BiH iznosila 52%. Također u izvještaju se navodi da je zaključno sa 31.12.2010.godine u BiH djelovalo 75 pružalaca internet usluga.[128] On je otvorena mreža kojoj nepoznate strane imaju pristup omogućen s bilo kojeg mjesta u svijetu, „rutiranjem" poruka preko nepoznatih lokacija i pomoću bežičnih uređaja. Iz istih se razloga uvelike povećava važnost sigurnosnih kontrola, tehnika provjere identiteta klijenata, zaštite podataka, postupaka ostavljanja pisanog revizijskog traga i standarda zaštite privatnosti stranke. S time u svezi treba se poštivati sigurnost i zaštita podataka i postupaka, ali i osigurati provođenje identifikacije stranaka s kojima se posluje preko Interneta, verifikacije prikupljenih podataka i poduzimanje odgovarajućih mjera zaštite vjerodostojnosti podataka o transakcijama elektronskog bankarstva, dokumentacije i ostalih informacija.[129]

3.6.5. Elektronsko bankarstvo i pranje novca

Elektronskim se transferima teško ulazi u trag upravo zbog minimuma identifikacijskih informacija o stranci, čime se omogućava međunarodno kretanje ogromnih iznosa novca u samo jednoj sekundi. „Samo se jedan takav transfer kreće u rasponu i do milion dolara, dok procjene govore da se na dnevnoj razini razmjenjuju čak i trilioni dolara (u novčanicama i obveznicama)".[130]

Međunarodni napori sprječavanja pranja novca i financiranja terorizma putem elektroniskih transfera novca, a samim time i elektronskog bankarstva, istaknuti su u točki 14. uvoda Treće direktive,[131] članu 26. Zakona o sprečavanju pranja novca i finansiranja terorizma[132], kao i u VII Specijalnoj preporuci FATF koja ističe značaj i opasnosti napredne tehnologije.

U tom svijetlu, VII Specijalna preporuka FATF ima za cilj poboljšati transparentnost svih vrsta transfera novca elektronskim putem, unutar zemlje i međunarodno, olakšavajući pri tome tijelima provođenja zakona slijed elektronskog prijenosa (nezakonitog) novca. Propisuje obvezu poduzimanja mjera financijskim institucijama, uključujući i one koje se bave međunarodnim novčanim doznakama, za pribavljanjem točne informacije o transferu sredstava, kao i provođenje pojačane kontrole i nadzora transfera koji ne sadrže propisane podatke o pošiljatelju.

Za svaki elektronski prijenos novca u iznosu od 1.000 Eura/dolara ili više finansijska je institucija dužna tražiti (i čuvati) podatke o pošiljatelju. Prikupljene će podatke[133] naknadno

[128] http://www.info-market.ba/bs/scena/12670,06.02.2012.,10,52.

[129] O načelima kontrole sigurnosti podataka vidjeti više u Baselski odbor za nadzor banaka, (2003), Načela upravljanja rizikom u elektronskom bankarstvu, Banka za međunarodne namire.

[130] Preuzeto iz Zagaris, B., MacDonald, S., B., (1992), "Money Laundering, Financial Fraud and Technology: the Perils of an Instantaneous Economy" preuzeto iz Savona, E., (2004), Responding to Money Laundering: International Perspectives, Harwood Academic Publishers, London, str. 153-154.

[131] Točka 14. uvoda Treće direktive njezin obuhvat proširuje na sve radnje radnje koje institucije i osobe obuhvaćene direktivom obavljaju na Internetu.

[132] Članom 26.Zakona o sprečavanju pranja novca je propisana obaveza kreditnim i finansijskim institucijama, uključujući društva koja obavljaju određene usluge platnog prometa ili prijenosa novca prikupljanja tačnih i potpunih podataka o uplatiocu i uključiti ih u obrazac ili poruku koja prati elektronski prijenos novčanih srestava,poslanih ili primljenih u bilo kojoj valuti.

[133] Obavezno prikupljanje, čuvanje i verifikacija podataka, uprema VII Specijalnoj Preporuci FATF, odnose se na: ime i prezime, podatke o računu (ili jedinstveni poslovni broj ako podaci o računu ne postoje) i adresu (ili ukoliko je dozvoljen jedinstveni matični broj osobe, broj osobne iskaznice ili datum i mjesto rođenja).

verificirati u skladu s 5. Preporukom FATF. Za elektronske transfere preko granice u istom iznosu potrebno je prikupiti sve podatke o pošiljatelju koji će pratiti daljnji transfer novca, dok je za transfere unutar zemlje dovoljno prikupiti: a) podatke tražene za međunarodne transfere ili b) podatke koji uključuju pošiljateljev broj računa ili drugi jedinstveni identifikator.

Podaci moraju pratiti transakciju. Sve transakcije uz koje nisu priloženi potpuni podaci o pošiljatelju podvrgnut će se procedurama za procjenu rizika. Time predstavljaju jedan od razloga sumnje na pranje novca ili financiranje terorizma. Takve će se transakcije odmah dostaviti nadležnim tijelima, odnosno FIU, a suradnja s financijskom institucijom koja je poslala nepotpune podatke ograničiti će se ili prekinuti, ovisno o sadržaju zaprimljenih podataka[134].

U cilju učinkovite implementacije VII Specijalne preporuke FATF, 1. siječnja 2007. stupila je na snagu Uredba 1781/2006 kojom se propisuje obveza da informacije o nalogodavcu prate transfer novca, u cilju sprječavanja, istraživanja i otkrivanja pranja novca te financiranja terorizma (u nastavku teksta: Uredba 1781/2006).

Kako tok „prljavog novca“ elektronskim transferima može naštetiti stabilnosti i ugledu financijskog sektora i ugroziti međunarodno tržište, Uredba 1781/2006 propisuje obvezu institucijama koje provode transakciju da svaki elektronski prijenos novca sadrži potpune informacije o osobi koja je dala nalog da se transakcija izvrši. Potpuni slijed prijenosa novca posebno je važan i koristan instrument prevencije, analize i otkrivanja pranja novca i finansiranja terorizma[135] zbog čega Uredba 1781/2006 detaljno propisuje postupanje institucija koje provode transakciju, posrednika pri njihovom provođenju i osoba koje ih primaju.[136]

Kao i u odredbama Treće direktive navodi se neupitnost procjene rizika, postupanje u situacijama kada nedostaju svi traženi podaci o nalogodavcu te obveza obavješćivanja FIU o transakcijama koje, zbog nemogućnosti pribavljanja traženih podataka, imaju karakter sumnjivosti.

Rok čuvanja prikupljenih podataka sa svim informacijama o nalogodavcu ostaje 5 godina radi učinkovite suradnje s tijelima koja sudjeluju u suzbijanju pranja novca i financiranja terorizma. Pod pretpostavkom zaštite osnovnih prava, predmetne će se informacije koristiti samo u svrhu sprječavanja, analize i otkrivanja pranja novca i financiranja terorizma. Za svako odstupanje od postavljenih pravila propisat će se predviđene kazne te provođenje učinkovitog nadzora.

[134] Vidjeti više u Financial Action Task Force on Money Laundering (2007), Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special recommendations.

[135] Značaj nadzora elektronskih transfera posebno je uočen nakon terorističkih napada na SAD 11. septembra 2001. i postavljanja bombi u Madridu 11. marta 2004., zbog čega je Vijeće Europe odobrilo plan koji se odnosi na unapređenje sudske i policijske suradnje, unapređenje međunarodnih pravnih instrumenata suzbijanja terorizma, sprječavanje financiranja terorizma, povećanje sigurnosti vazdušnog prometa i veću konzistenciju svih relevantnih politika postupanja. Vidjeti više u uvodu Uredbe 1781/2006.

[136] Obim informacija koje je institucija dužna prikupiti jednak je onom iz VII Specijalne Preporuke FATF., osim identifikacije traži se i verifikacija prikupljenih podataka o nalogodavatelju naq osnovu dokumenata, podataka ili informacija dostupnih iz pouzdanih i nezavisnih izvora.

3.7. Korespondentno bankarstvo

Korespondentno bankarstvo predstavlja još jednu potencijalno slabu kariku efikasnog sustava sprječavanja pranja novca i financiranja terorizma. Samim time što podržava bezgotovinski prijenos novca između nekoliko zemalja i preko većeg broja računa te otvara mogućnost suradnje s visoko rizičnim stranim bankama, dozvoljava i ulaz „prljavog novca“ u finansijski sistem.

Pojam „korespondentno bankarstvo“ predstavlja pružanje usluga prijenosa novca jedne (korespondentne) banke, uz proviziju, drugoj (respondentnoj) banci. Nastavno na prednosti elektronskog poslovanja, korespondentno bankarstvo omogućava provođenje transakcije bez fizičke prisutnosti stranaka. Potencijalna anonimnost i brzina provođenja većeg broja transakcija preko nekoliko zemalja tipična je za pranje novca u fazi oplemenjivanja i integracije kada „perači“ pokušavaju sakriti pravu prirodu nezakonitih sredstava prethodno ubačenih u financijski sustav[137].

Problem predstavljaju korespondentni odnosi s visoko rizičnim bankama koje imaju manjkavu pravnu regulativu, nepouzdani (ili korumpirani) management, a samim time i lošu preventivnu strategiju suzbijanja pranja novca i financiranja terorizma.
U visoko rizične strane banke mogu se ubrojiti:

- *shell* banke – koje fizički ne postoje niti u jednoj zemlji[138];
- *offshore* banke[139] – kojima je licenca ograničena na poslovanje samo s osobama izvan teritorija te zemlje ili joj je onemogućeno poslovanje s lokalnom valutom;
- banke koje se nalaze unutar države koja ne primjenjuje odgovarajuće standarde ili ne surađuje u međunarodnim nastojanjima sprječavanja pranja novca i financiranja terorizma[140].

Stav spram poslovanja sa *shell* bankama pokazuje i Treća direktiva koja u članu 13. stavu 5., propisujući pojačane mjere dubinske analize stranke, kreditnim institucijama zabranjuje uspostavljanje ili nastavak korespondentnih bankovnih odnosa s fiktivnom bankom i zahtijeva poduzimanje prikladnih mjera za sprječavanje uspostave ili nastavka provođenja korespondentnih bankovnih odnosa s bankom za koju je poznato da dopušta fiktivnim bankama otvaranje računa.

---

[137] Iz izvještaja o korespondentnom bankarstvu „Ulaz za pranje novca“ (2001) proizlazi da američke banke, putem korespondentnih računa stranih banaka, predstavljaju ulaz prljavog novca u financijski sistem pomažući pri finaliziranju trgovanja drogom i financijskim prevarama. Vidjeti više u Report on Correspondent Banking: A Gateway for Money Laundering, (2001), Minority Staff of the Permanent Subcommittee on Investigations, U. S. senate Committee on Governmental Affairs, preuzeto iz: Gup , B., E., (2006) Money Laundering, Financing Terrorism And Suspicious Activities, Nova Science Publishers, str. 92.

[138] Shell banke (fiktivne banke) se člankom 3. stavak 1. točka 10. Treće direktive definiraju kao kreditne institucije ili institucije za obavljanje istovjetnih poslova, inkorporirane u nadležnost države u kojoj nisu fizički prisutne (uključujući autentičnost i management), a nisu povezane niti sa zakonski reguliranom financijskom grupom.

[139] Off shore zone su područja, države, protektorati s vrlo liberalno postavljenom legislativom glede poslovanja i otvaranja banaka i tvrtki, s vrlo malim postotkom poreznih obveza, a vrlo jakom bankarskom tajnom.

[140] Vidjeti više u Gup , B., E., (2006) Money Laundering, Financing Terrorism And Suspicious Activities, Nova Science Publishers, i u Gustitus, L., Bean, E., Roach, R., (2001), Economic Perspectives, An Electronic Journal of the U.S. Department of State, Vol. 6, No. 2.

3.8. Elektronsko plaćanje

Elektronsko plaćanje je svaka finansijska transakcija koja koristi podatke razmijenjene elektronskim putem.[141] Elektronsko plaćanje je po svojoj funkcionalnosti ekvivalent nekog od klasičnih ne-elektronskih plaćanja. Po vrsti plaćanja modu se podijeliti na dvije grupe: (1) notacijski ili bezgotovinski (2) simbolički ili gotovinski.

3.8.1. Notacijski/bezgotovinski sistem elektronskog plaćanja

Kod notacijskog sistema elektronskog plaćanja kupac koji ima otvoren račun u banci koristeći jedan od oblika bezgotovinskog plaćanja zapravo trgovcu predaje nalog za prebacivanje sa svog računa na račun trgovca. U ovom slučaju je to elektronski nalog. To može biti e-ček, kreditna kartica, debitna kartica i sl.

3.8.1.1. E-ček

Elektronski ček je ekvivalent klasičnog papirnog čeka. Izdaje ga kupac trgovcu, a trgovac ga polaže u svoju banku, koja obavlja naplatu od banke izdavaoca e-čeka.

Proces naplate e-čeka:

1. Banka izdaje bjanko e - ček kupcu sa elektronskim potpisom banke,
2. Kupac upisuje u elektronski ček iznos i datum, potpisuje ga svojim digitalnim/elektronskim potpisom i predaje trgovcu. Trgovac izdaje robu/uslugu kupcu.
3. Trgovac upisuje na ček svoj broj računa i prosljeđuje e-ček svojoj banci, potpisujući ga svojim digitalnim potpisom,
4. banka trgovca provjerava potpise trgovca i potpise banke izdavaoca i prosljeđuje ček banci izdavaocu na naplatu,
5. banka izdavalac provjerava svoj digitalni potpise i digitalni potpise kupca na prispjelom čeku,provjerava stanje novca na računu i ako je sve u redu, prebcuje novac s računa kupca na račun trgovca.

E-ček predstavlja rizik za trgovca pošto ne može znati da li kupac ima na svom računu u banci dovoljno novca za pokriće čeka.Osim toga, kupac može falsificirati svoj digiotalni potpis. Ako želi biti siguran ,trgovac morati ima on-lene vezu s bankom izdavaocem čeka,što bitno komplicira I poskupljuje transakciju jer takvih banka može biti više.

3.8.1.2. Kreditne kartice

Plaćanje kreditnom karticom nije u pravom smislu elektronski način plaćanja,ali obzirom da se prilikom plaćanja kreditnom karticom ipak plaćanje vrši prenosom informacija koje ne moraju imati svoju potpunu materijalizaciju (broj kartice, ime i prezime nosioca i datum valjanosti kartice) i moguće je njom plaćati u sistemu koji omogućava elektronski prenos poruke. Osim svoje funkcije naloga za plaćanje,kreditna kartica ima I dodatnu funkciju odgođenog plaćanja odnosno kredita. Plaćanje kreditnom karticom zbog velike je raširenosti kartica postalo najzastupljeniji način plaćanja na Internetu.

[141] Vidi više CARNet.HRVATSKA AKADENSKA I ISTRAŽIVAČKA MREŽA, Elektronički novac NCERT-PUBDOC-2010-09-311, Nacionalni CERT+(www.cert.hr) u suradnji s LS&S(www.LSS.hr).,

Tehnika naplate kreditne kartice se odvija na slijedeći način:

1. banka u propisanoj proceduri svom klijentu izdaje kreditnu karticu,
2. imalac kartice u ulozi kupaca proizvoda i usluga šalje dobavljaču kupljenih proizvoda I/ili usluga podatke sa svoje kartice (broj kartice, ime i prezime nosioca i datum valjanosti kartice),
3. trgovac preko on-line sistema provjerava valjanost kartice kod banke izdavaoca(vrši autorizaciju kreditne kartice)
4. ako je kartica autorizirana, dobavljač kupljenih roba i/ili usluga šalje banki odnosno finansijskoj instituciji koja je autorizirala karticu ,iznos koji kupac želi platiti. Ako je iznos koji kupac želi platiti ispod limita koji ima kreditna kartica, dobavljač dobija odobrenje za naplatu,
5. nakon što je dobio odobrenje, dobavljač kod sebe evidentira broj trnsakcije koju je dobio skupa sa odobrenjem,
6. autorizacijski centar obavlja kliring transakcije s bankom izdavaocem kreditne kartice,
7. Kartičar periodično plaća dobavljaču iznose svih uspješno autoriziranih transakcija,
8. Dobavljač roba i/ili usluga periodično dobije račun od kartičara za sve troškove koje je napravio u toku mjeseca.

Plaćanje na otvorenim mrežama kreditnom karticom ima više nedostataka od kojih su najznačajniji:

1. Sigurnost transakcije,
2. Cijena transakcije,
3. da bi se transakcija obavila neophodno je da dobavljač/trgovac ima on-line vezu s bankom kao bi provjerio valjanost kreditne kartice,
4. Transakcije nije moguća između dvije fizičke osobe,
5. Izdavalac kartice obzirom da raspolaže sa svim podacima o izvršenim transakcijama (iznos, vrijeme , mjesto i učestalost) je u prilici da bez odobrenja klijenta prati njegove potrošačke navike I tako narušava njegovu privatnost.

3.8.1.3. Debitne kartice

Debitna kartica je kartica koju banka izdaje vlasniku tekućeg ili deviznog računa koji on ima kod te banke. Preko debitne kartice njen vlasnik raspolaže sa novcem koji im na računu. Debitna kartica je slična kreditnoj kartici,s razlikom da vlasnik kartice kao kupac roba i/ili usluga u trenutku kupnje mora imati novac na računu. Prodavac roba i/ili usluga preko on-line veze s bankom koja je izdavalac debitne kartice istovremeno provjerava valjanost kartice I odmah prebacuje novac sa računa kupca na svoj račun.Debitne kartice u pravilu su zaštićene četverocifernim PIN brojem, tako da u slučaju njenog gubljenja ili krađe njen nelegalni posjednik ne može njom neovlašteno raspolagati. Četverocifereni PIN broj dovoljan zaštićen kada se lično utipkava na bankomatu,ali kada se ubaci u elektronski sistem plaćanja nerijetko postaje sredstvo brojnih cyber zloupotreba, krađa i prevara te je to čini nepraktičnom ta korištenja na Internetu. Debitna kartica ne predstavlja nikakav rizik za trgovca /dobavljača roba i/ili usluga.

Tehnika plaćanja debitnom karticom prodavcu/dobavljaču roba i usluga odvija se na slijedeći način:

1. Banka izdaje debitnu karticu imaocu tekućeg i/ ili deviznog računa,
2. Imalac debitne kartice kao kupac posjećuje www stranicu prodavca odnosno dobavljača roba i usluga i nakon odabira roba i/ili usluga naručuje iste i upisuje PIN broj debitne kartice,
3. banka u skladu sa instrukcijom prenosi novac sa računa kupca na rašun prodavca,
4. Trgovac nakon toga provjerava stanje svog računa i izdaje robu i/ ili izvršava uslugu kupcu vlasniku debitne kartice.

3.8.1.4. Zloupotrebe kreditnih i debitnih kartica

Globalna rasprostranjenost platnih kartica, njihovo korištenje te laka dostupnost modernih tehnologija, učinile su ih izuzetno atraktivnim objektom napada kriminalaca. Na udaru su nova i nedovoljno razvijena tržišta, bez dovoljnog tradicije i sigurnosne kulture u kojima ne postoji sistem za prepoznavanje i sprječavanje zloupotreba. Takvo tržište je potencijalno lagan plijen za vješte i iskusne kriminalce i organizovane kriminalne grupe.

Najčešći pojavni oblici zloupotrebe I falsifikovanja platnih katica su:

- ✓ Zloupotreba ukradenih ili izgubljenih platnih kartica;
- ✓ Zloupotreba neisporučenih platnih kartica;
- ✓ Neovlašteno korištenje tuđe platne kartice;
- ✓ Izrada I korištenje lažnih platnih kartica;
- ✓ Prikupljanje podataka za izradu lažne platne kartice;
- ✓ Zloupotreba platnih kartica od strane akceptanta;
- ✓ Zloupotreba od strane korisnika.

Iz široke lepeze zloupotreba platne kartice treba izdvojiti –krađu podataka kartice I krađa identiteta korisnika -što kasnije "novom korisniku"- dvojniku daje priliku da koristi sredstva veoma dugo ,praktično dok je dovoljno oprezan da korisnik kartice ne identificira ilegalno korištenje preko stanja na izvodu. Krađa podataka kartica se vrši uređajima za nelegalno čitanjem koji se postavlja na bankomate ili na naplatnim mjestima. Takvi uređaji kopiraju podatke sa kartice kao i unesene PIN kodove. Nelegalno prikupljeni podaci se kasnije koriste za izradu lažnih kartica tzv. duplikata.

Krađa identiteta korisnika se najčešće vrši putem interneta-lažnim sajtovima za kupovinu ili lažnim sajtovima banaka, tzv. phising sajtovi. Korisnici računara se vrlo naivnom prevarom navedu da ostave svoje podatke na tim sajtovima.

3.8.1.5. Pametne/Smart kartice

Tehnologija pametnih kartica je već odavno poznata,a svoju primjenu je između ostalog načela i u mobilnoj telefoniji. Naime već duže vrijeme u upotrebi su telefonske katice(SIM) sa memorijskim čipom u kojem su pohranjene određene inormacije. Razvojem mobilne telefonije i tzv. Prepaid usluge (unaprijed plaćena usluga) pametne kartice postaju sve popularnije i prihvatljivije. Smart kartica je plastična kartica dimenzija uobičajenih za kreditne I debitne kartice s tom razlikom da je u nju ugrađen čip. Drugim riječima ,plastičnu karticu "pametnom" čini čip. Čip je u suštini ,mikroprocesor sa memorijskim kapacitetima u kojima se mogu pohraniti značajne količine informacija . Na pametnoj kartici koja sadrži mikroprocesor postoji mogućnost upisivanja podataka, brisanja ili neke druge vrste

manipulacije podacima. Kartica koja ima samo memorijski čip može izvoditi samo predefiniranirane funkcije. Smart kartica za razliku od kartica sa magnetnom trakom,sadrži sve potrebne funkcije za autorizaciju, zbog čega u trenutku transakcije nije potreban pristup udaljenim bazama podataka.

Da bi se mogla koristiti, na računaru se mora imati instaliran čitač smart kartice. Čitač kao i softver potreban za instalaciju čitača, na računar,korisnik mora kupiti od banke pri registraciji za korištenje usluge.

Smart kartica se zasniva na PKI (Public Key Infrastructure) tehnologiji koja se zasniva na asimetričnoj kriptografiji, odnosno paru javnih i tajnih ključeva za šifriranje podataka. Svaki korisnik ima svoj tajni ključ i svoj javni ključ. Samo se javni ključ korisnika daje drugima na uvid. Korisnik koji želi podatke poslati nekome šifrira svojim tajnim ključem. Kada se ti podaci pošalju pročitati ih može svako ko posjeduje javni ključ pošiljatelja. Iz tog razloga pošiljatelj šifrira podatke još jedanput ,samo ovaj put javnim ključem primatelja podataka. Na taj način podaci su dostupni samo primatelju podataka. Naime primatelj podataka ih mora dešifrirati najprije pošiljteljevim javnim ključem, a zatim i svojim tajnim ključem. Svi su ti ključevi u digitalnom obliku pohranjeni na smart kartici.

Smart kartica se uvelike razlikuje od kreditne kartice unatoč sličnostima u obliku i veličini. Dok je u unutrašnjost smart kartice umetnut 8-bitni mikroprocesor,normalna kreditna kartica u potpunosti je sačinjena od plastike. Mikriprocesor se u smart kartici nalazi ispod "zlatnog čipa" na prednjoj strani kartice. Radi lakšeg poimanja uloge čipa treba ga razumijevati kao zamjenu za magnetnu traku prisutnu na kreditnim ili debitnim karticama. Kod magnetne trake podaci se mogu jednostavno čitati, upisivati, brisati ili pak mijenjati. Kako pristup podacima ne bio jednostavan kao kod magnetne trake na samrt karticu se ugrađuje mikroprocesor.

Samrt kartice se najčešće koriste kao:

1. kreditne kartice,
2. elektroničke kartice,
3. kartice za internet bankarstvo,
4. kartice za kodirane satelitske programe,
5. kartice za identifikaciju u vladinim institucijama,
6. kartice kod bežične komunikacije,
7. kartice za računarski sigurnosni sistem,
8. kartice za mobilne uređaje[142].

Prednost PKI tehnologije jeste izuzetno visok nivo sigurnosti. Naime, još uvijek nije zabilježen niti jedan slučaj upada ili zloupotrebe bankarske transakcije na Internetu u kojoj su se korisnici autorizirali uz pomoć ove tenologije. Zbog izuzetno visokog nivoa sigurnosti ,ali i visoke cijene čitača samrt kartica ,opisana tehnologija/metoda autorizacije je najprikladnija za pravne osobe. Pored vioke cijene, nedostatak smart kartice je i potreba za čitačem na svakom računaru sa kojeg se želi obaviti transakcija. Zbog toga je upotreba smart kartice prihvatljiva za sada smo pravnim licima koja inače obavljaju transakcije uvijek sa istih mjesta(iz svojih ureda).

[142] http://ahzco.ffri.hr/seminar/2005/ebankarstvo/smart kartice.htm

3.8.2. Simbolički sistem elektronskog plaćanja

Za razliku od notacijskog sistema gdje novac zapravo nikad ne napušta banku ili banke, simboličkom ili gotovinskom sistemu sama reprezentacija nosi njegovu vrijednost. Ovo praktično znači da se iznos na računu umanjuje čim se e-novčanica podigne iz banke. Ova vrsta e-novca analogna je klasičnoj gotovini i zato se obično naziva e-gotovina.

3.8.2.1. E-gotovina

E-gotovina ima karakteristike slične klasičnoj materijalnoj gotovini. Klasična matrijalna gotovina je univerzalno prihvaćena, prihvaćena je za plaćanje od strane pravnih I fizičkih lica,kupci pri upotrebi gotovine ostaju anonimni,autentičnost novca se lako obavlja pri samoj gotovinskoj transakciji odnosno plaćanju, za posjedovanje i raspolaganje gotovinom nije nephodan račun u banci, prenosiva je između pravnih i fizičkih osoba, korisnici ne moraju imati poslovnu sposobnost i sl.

Pored navedenih dobrih strana klasične materijalne gotovine ona ima i brojne nedostatke od kojih su najvažniji: relativno visoki troškovi za proizvodnju, distribuciju, povlačenje i zamjenu,nepraktičnost fizičkog nošenja veće količine novca, na raspolaganju je ograničen broj nominacija (apoena), lako ga je otuđiti i krivotvoriti, gotovina egzistira u brojnim valutama ,a njihovu konverziju prate nemali troškovi, neupotrebljiva u području cyber ekonomije i sl.

Da bi u potpunosti perspektivno supstituisala klasičnu materijalnu gotovinu ,e-gotovina mora zadržati sve dobre strane klasične materijalne gotovine i eliminirati po mogućnosti što više loših osobina klasične materijalne gotovine. Idealna gotovina morala bi zadovoljiti slijedeće zahtjeve:

1. mora se onemogućiti krivotvorenje e-novčanica,
2. mora se omogućiti jednostavno i besplatno pretvaranje klasične materijalne gotovine u e-gotovinu i obrnuto,
3. mora se onemogućiti plaćanje dva puta istom e-novčanicom,
4. mora se sačuvati anonimnost onoga ko raspolaže e-novčanicom,
5. mora se omogućiti *off line* provjera auitentičnosti e-novčanica,
6. mora biti moguć prenos e-novčanica bez dozvole treće strane,
7. e-novčanica mora biti upotrebljiva bez računa u banci,
8. mora se omogućiti "usitnjavanje" e-novčanica u željene iznose,
9. mora biti jednostavan za računarske resurse,
10. mora biti neinteraktivan.

Postoji nekoliko modela e-gotovine. Najčešće se pominju Chaumov i Brandsov model. Oba pomenuta modela ispunjavaju prva četiri zahtijeva. Chaumov model predviđa detekciju dvostrukog plaćanja istom novčanicom,a Brandsov model njezino sprečavanje hardvesrskim sklopom. Samo Bransov model omogučava i usitnjavanje. Ni jedan ni drugi model ne predviđaju mogučnost prenosa e-novčanica između osoba bez posrednika(banke),već prilikom svakog prijema e-novca kao utška primalac mora novac položiti u banku,a onda ga ponovo podići iz banke za dalje elektronsko plaćanje.

3.8.2.2. Problemi u prenosu e-novčanica

Kod prenosa e-novčanice između dva sudionika javljaju se dva vrlo značajna problema:

- pri svakom prenosu e-novčanica "raste" s obzirom na činjenicu da se na nju dodaju podaci o novom vlasniku na koga je ista prenešena,
- obzirom da se polaganje e-novčanica u banku može odlagati na neodređeno vrijeme,odgađa se i potencijalna detekcija višektrano potrošene e-novčanice

Više nego očigledan je da sistem koji omogućava prenosivost e-novca mora počivati na fizičkom sprječavanju višekratnog plaćanja istom e-novčanicom. Osim navedena dva modela u literaturi se spominje i Fergusonov model,koji ima propust u sigurnosnom sistemu i Okamotov model koji je svojevrsna nadgradnja Brandsovog modela i zadovoljava tačke 1-7,ali je suviše složen i zahtijevan.

Tačka 10. posebno je zahtjevna. Neinteraktivnost podrazumijeva d je moguće poslati e-gotovinu samo posredstvom jedne poruke, bez povratne poruke ili dodatne interakcije među korisnicima.

3.8.2.3. Plaćanje e-gotovinom

E-gotovina se sastoji od e-novčanica koje su ekvivalent papirnatih i kovanih novčanica. Prije raspolaganja e-gotovinom klijent odnosno kupac je mora podignuti u banci.Prilikom plaćanja trgovcu odnosno dobavljaču mora biti omogućen provjera autentičnosti e-novčanica. Postoje dva modela provjere autentičnosti ovisno o tome ima li trgovac on-line vezu s bankom u trenutku plaćanja ili ne.

3.8.2.3.1. On-line

Ako trgovac ima on-line vezu s bankom u trenutku kupnje,tada promet e-gotovine teče na slijedeći način:Kupac podnese banci nalog za izdavanje e-novčanice. Banka prima zahtijev i provjerava identitet podnositelja zahtijeva. Ako je provjera pozitivna banka umanjuje saldo na računu podnositelja zahtijeva i izdaje e-novčanice u zahtijevanom iznosu,s jedinstvenim serijskim brojem I digitalnim potpisom banke s bančinim privatnim ključem. U bazi podataka automatski bilježi serijski broj e-novčnice. Kupac odlazi u viritualnu trgovinu,gdje kupuje ropbu i usluge od trgovca tem u predaje elektroničku novčanicu.Trgovac kontaktira banku i traži provjeru ispravnosti dobivene novčanice. Ako je novčanica ispravna,trgovac je odmoh polaže na svoj račun i kupcu daje robu.

3.8.2.3.2. Off-line

(U *off-line* sistemu trgovac nema veze sa bankom u trenutku plaćanja, pa stoga mora imati način provjere autentičnosti e-novčanice na licu mjesta. Način plaćanja u *off-line* sistemu teče na slijedeći način:kupac podnese banci nalog za izdavanje e-novčanice. Banka prima zahtjev ,provjerava identitet podnosioca zahtijeva i ako je provjera pozitivna,umanjuje saldo na računu podnositelja zahtijeva i izdaje e-novčanice u zahtijevanom iznosu,s jedinstvenim serijskim brojem i digitalnim potpisom banke s bančinim privatnim ključem. U bazi podataka automatski bilježi serijski broj e-novčanice. Kupac odlazi u virtualnu trgovinu, gdje kupuje robu i usluge od trgovca te mu predaje elektronsku novčanicu. Trgovac provjerava ispravnost bančinog elektronskog potpisa uz pomoč bančinog javnog ključa. Trgovac izdaje robu kupcu

i zatim polaže e-novac u banku. Banka provjerava autentičnost potpisa izdavatelja i provjerava je li već ranije položena. Ako je eve uredu uvećava iznos na računu trgovca.

3.8.2.4. Nedostaci u plaćanju elektronskim novcem

Predstavljeni model plaćanja e-gotovinom je jednostavan ali ima i brojne nedostatke. S obzirom na činjenicu da banka u trenutku izdavanja e-novčanica kupcu zna njegov identitet, može za svaku izdanu novčanicu uz serijski broj u bazi podataka zabilježiti datum i vrijeme, kao i identitet kupca. Nakon što trgovac položi e-novac u banku, banka može tačno znati kada, gdje i za koji iznos je kupac nešto kupio, što znatno narušava privatnost kupca. Također, s obzirom na činjenicu da su e-novčanice samo podaci (u memoriji kartice ili na disku), kupac bi mogao novčanice jednostavno iskopirati i njima ponovo platiti robu ili uslugu. Ukoliko bi se to desilo trgovac koji je primio kopirnu novčanicu ukoliko bi pokušao položiti novac naišao bi na odbijanje banke da prizna tu novčanicu, jer je već ranije potrošena. Ovaj problem se zove problem dvostruke potrošnje i ključan je u implementaciji e-gotovine.

3.8.2.5. Mikroplaćanje

Mikroplaćanja su posebna vrsta e-gotovine, čije obilježje su vrlo mali iznosi, npr. reda veličine 1 centa ili feninga ili manje. Ovakva vrsta plaćanja je potrebna za plaćanje vrlo jeftinih sadržaja, koji se međutim moraju kupovati vrlo brzo. Tipičan primjer potrebe za ovakvim plaćanjem je telefonska govornica. Ova plaćanja se u pravilu riješena kao *off-line* plaćanja.

3.8.2.6. Rizici pri korištenju elektronskog novca

Brojni su rizici imanentni korištenju elektronskog novca od kojih se posebno treba izdvojiti (1) Odabir algoritma za kripitiranje, (2) Odabir ključa (duljina i vrijednost), (3) Propusti u dizajnu, (4) Propusti u implementaciji, (5) Propusti u izvedbi, i (6) ljudski faktor.

3.8.2.7. Zakonski preduslovi za korištenje e-novca

Korištenje elektronskog novca zahtijeva donošenje zakona koji rješavaju četiri ključna pitanja:

1. formalnopravnu valjanost digitalnog potpisa;
2. pozicija elektronskog novca u postojećem monetarnom sistemu;
3. pozicija elektronskog novca u poreznom sistemu;
4. sprječavanje kriminalnih radnji.

Bosna i Hercegovina je pristupila donošenju zakona koji bi trebalo da riješe navedena pitanja. Prvi korak je bio ratifikacija Konvencije o kibernetičkom kriminalu i Dodatnog protokola čime je stvorena pretpostavka da se u domaćem krivično-materijalnom i krivično-procesnom zakonodavstvu stvore pretpostavke za efikasno i efektivno suprotstavljanje *cyber* kriminalu. Nakon ratifikacije Konvencije i Dodatnog protokola donesen je savremen Zakon o elektronskom potpisu BiH[143] i Zakon elektronskom pravnom i poslovnom prometu[144] sa

[143] Vidi "Službeni glasnik BiH", broj 91/06,
[144] Vidi "Službeni glasnik BiH", broj 88/07,

pratećim podzakonskim propisima. Zakon o elektronskom potpisu su također donijeli entitet Republika Srpska[145] kao i Brčko Distrikt Bosne i Hercegovine[146]. Federacija nema legislative za primjenu elektronskog potpisa, jer se oslanja na Zakon o elektronskom potpisu BiH.

Navedenim zakonima uređena je upotreba elektronskog potpisa u pravnim poslovima i drugim pravnim radnjama, kao i prava i obaveze i odgovornosti u vezi sa elektronskim certifikatima (potvrdama). U Republici Srpskoj pored zakona, a u skladu sa Strategijom Vlade od 2009. do 2012. godine Vlade Republike Srpske, donesen je cijeli niz podzakonskih akata koji uređuju područje kao što su evidencija davaoca usluga certificiranja elektronskih potpisa, jedinstveni registar davaoca usluga certificiranja elektronskih potpisa koji izdaju kvalificirane certifikate, mjere i postupci upotrebe i zaštite elektronskog potpisa, sredstva za izradu elektronskog potpisa, obaveznog osiguranja davaoca usluga izdavanja kvalificiranih certifikata. Preostala pitanja dva pitanja još uvijek se nisu u postupku rješavanja iz više razloga čija elaboracija bi zahtijevala više prostora.

3.8.2.8. Elektronski novac u praksi

Iako su dostignuća u kriptografiji pokrila gotovo sve sigurnosne i praktične zahtjeve za sve oblike elektronskog plaćana i elektronskog novca, rasprostranjenost ovih načina plaćanja je zanemariva u odnosu na klasične oblike plaćanja. Kompanije koje su u devedesetim godinama ušle na područje elektronskog novca uglavnom su bankrotirale. Druga generacija koja se pojavila krajem devedesetih nešto je uspješnija,a to su DigiCash, CyberCash, Billpoint, PayPal, Chipknip i Mondex.

3.8.2.9. Rizici u sistemu elektronskog plaćanja

Primjena novih elektronskih sistema plaćanja nosi sa sobom i određene rizike, koji se odnose na mogućnost zloupotrebe ovih sistema u svrhu pranja novca. Eksperti Radne grupe za finansijske akcije (FATF) su u svom izvještaju o tipologijama pranja novca za period 1998. do 1999. godine identifikovali slijedeće rizike:

- Nemogućnost identifikovanja i potvrđivanja lica koja koriste nove tehnologije,
- Nivo transparentnosti transakcija,
- Odsustvo ili neadekvatnost kontrole u vođenju evidencija ili izvještavanju o sumnjivim transakcijama od strane prodavca tehnologije,
- Korištenje šifrovanja na visokom nivou (čime se blokira pristup sudskih organa,
- Transakcije koje nisu obuhvaćene trenutnom legislativom ili regulatornim definicijama.
-

3.8.3. Elektronski transfer sredstava i međubankarsko plaćanje

Razvoj cyber/elektronskog bankarstva podrazumijeva da se sve više uvode savremene elektronske procedure plaćanja, isključivo zasnovane na elektronskom transferu sredstava. Elektronski transfer sredstava (*Electronic Funds Transfer – EFT*) eliminiše potrebu fizičkog prenosa kreditnih poruka na papirnim nosiocima podataka, odnosno primjena EFT sistema omogućava da se za nekoliko sekundi izvrši plaćanje sa računa dužnika na račun povjerioca. Treba praviti razliku između EFT i EPS sistema, jer je EFT sistem širi pojam od EPS sistema.

[145] Vidi Zakon o elektronskom potpisu RS („Službeni glasnik RS “,broj 59/08),
[146] Vidi Zakon o elektronskom potpisu Brčko distrikta Bosne i Hercegovine („Službeni glasnik Brčko Distrikta Bosne i Hercegovine“, broj 39/10, 61/10, 14/11, 56/11).

EPS sistem (*Electronic Payments System*) se odnosi samo na elektronski sistem plaćanja, dok se EFT sistem odnosi na svaki oblik elektronskog prenosa sredstava.

U oblasti međubankarskog plaćanja trenutno dominira SWIFT mreža. Primjenom SWIFT sistema u međubankarskim plaćanjima zamijenjene su komunikacije putem telefona, telefaksa, pošte kurira i sl. Radni dan SWIFT sistema traje 24 časa tokom 365 dana u godini. Sistem radi on line, transferi se vrše u vrlo kratkom vremenu, tajnost podataka je osigurana preko šifriranih poruka. Svaki korisnik SWIFT sistema ima svoj kod, što u stvari predstavlja SWIFT adresu. SWIFT sistem počinje da funkcioniše kada banka iz jedne zemlje izvrši formatiranje poruke i istu prenose terminalom do regionalnog koncentratora. Poruka se putem SWIFT mreže daje prosljeđuje do operativnog centra, a potom se dalje upućuje na regionalni centrator i terminal banke koja je primalac elektronske poruke.

3.9. Međunarodni propisi i standardi kojim se regulira sprečavanje pranja novca

U ovom dijelu edukativnog modela slijedi kratko predstavljanje temeljnih međunarodnih propisa i standarda koji reguliraju sprječavanje pranja novca i financiranja terorizma. Naglašavamo da su radi preglednosti nazivi konvencija , direktiva uredbe u naslovima navedeni u cijelosti, dok u tekstu i nadalje koristim skraćenice slijedom supra navedenog.

3.9.1. Konvencija Ujedinjenih naroda protiv nezakonitog prometa opojnih droga i psihotropnih tvari

Konvencija UN protiv nezakonitog prometa opojnih droga i psihotropnih tvari kao međunarodna konvencija je svojim obuhvatom usmjerena konkretno protiv nezakonitog prometa opojnih droga i psihotropnih tvari, s posebni naglaskom na ozbiljnost problema opojnih droga i mjera za njegovo iskorjenjivanje. Osim što predstavlja značajan trenutak u međunarodnom suzbijanju prometa opojnih droga, sadržajno gradi i prvi sveobuhvatan sporazum koji zahtjeva poduzimanje preventivnih i represivnih mjera pranja novca za njezine potpisnice[147]. Zapravo, radi se o prvom međunarodnom sporazumu za kažnjavanje pranje novca, „iako se kažnjavanje odnosi samo na ograničeni broj predikatnih djela (konvencija se odnosi samo na promet droge) iz kojih prljavi novac zapravo proizlazi“

Naglašava se važnost međunarodne suradnje, „teži za ujedinjavanjem kazneno-pravne regulative“ te propisuju mjere zaplijene i konfiskacije profita stečenih od nezakonite proizvodnje i prometa narkoticima. „Konvencija UN sadrži vjerojatno najveći nagovještaj o prijetnji nezakonite prodaje droga na globalnom nivou“.

3.9.2. Konvencija 141. Vijeća Europe o pranju, traganju, privremenom oduzimanju i oduzimanju prihoda stečenog krivičnim djelom (Strazburg 1990)

Konvencija VE donijeta je u Strasburgu 1990. kao cjeloviti akt usmjeren na postizanje većeg jedinstva u vođenju zajedničke krivične politike usmjerene na suzbijanje teških kaznenih djela i lišavanju počinitelja kaznenog djela tako stečenih prihoda. Nekim odredbama (npr. okvirni opis kaznenog djela pranja novca) bazira se na Konvenciji UN koja svakako predstavlja značajni korak prema „integraciji pojedinih oblika suradnje između država u kaznenim stvarima objedinjavanjem odredaba o izručenju, transferu zapisnika i uzajamnoj

[147] Slično u Graham, T., Bell, E., Elliott, N, (2006) Money Laundering (Butterworth's Compliance Series), Butterworth-Heinemann, Wiltshire, str. 29.

pravnoj pomoći te najnovijem modalitetu suradnje u kaznenim stvarima, a vezano za privremeno oduzimanje i konfiskaciju imovine".

Zbog ograničenja glavnim ciljem Konvencije UN – zabrana nezakonitog prometa droge, jasna je nužnost donošenja Konvencije VE koja je objedinila mehanizme uzajamne pravne pomoći, privremene mjere i oduzimanje prihoda stečenog kaznenim djelom, a sve to vezano uz materiju sprječavanja pranja novca.

U tom nastojanju, Konvencija VE predstavlja sveobuhvatan sistem pravila koji obuhvata brojne proceduralne aspekte povezane s pranjem novca - od inicijalne istrage do zaključne konfiskacije. „Takav pristup pruža posebne mehanizme koji predstavljaju zahtjev za najvećim opsegom međunarodne suradnje, a ujedno onemogućavaju zločinačkim organizacijama pristup instrumentima pranja novca i sredstvima stečenim počinjenjem kaznenog djela".

Temeljni ciljevi Konvencije VE odnose se prvenstveno na postizanje većeg jedinstva među državama članicama u vođenju zajedničke kaznene politike. Suzbijanje teških kaznenih djela sve više dobiva obilježja međunarodnog problema i zahtjeva uporabu suvremenih metoda na međunarodnoj razini. Najvećim se djelom te metode odnose na učinkovitu međunarodnu suradnju i međunarodnu pravnu pomoć u kaznenim postupcima i istragama kaznenih djela te pronalaženje, oduzimanje i konfiskaciju profita nastalih istim kaznenim djelima.

Generalno gledajući, potpisnice Konvencije VE poduzimaju mjere u cilju kriminalizacije pranja prihoda iz kaznenih dijela te oduzimanja instrumenata i profita ili imovine koja odgovara tim iznosima. Istaknut je značaj suradnje u istragama, osiguravanju dokaza, kao i spontano dostavljanje podataka drugoj članici. Uklanja se bankarska tajna. Također se određuju privremene mjere kao što su blokiranje bankovnih računa i privremeno oduzimanje imovine sprječavajući daljnju kupoprodaju, a sve u cilju oduzimanja nezakonito stečenih prihoda i provođenja naloga za konfiskaciju, odnosno nacionalna postupanja koja vode konfiskaciji na zahtjev druge države članice.

3.9.3. Konvencija Vijeća Europe o pranju, traganju, privremenom oduzimanju i oduzimanju prihoda stečenog krivičnim djelom te o finansiranju terorizma

Izmjene i ažuriranje Konvencije VE 148, razvoj metoda i tehnika pranja novca, a ponajviše uznapredovali terorizam na globalnom nivou doprinijeli su donošenju Varšavske konvencije. Bit Varšavske konvencije ne odudara previše od Konvencije VE jer se i nadalje fokusira na mjere provođenja istrage, zamrzavanja, privremenog oduzimanja i konfiskacije prihoda stečenog kaznenim djelom, kaznenim djelom pranja novca te međunarodnu suradnju, međutim unosi i vrijedne novine.

Već u samoj preambuli, a kasnije i u prvom poglavlju gdje su objašnjeni termini Varšavske konvencije, jasne su novine u pogledu problematike terorističkih akcija kao prijetnje međunarodnom miru i sigurnosti, određivanja financiranja terorizma kaznenim djelom te značaja prevencije pranja novca i financiranja terorizma, a nastavno i uloga financijsko-obavještajne jedinice.

[148] Konvencija VE ažurirana je 2001. usvajanjem Okvirne odluke Official Journal L 182, 5.7.2001.

3.9.4. Preporuke FATF-a

Dok se problem pranja novca na nacionalnoj razini rješava učinkovitom legislativom, najbolje rješenje međunarodnog problema pranja novca može se naći samo na međunarodnoj razini. Sve veća zabrinutost međunarodne zajednice zbog rizika pranja novca koji predstavlja prijetnju bankarskom sustavu i drugim financijskim institucijama, navela je u srpnju 1989. grupu zemalja G-7 (SAD, Japan, Francuska, Njemačka, Italija, Ujedinjeno Kraljevstvo i Kanada) da na Samitu u Parizu osnuju Grupu za financijsku akciju protiv pranja novca (FATF).

Osnovna zadaća FATF očituje se u uspostavljanju međunarodnih standarda i globalne akcije u suzbijanju pranja novca i financiranja terorizma, na nacionalnoj i međunarodnoj razini. Djelovanje FATF odnosi se konkretno na nadzor procesa prevencije i represije u državama članicama, razmatranje trendova pranja novca i financiranja terorizma te izradu tipologija, pregled radnji poduzetih na nacionalnom i međunarodnom nivou, kao i implementaciju odgovarajućih mjera za njihovo suzbijanje na globalnom planu.

Drugim riječima, mandat FATF se odnosi na „procjenjivanje rezultata već ostvarene suradnje s namjerom prevencije iskorištavanja bankarskog sustava i financijskih institucija u svrhu pranja novca te razmatranje dodatnih preventivnih mjera na tom području, uključujući prilagođavanje pravnog i nadzornog sistema kako bi se unaprijedila multilateralna pravna pomoć“.

U taprilu 1990. što je manje od godine dana od njegovog osnutka, FATF je izradio izvješće s 40 Preporuka za sprječavanje pranja novca. Izvješće je predstavljalo „djelotvorni alat u izgradnji jedinstvene politike u suzbijanju pranja novca, iako nije imalo pravnog učinka“, ali su zato Preporuke postavile temelj jasnog cilja suzbijanja organiziranog kriminaliteta i pranja novca obuhvaćajući pravni, financijski i nadzorni aspekt. Od država se tražilo kriminaliziranje pranja novca, omogućavanje njegove konfiskacije i razmjenjivanje informacija o sumnjivim transakcijama. Na taj će način financijski i nefinancijski sektor osvježiti novim pravilima prevencije pranja novca.

Preporuke FATF su snažno podupirale implementaciju UN Konvencije, ograničenje bankarske tajne u mjeri u kojoj ne ometa otkrivanje i suzbijanje pranja novca, kao i osnaženu uzajamnu pravnu pomoć u istragama pranja novca. Nadalje, pozivale su na kriminalizaciju pranja novca ograničenu na novac podrijetlom iz kriviČnog djela vezanog za drogu ili narkotike, odnosno predlagale su minimum odredbi kaznenog zakona koje reguliraju problematiku pranja novca.

Obuhvat Preporuka je 1996. znatno proširen i zahtijeva kriminalizaciju pranja novca s obzirom na utvrđena teška kaznena djela. Međutim, već 2003. Preporuke FATF su ponovno revidirane. Zahtjevi efikasnog sistema sprječavanja pranja novca nadopunjeni su smjernicama za sprječavanje financiranja terorizma. Kriterij sustavnog pristupa preventivnim i represivnim mjerama time je još više pooštren.

3.9.4.1. Preporuke vezane za sprječavanje pranja novca

Glavna uloga FATF očituje se u ispitivanju tehnika i trendova pranja novca, pregledu mjera koje su već poduzete na domaćoj i međunarodnoj razini te planiranju onih koje se još trebaju

poduzeti po pitanju suzbijanja pranja novca, ali i financiranja terorizma[149]. U tom svijetlu, razvojem metoda i tehnika pranja novca razvijala se i mijenjala svijest o problemu koji on predstavlja. U tom su se smjeru usavršavale i Preporuke koje su sve detaljnije navodile pojedine obveze, ali bez velikih ograničenja. Postale su jasnije i lakše za primjenu, uz proširen obuhvat njihove primjene na nove obveznike.

U okviru 40 Preporuka obrađuju se sve najvažnije mjere efikasnog sistema suzbijanja i sprječavanja pranja novca između kojih vrijedi istaknuti proširivanje kruga obveznika (s financijskih) na nefinancijske institucije, identifikaciju stvarnog vlasnika, poduzimanje mjera dubinske analize, povratnu informaciju, izvješćivanje, nadzor i regulaciju sumnjivih transakcija te međunarodnu suradnju.

Postavljenim standardima FATF neprekidno potiče sve zemlje svijeta da usvoje mjere iz Preporuka. Ne postoji ograničenje za njihovo prihvaćanje, bez obzira na različitost pravnih i financijskih sistemaa upravo zbog toga što dopuštaju fleksibilnost, a ne predviđaju svaki detalj provedbe. Preporuke predstavljaju najbolju međunarodnu praksu, ali postavljaju i visoke standarde u zaštiti financijskog i nefinancijskog sektora od štetnih utjecanja prihoda nezakonitih aktivnosti.

Originalnih 40 Preporuka iz aprila 1990. postavile su osnove sistema sprječavanja pranja novca, uključujući njihov značajni utjecaj na financijske institucije i nadzorna tijela. Već 1996. FATF predlože čitav niz aktivnosti za uspješnije suzbijanje pranja novca, bez obzira na različitost pravnih i financijskih sustava pojedinih zemalja. To su vrlo važne odredbe o ulozi pravnih i financijskih sistema u suzbijanju pranja novca primjenom kojih je velik broj banaka uskladilo svoje poslovanje s Preporukama FATF.

Osobito je važno definiranje složene problematike uočavanja i prijavljivanja sumnjivih transakcija zbog čega Preporuke iz 1990. zahtijevaju obavješćivanje nadležnih tijela prilikom svake sumnje na nezakonite aktivnosti. Revidirane Preporuke iz 1996. usvajaju specifičniji zahtjev za prijavom sumnjivih transakcija. U vezi s time vrlo je malo nadopuna i pomnijeg definiranja sumnjivih transakcija u 2003.

Kako su se države sve više približavale uređivanju tradicionalnog financijskog sektora, FATF je uočio da su perači novca pronašli alternativne načine kao što su *shell* tvrtke, elektronski prijenos novca, nebankarske financijske institucije (putničke agencije, posrednici pri prodaji nekretnina i sl.). zbog čega više ne postoji mjesto ili struka koja ne pruža mogućnost pranja novca, a kasnije i financiranja terorizma.

Važno je napomenuti da su Preporuke iz 1990. općenito regulirale obveze koje se odnose na financijske i nebankarske financijske institucije, 1996. odgovarajuće Preporuke protežu svog doseg i na druge profesije, a 2003. nameću više detalja u odnosu na probni pristup prema drugim profesijama koje su u funkciji financijskih posrednika.

Postoje i druge jednako važne ispravke Preporuka koje se odnose na financijske institucije i njihove obveze prisustvovanja u suzbijanju pranja novca. Konciznost je osnovna značajka

[149] FATF je od samog trenutka osnivanja predstavljao nastojanje da se usvoje i implementiraju mjere osmišljene protiv prodiranja nezakonito stečenih sredstava u financijski i nefinancijski sustav. Kako bi se osiguralo da Preporuke prate trendove i evoluciju pranja novca, a kasnije i financiranja terorizma, inicijalnih 40 Preporuka revidirano je 1996. i 2003., čime su udareni temelji sustava sprječavanja pranja novca i namjena njihove univerzalne primjene.

Preporuka iz 1990. dok su revidirane Preporuke iz 1996. pružale više detalja. „Preporuke iz 2003. su promijenile strukturu, a odraz su problema kao što su efikasna dubinska analiza, problematika politički eksponiranih osoba i prekogranični korespondentni bankovni odnosi."

Iako nisu bile obvezujuće za primjenu, svih 40 Preporuka bilo je „potvrđeno širom međunarodne zajednice i relevantnih organizacija kao međunarodni standard za sprječavanje pranja novca". Preporuke su dostupne na Internet stranci FATF[150] .

3.9.4.2. Preporuke vezane za sprječavanje financiranja terorizma

Napredak rada FATF praćen je razvojem i dopunom Preporuka. Naknadno donošenje 9 Specijalnih preporuka vezanih za terorizam zapravo je odgovor na terorističke napade 11. rujna 2001. „Razvoj Preporuka zapravo reflektira promjenjivost trendova pranja novca i predstavlja odgovor FATF na promjenjivu ekonomsku realnost i kriminalne aktivnosti".

Samo sedam dana nakon napada na New York i Washington, 30. listopada 2001. FATF je izdao osam Specijalnih preporuka izrađenih u cilju suprotstavljanja financiranja terorizma kojima se osnažuju postojeće mjere predviđene Konvencijom UN za suzbijanje financiranja terorizma: određivanje financiranja terorizma kaznenim djelom i zamrzavanje imovine terorista. Nadalje, sadržajno su usmjerene na tri glavna kanala koje teroristi koriste za premještanje svojih sredstva: alternativni sustavi prijenosa ili doznake novca, transfer novca elektronskim putem i neprofitne organizacije.

Naredne istrage provedene nakon 9. rujna 2001. jasno ukazuju na još neke kanale za prijenos novca namijenjenog financiranju terorizma. Najvećim djelom se novac osobno, fizički prenosi preko granice ili to za nekog drugog rade „dostavljači novca u gotovini". U cilju ispravka učinjenog propusta u međunarodnim mjerama koje se odnose na sprječavanja fizičkog prijenosa novca predviđenog za financiranje terorizma ili pranja novca, FATF je izdao novu, IX Specijalnu preporuku koja se odnosi upravo na to specifično pitanje.

Za potrebe ovog modela posebno treba izdvojiti VII specijalnu preporuku koja za cilju ima poboljšanje transparentnosti svih vrsta transfera novca elektronskim putem, unutar zemlje i međunarodno,olakšavajući pri tome tijelima provođenja zakona da slijede elektronski prijenos novaca od strane kriminalaca i terorista. Ona propisuje obvezu poduzimanja mjera financijskih institucija (uključujući i institucije koje se bave međunarodnim novčanim doznakama), u cilju pribavljanja tačne informacije o transferu sredstava, kao i provođenja pojačane kontrole i nadzora transfera sredstava koji ne sadrže osnovne informacije o pošiljatelju.

Tragom svojih nastojanja FATF se pretvara u međunarodni forum za razmatranje problema pranja novca, a značaj mu se povećava i zbog zacrtanih osnovnih ciljeva: razvoj Preporuka protiv pranja novca i financiranja terorizma, provođenja uzajamne evaluacije država članica FATF, izrade tipologija pranja novca, poduzimanje inicijativa vezanih za nekooperativne države i teritorije te kontinuiranog obnavljanja i prilagođavanja Preporuka novim metodologijama i tehnikama pranja novca, a posebice financiranja terorizma.

[150] http://www.fatf-gafi.org.

3.9.5. Direktiva 91/308/EEC o sprječavanju korištenja financijskog sistema u svrhu pranja novca

Nakon Konvencije UN, Konvencije Vijeća Europe, 40 Preporuka FATF i bankarske prakse objavljene u Bazelskim načelima koje zajedno predstavljaju temelj sustavnog suzbijanja pranja novca, Direktiva 91/308/EEC o sprječavanju korištenja financijskog sistema u svrhu pranja novca (u nastavku teksta: Prva direktiva) svojim je odredbama uokvirila najbolju međunarodnu praksu, postavljajući visoke standarde u zaštiti financijskog i nefinancijskog sektora od štetnih efekata koje mogu prouzročiti nezakonita sredstva.

Prva je direktiva jednim djelom predstavljala dokaz da sloboda kretanja kapitala i prednosti globalne ekonomije neće utjecati na organizirani zločin, odnosno neće pridonijeti ili olakšati veću pokretljivost nezakonitih prihoda izvan granica matičnih zemalja. U tom se smislu njezin cilj očituje u „onemogućavanju prihvaćanja mjera pojedinim državama koje su u suprotnosti sa slobodnim i jedinstvenim europskim financijskim tržištem“[151], već usvajanje odredaba namijenjenih prvenstveno sprječavanju pranja novca, dok se ujedno se štiti povjerenje javnosti u cjelokupni financijski sistem.

Zajednički stav država u nastojanju sprečavanja i suzbijanja pranja novca očituje se kroz „primarne ciljeve Prve direktive: 1) zahtijevati od država članica da u svoje zakonodavstvo uvedu zabranu pranja novca najkasnije do 1. siječnja 1993. i 2) pojačati suradnju između država članica u istragama i kaznenom progonu vezano za pranje novca“.

U uvodnom dijelu, Prva direktiva nameće državama obvezu zabrane pranja novca, vrlo slično Konvenciji UN. Vrlo podrobno definira obuhvat pranja novca obuhvaćajući samo nezakonite prihode od prodaje droge. Jednako tako, potiče zemlje članice da primjenjuju pristup Konvencije VE, odnosno na suzbijanje pranja prihoda koji potiču od šireg spektra kaznenih djela (predikatno djelo)

Kako bi se odgovorilo na zabrinjavajuće pojave u području pranja novca koje narušavaju stabilnost i ugled financijskog sektora te zloupotrebu slobode kretanja kapitala i pružanja financijskih usluga, Prva direktiva je od država članica zahtijevala da zabrane pranje novca i nametnu obvezu propisivanja i provođenja mjera sprječavanja pranja novca prvenstveno financijskom sektoru.

Zakonima i podzakonskim aktima države su obvezne postaviti standarde za identifikaciju stranke, granicu prijave transakcija, vođenje i čuvanje podataka te provođenje posebnih programa obuke vezanih za sprječavanje pranja novca.

Posebno se naglašava obveza suradnje s organima odgovornim za suzbijanje pranja novca, zabranjuje otkrivanje stranci bilo kakve sumnje da se radi o nelogičnoj ili sumnjivoj transakciji, odnosno prosljeđivanje informacije da je transakcija prijavljena nadležnim tijelima.

Nadalje, ističe se zaštita dostavljanja informacija o sumnjivim transakcijama u dobroj vjeri, a kao najvažnija navodi obveza obavješćivanja nadležnih tijela o svim sumnjivim transakcijama kod kojih postoji naznaka mogućeg pranja novca.

[151] Preuzeto iz Savona, E., (2000), Responding to Money Laundering: International Perspectives, Harwood Academic Publishers, Amsterdam, str. 42.

3.9.6. Direktiva 2001/97/EC kojom se mijenja Direktiva 91/308/EEC

Kako je Prva direktiva predstavljala inicijalno nastojanje preventivnog sustava u suzbijanju pranja novca, uključujući većim djelom financijski sektor, revidirane Preporuke FATF i Konvencija VE nametale su nove standarde i samim time zahtijevale izmjene postojeće Direktive. Iako postoje oprečna mišljenja o učinkovitosti njene provedbe, deset godina nakon donošenja Prve direktive, „dana 4. prosinca 2001. usvojen je kompromisni tekst u cilju njezinog ažuriranja".

Novine koje donosi Direktiva 2001/97/EC (u nastavku teksta: Druga direktiva) mogu se izdvojiti u nekoliko kategorija:

a. uključivanje podružnica kreditnih i financijskih institucija, uz obvezu prijavljivanja sumnjivih transakcija nadležnim tijelima te djelovanja u skladu s odredbama Druge direktive,

b. jasan stav da su mjenjačnice i uredi za prijenos i doznaku novca također izloženi opasnostima pranja novca što je razlog njihovog uključivanja u obveznike,

c. iz istih su razloga u obveznike uključeni i investicijski fondovi, čime se želi financijski sektor obuhvatiti u što većem opsegu,

d. proširenje opsega predikatnih djela, odnosno definicije „kriminalna aktivnost" koja osim kaznenih djela u smislu članka 3. stav 1. Konvencije UN obuhvaća i aktivnosti kriminalnih organizacija, prijevaru, korupciju i kazneno djelo koje može donijeti značajni prihod i koje je kažnjivo teškom zatvorskom kaznom u skladu s kaznenim zakonom države članice.

Činjenica da pooštravanje kontrole u financijskom sektoru navodi perače novca da traže alternativne metode prikrivanja izvora prihoda od kriminala, odnosno peru novac putem nefinancijske djelatnosti, uvjetovala je proširenje obveze iz Druge direktive u svezi s identifikacijom stranke, vođenjem evidencije i izvještavanjem o sumnjivim transakcijama i na ograničeni broj djelatnosti i zanimanja za koje se pokazalo da su osjetljivi po pitanju pranja novca.

Prošireni opseg nefinancijskih institucija koje su dužne izvješćivati o sumnjivim transakcijama revidirani tekst proteže na profesije i nefinancijske djelatnosti. Posebno mjesto pritom zauzimaju trgovci predmetima velike vrijednosti (dragulji ili plemenite kovine i umjetnička djela) i organizatori izvođenja dražbi, bez obzira da li je plaćanje izvršeno gotovinom u iznosu od 15.000 Eura ili više, te kockarnice, uz određene izuzetke.

3.9.7. Direktiva 2005/60/EZ o sprječavanju korištenja financijskog sustava u svrhu pranja novca i financiranja terorizma

U posljednjem desetljeću pranje novca i financiranje terorizma imaju sve veći značaj i zauzimaju svoje mjesto na financijskom tržištu i drugim izloženim područjima, u međunarodnim razmjerima, uključujući se više država. S obzirom da se taj problem ne može riješiti isključivo represivno putem tijela provođenja zakona, naglasak se stavlja na prevenciju i ulogu financijskog, a u posljednje vrijeme sve više i nefinancijskog sektora.

Kako je specifičnost pranja novca njegov međunarodni karakter, ujedno predstavlja i osnovu za zloupotrebu slobode kretanja kapitala i pružanja financijskih usluga čemu pogoduje upravo objedinjeno financijsko područje Europske unije (u nastavku teksta: EU) . Iz istog bi se razloga nepovredivost i stabilnost kreditnih i financijskih institucija te povjerenje u financijski sustav u cjelini mogli ozbiljno narušiti, stoga ne čudi donošenje Treće Direktive koja predstavlja skup mjera donesenih u cilju ujednačavanja zakonodavstva na području sprječavanja pranja novca i financiranja terorizma.

Još jedan od razloga donošenja Treće direktive u vrlo kratkom vremenu nakon Druge direktive može se naći u okolnostima proizašlim nakon 11. rujna 2001. i postavljanja bombi u Madridu. Trećom se direktivom osnažuju postojeće mjere sprječavanja pranja novca, a značaj terorizma podignut je na višu razinu. Prema Okvirnoj odluci 2001/500/JHA koja propisuje definiciju terorizama, proširuje se i lista predikatnih djela, a vrlo se detaljno obrađuje i problematika dubinske analize stranke i pitanje utvrđivanja stvarnog vlasnika .

Kao najistaknutije međunarodno tijelo u suzbijanju pranja novca i financiranja terorizma, FATF je već do 2003. stvorio dobru podlogu i međunarodne standarde za suzbijanje pranja novca, kao i Specijalnih 9 Preporuka za sprječavanje financiranja terorizma. Kao najvažnija područja, Preporuke pokrivaju kaznenu materiju, financijska pitanja i pitanja metodologije rada i provedbe te međunarodnu suradnju na svim razinama, što čini temeljne standarde prihvaćene od svih relevantnih međunarodnih tijela (IMF, Moneyval i sl.). Upravo zbog izmjena i proširenja Preporuka FATF ukazala se potreba za usklađenjem Treće direktive s potvrđenim međunarodnim standardima, čime se nova metodologija rada prenosi u okvire EU.

Treća direktiva je prvenstveno preventivnog karaktera, a sadrži izmijenjene, nadograđene i detaljno razrađene odredbe Prve i Druge direktive. Sadržajem predstavlja širi i kompleksniji sistem sprječavanja pranja novca EU, koji u skladu s Preporukama FATF, predstavljene standarde još više osnažuje.

Iako stupanjem na snagu Treće direktive prestaje važiti Prva, a time i Druga direktiva, u narednim poglavljima obrade Treće direktive izložene su samo njene novine ili najznačajnije izmjene zbog toga što se većim djelom temelji na odredbama prvih dviju direktiva.

Područje primjene Treće direktive ostaje približno u istim okvirima uz izuzetak pravnih i fizičkih osoba koje obavljaju financijske aktivnosti povremeno ili u ograničenoj mjeri te ukoliko postoji slab rizik da se one vrše u svrhe pranja novca ili financiranja terorizma. Drugim riječima, takve institucije i osobe ne ulaze u okvir člana 3. kojim se propisuju definicije institucija, osoba i pojmova koji su predmet uređenja iste Direktive.

S druge strane, opseg Treće direktive je proširen na davatelje usluga povjereničkim društvima i tvrtkama te fizičke i pravne osobe koje trguju robom samo ukoliko su plaćanja izvršena gotovinom u iznosu od 15.000 Eura ili više..

Sistem temeljen na stepenu rizika, za razliku od sistema temeljenog isključivo na pravilima, jedna je od temeljnih značajki Treće direktive. Ovaj se sustav očituje u svakoj odredbi koja prilagođava sadržaj Direktive trenutnim uslovima opasnosti od sprječavanja pranja novca i financiranja terorizma, a što se isključivo odnosi na dubinsku analizu stranke. Stoga, vrlo se često ostavlja ograda postupanja ovisno o stepenu rizika.

Isto se može zaključiti iz odredaba koje se odnose na stvarnog vlasnika, u vezi kojeg bi institucije i osobe trebale moći same odrediti hoće li se prilikom utvrđivanja njegovog identiteta služiti javnim podacima ili će podatke tražiti od svojih klijenata. Pritom je potrebno uzeti u obzir činjenicu da su opseg dubinske analize stranke i rizik od pranja novca i financiranja terorizma međusobno povezani, što ovisi o vrsti stranke, poslovnom odnosu, proizvodu ili transakciji.

Uz stvarnog vlasnika propisuje se još nekoliko novih, ključnih termina koji se odnose na određene osobe ili institucije, uz napomenu da se odredbe, u skladu sa članom 4. Treće direktive, mogu proširiti i na struke i kategorije poduzeća osim navedenih. U pitanju su svakako aktivnosti za koje postoji posebno velika vjerovatnost da služe u svrhe pranja novca ili financiranja terorizma.

Nadalje, u smislu ove Direktive, predikatna djela uključuju sva teška kaznena djela uključujući: kaznena djela vezana uz terorizam, drogu, aktivnosti kriminalnih organizacija, prijevara, korupcija i sva druga kaznena djela kažnjiva lišavanjem slobode ili nalogom za pritvor u maksimalnom trajanju od godine dana ili većem, ili, za države čiji pravni sustav sadrži donju granicu za kaznena djela, sva kaznena djela kažnjiva lišavanjem slobode ili nalogom za pritvor u trajanju od najmanje šest mjeseci.

3.9.8. Direktiva 2006/70/EZ koja utvrđuje provedbene mjere za Direktivu 2005/60/EZ

Direktiva 2006/70/EZ je provedbenog karaktera. Utvrđuje prvenstveno provedbene mjere za Treću direktivu, vezano za tehničke aspekte definicije politički izloženih osoba, tehničke kriterije za procjenu određenih situacija u smislu predstavljaju li one nizak rizik od pranja novca i financiranja terorizma te tehničke kriterije za procjenu da li je opravdano u svezi određenih pravnih i fizičkih osoba koje provode financijsku aktivnost na povremenoj ili vrlo ograničenoj osnovi napraviti izuzetak od primjene Treće direktive.

3.9.9. Uredba br. 1889/2005 o kontroli ulaska i izlaska gotovine iz Zajednice

Osnovna svrha *supra* navedenih Direktiva EU očituje se ponajprije u želji za uvođenjem efikasnih mjera sprječavanja pranja novca i financiranja terorizma, praćenjem transakcija kroz financijski i nefinancijski sektor. Usklađivanje i prilagođavanje zakonodavstva navedenim smjernicama, a prvenstveno izrada tipologija i indikatora za praćenje sumnjivih transakcija na cijelom području obuhvata direktiva, može rezultirati alternativnim načinima ili pokušajima pranja novca (npr. porastom fizičkog prenosa gotovine preko granice u nezakonite svrhe).

Kako se velika gotovinska plaćanja i prekogranični prenosi gotovine ocjenjuju vrlo podložnim za pranje novca, već je 2005. donesena Uredba 1889/2005 o kontroli ulaska i izlaska gotovine iz Zajednice (u nastavku teksta: Uredba 1889/2005) radi uspostave mjera za otkrivanje fizičkih prenosa gotovine preko državne granice.

Propis ima formu uredbe zbog veće pravne snage, a izrađen je u svrhu dopune Prve direktive. Svojim sadržajem uređuje obvezu prijavljivanja gotovine prilikom ulaza ili izlaza iz EU, ovlaštenja nadležnih tijela, evidentiranje i obradu podataka, njihovu razmjenu, dužnost čuvanja službene tajne te sankcije u slučaju ne udovoljavanja propisanim obvezama.

Uz to što je Uredba donesena kao dopuna Prve direktive, u skladu je i s IX Specijalnom preporukom FATF koja države obvezuje na uspostavu mjera za otkrivanje fizičkog prijenosa gotovine (i prenosivih vrijednosnih papira na donosioca) preko državne granice i promovira zakonsko ovlaštenje nadležnih tijela na zadržavanje ili oduzimanje gotovine (i prenosivih vrijednosnih papira) ukoliko postoji sumnja na povezanost s pranjem novca ili financiranjem terorizma. Osim toga, važno je uspostaviti efikasan sistem prijavljivanja ili druge obveze očitovanja, kao i propisivanje djelotvornih, proporcionalnih i vrlo visokih kazni za postupanje s osobama koje lažno prijavljuju ili se lažno očituju.

Obveza prijave gotovinskog prijenosa preko granice odnosi se na gotovinu u vrijednosti od 10.000 Eura koju fizičke osobe prijavljuju nadležnim tijelima zemlje članice prilikom ulaza ili izlaza iz Zajednice. Predmet prijave je gotovina koju nosi fizička osoba, bez obzira da li je ona njezin vlasnik.

Limit od 10.000 Eura postavljen je sasvim realno s obzirom da je svrha prijave prevencija i odvraćanje kriminalaca od nezakonitog prijenosa gotovine preko granice kao načina pranja novca ili financiranja terorizma, povlačeći paralelu i s iznosom od 15.000 Eura što predstavlja limit za provođenje dubinske analize stranke.

Prenošenje financijskih sredstava preko granice ne smije se, prema članu 4. Direktive 88/361, uslovljavati izdavanjem odobrenja za to kretanje od strane nadležnih tijela. „Prethodna autorizacija ocjenjuje se mjerom koja bitno smanjuje stepen slobode odvijanja ovih transakcija i povlači za sobom pažnju administrativnih tijela koja tu slobodu čini pukom iluzijom“.

Međutim, predmetna Uredba dozvoljava propisivanje prethodne prijave prekograničnih prijenosa gotovine iznad određenih limita, što nema učinak zabrane ili suspenzije obavljanja transakcije kakav posjeduje prethodna autorizacija, ali „kao mjera omogućava nadležnim kontrolnim tijelima preveniranje ilegalnih aktivnosti povezanih s velikim gotovinskim plaćanjima i prijenosima – poput trgovine drogom, ljudima, pranja novca i financiranja terorizma“.

Svaka zemlja zasebno određuje da li će prijava imati pismeni, odnosno usmeni oblik ili će biti poslana elektronskim putem, uz napomenu da na svoj osobni zahtjev deklarant ima pravo dati informacije u usmenom obliku.

3.10. Cyber kriminal, nedobronamjerni programi namijenjeni cyber bankarstvu i pranje novca

Očito je da se sve više novca prenosi putem Internet bankarstva te da je broj *cyber*-kriminalaca u porastu. *Cyber*-kriminalci su kriminalci koji koriste slabosti Interneta i računalnih aplikacija kako bi učinili kriminalno djelo, kao što je pljačka banke. Banke više ne drže velike svote novca u svojim sefovima, sigurnosni sistemi nadzora I fizičke zaštite trezora I sefova značajno napredovali pa su i fizičke pljačke banaka su vrlo riskantne I veoma rijetke. Kako bi izbjegli ogromne rizike fizičke pljačke, kriminalci pribjegavaju cyber-pljačkama.

Napadači koriste nekoliko metoda prikupljanja informacija potrebnih za izvođenje pljački. Jedna od njih je *phishing* tehnika napada. Phishing se temelji na slanju lažiranih poruka elektroničke pošte u kojima se navodi korisnika da otkrije osjetljive podatke. Osim primjene

phishing napada, pljačkaši mogu koristiti posebne zlćudne programe, kao što su trojanski konji. Takvi se programi instaliraju na korisnikov računar i prate njegove navike te prikupljaju podatke potrebne za pristup Internet bankarstvu i obavljanje novčanih transakcija. Pri tome se služe alatima za praćenje unosa znakova s tipkovnice (eng. *keylogger*). Ukoliko je pljačka uspješna, napadači dobivaju veliku količinu novca uz vrlo mali rizik jer ih se vrlo rijetko uhvati. Mnoge velike kompanije, posebice banke često skrivaju činjenicu da ih je netko opljačkao elektronskim putem zbog toga to bi to značilo da njihovi sistemii nisu dovoljno sigurni. Uz to, takav zaključak mogao bi izazvati paniku kod klijenata banke te bi mnogo njih moglo povući svoja sredstva iz banke, što bi ako dovoljno klijenata to učini moglo dovesti i do propasti banke.

Ukoliko neko uđe u poslovnicu banke i opljačka je, vijesti o tom događaju objavljuju se elektronskim i printanim medijima u udarnom terminu i naslovnicama. Ako neko opljačka pet banaka na taj način, ljudi također o tom događaju slušaju vijesti na svim televizijskim kanalima i čitaju o tome na web stranicama i u novinama. Međutim, ukoliko pljačkaš opljačka banku putem računara, odnosno Interneta, o tome neće biti riječi u javnosti jer bi to značilo da je sigurnost banke ugrožena te da su i financijska sredstva klijenata također ugrožena. Naravno, očit motiv napada na banke je novac, odnosno ilegalno preuzimanje novca iz banke. U posljednjih nekoliko godina uočen je porast *cyber* napada na banke. *Cyber*-napad je napad na računalni resurs ili sistem upotrebom neke od tehnika zloupotrebe ranjivosti tog sistema ili korištenje korisnika računara kao posrednika za uspješno izvođenje napada. Napadači koriste raznovrsne vrste napada i inovativna sredstva kako bi opljačkali banke. Neke od metoda koje napadači koriste su krađa identiteta i/ili brojeva kreditnih krtica te korištenje keyloggera[152], trojanskih konja, crva, virusa i drugih malicioznih programa. Napadači koriste jednostavnost, brzinu i fleksibilnost Internet bankarstva namijenjenog klijentima banke za poboljšavanje "uslova" korištenja bankarskih usluga[153].

3.10.1. Programi za praćenje unosa znakova s tipkovnice (eng. Keyloggers)

Keyloggeri su zapravo špijunski programi koji prate i bilježe svaku tipku koju korisnik pritisne. Dijele se u dvije skupine:

- alati u obliku programskih paketa i
- uređaji koji se ugrađuju u dijelove računara.

Programi za praćenje unosa znakova s tipkovnice se uključuju u lanac događaja između pritiska tipke na tipkovnici i prikaza znaka na zaslonu računala. To se postiže na više načina:

- postavljanjem video nadzora,
- podmetanjem prislušnog uređaja u tastaturu,
- presretanje znakova upotrebom samog računara,
- promjenom upravljačkih programa tastature,
- promjenom programa za obavljanje posebnih funkcija tastature presretanjem funkcija jezgre operacijskog sustava ili

[152] Keyloggeri su zapravo špijunski programi koji prate i bilježe svaku tipku koju korisnik pritisne.
[153] Vidi više CARNet HRVATSKA AKADEMSKA ZAJEDNICA i ISTRAŽIVAČKA MREŽA, Bankarski zločudni programi, NCERT+(www.cert.hr) u suradnji sa LS&S(www.LSS.hr)

- presretanjem *dll* (eng. *Dynamic-link library*) funkcija (*dll* je dinamička biblioteka koja se koristi na operacijskim sistemima Windows)[154].

Uređaji za praćenje unosa znakova s tastature su obično male veličine i postavljaju se u tastaturu, na komunikacijski kabl koji povezuje tastaturu i računar ili u samo računar, dok se programski paketi sastoje od alata koji prate i bilježe pritiske tipki na tastaturi.

Napadači koriste opisane programe kako bi preuzeli osjetljive informacije kao što su brojevi kreditnih kartica, PIN-ovi, korisnički podaci i slično. Programi za praćenje unosa znakova s tastature prikupljaju podatke i dostavljaju ih na poseban računar za odlaganje takvih podataka (eng. *dropzones*) s kojih ih napadač lako može koristiti. Moguće je otkriti računar na koji program šalje prikupljene podatke obavljanjem dinamičke analize upotrebom programa za analizu ponašanja nedobronamjernih programa i simulacijom nedobronamjernih programa u kontrolisanom okruženju. Podaci dobiveni na takav način mogu se iskoristiti za automatsko otkrivanje računara za odlaganje podataka koje je prikupio program za praćenje unosa znakova s tastature. Upotreba ove tehnike vrlo je uspješna.

3.10.2. Trojanski konj

Trojanski konji jedan su od najjednostavnijih i vrlo rasprostranjenih oblika neprijateljskih programa. Oni sadrže neku korisnu funkcionalnost i time privlače korisnika da ih preuzme na svoj računar i pokrene. Tom akcijom korisnik omogućava napadaču pokretanje tzv. zlonamjernog programskog koda, odnosno pristup određenim podacima na računaru ili čak preuzimanje kontrole nad cijelim računarom (zavisno o namjeni trojanskog konja). Trojanskog konja može izraditi sam napadač ili ga može preuzeti (kupiti) od nekog drugog napadača ili skupine. Posebno opasna vrsta trojanskih konja su bankarski trojanski konji koji su prvenstveno oblikovani za napad na bankarske sisteme, ali i berze dionica/akcija koje se oslanjaju na Internet za prijenos podataka. Osnovna funkcija spomenutih trojanskih konja je krađa ličnih podataka žrtve, kao što su brojevi kreditnih kartica i PIN-ovi (*eng. Personal Identification Number*), te preuzimanje potpune ili djelomične kontrole nad računarom korisnika. Trenutno ne postoji efikasna zaštita protiv njih pa se niti jedan korisnik Internet bankarstva ne može osjećati potpuno sigurno. Naravno, postoje određene mjere zaštite, ali niti jedna od njih ne pruža potpunu zaštitu. Trojanski konji se mogu podjeliti u nekoliko porodica. Razlikuju se prema bankarskim institucijama koje napadaju, ,alatima za sažimanje koje koriste i prema ponašanju u sistemu zaraženog korisnika. Najpoznatije dvije porodice koje su značajno prisutne na Internetu su: Limbo/Nethell i ZeuS/Zbot/Wsnpoem[155].

3.10.3. Otimanje autenticiranih sjednica /veza

Trojanski konji, osim što se mogu koristiti za krađu korisničkih i autentikacijskih podataka, mogu se koristiti i za otimanje autenticiranih veza/sjednica. Ukoliko trojanski konj preuzme administratorske podatke, čak ni višeslojni autentifikacijski sistem neće pružiti zaštitu od upotrebe autenticirane sjednice/veze za pokretanje ili izmjenu transakcija. Problem leži u činjenici da web preglednici na osobnim računarima korisnika pristupom Internet bankarstvu postaju bankovni terminali.

---

[154]Vidi CARNet HRVATSKA AKADEMSKA ZAJEDNICA i ISTRAŽIVAČKA MREŽA,Bankarski zločudni programi, NCERT+(www.cert.hr) u suradnji sa LS&S(www.LSS.hr),strana 5.

[155]iseclab.org/papers/impersonation,01.02.2012.23,17.,stage.owasp.org/.../OWASP_Anti-Malware_-_K...01.02.2012.23,23.,

Prilikom izvođenja napada otimanjem sjednica, zloćudni program može promijeniti sadržaj transakcija. Na primjer, neka korisnik unosi nalog za prijenos 100 KM na tekući račun osobe N.N. Ukoliko napadač otme sjednicu, on može promijeniti iznos od 100 KM u 900 KM te umjesto N.N. osobe upisati podatke o svom računu ili računu kojim on upravlja. Osim toga, napadač može unijeti i potpuno novi nalog za prijenos novca. Kada je transakcija provedena, napadač može pokupiti novac. Naravno bilo bi prejednostavno da kriminalci koriste vlastiti identitet za obavljanje opisane pljačke i prikupljanje novca[156].

3.10.4. Preuzimanje kontrole nad podacima u predlošcima (eng. form grabbing)

Prikupljanje podataka potrebnih za upotrebu Internet bankarstva obično obavljaju programi za praćenje unosa znakova sa tipkovnice. To nije efikasno jer takvi programi bilježe sve što korisnik utipka, što znači da napadač mora u gomili podataka pronaći one za njega korisne podatke. Zbog toga su 2003. godine napadači počeli koristiti preuzimanje kontrole nad podacima u prozorima. Spomenuta metoda odnosi se na trojanca koji presreće podatke samo u slučaju kada korisnik popunjava neki predložak koji sadrži polja za ispunjavanje. Kada korisnik popunjava nalog za novčanu transakciju, podatke unosi u za to predviđena polja na predlošku. Podaci koje korisnik unosi obično su osjetljivi (npr. brojevi bankovnih računa i slično).

3.10.5. Pharming

Neki bankarski trojanci preusmjeravaju korisnika prilikom prijave na Internet bankarstvo na lažnu web stranicu. Ova metoda napada naziva se *pharming*. Napadač oblikuje stranicu tako da ona fingira web stranicu banke. Takva stranica također može služiti za napad s čovjekom u sredini, mijenjajući sadržaj prometa koji se prenosi između bankarske stranice i korisnikovog web preglednika. Postoji mnogo različitih tehnika *pharming* napada. Na primjer, trojanski konj može dodati nazive web stranica banke u datoteku s IP adresama koje upućuju na zlonamjernu web stranicu. Mnogi web preglednici imaju opciju upozoravanja korisnika da web stranica koju posjećuju nema valjani certifikat. Bankarski trojanski konj koji izvodi *pharming* napade upotrebom funkcija „wininet.dll“ u pregledniku može zaobići ili potisnuti dijaloške prozore o upozorenjima. Također, trojanski konj koji može mijenjati datoteke na korisničkom računaru, može i instalirati vlastiti certifikat te na taj način spriječiti pojavu upozorenja.

3.10.6. Nedobronamjerni višefazni programi

Postoje programi kojim se izvode napadi na bankovne račune u više faza/koraka. Prvi je korak početna infekcija računara. Maligni se program instalira na korisnikov računar ukoliko on posjeti stranicu koja ga sadrži. Preuzeti program šalje svaki URL (*engl.Uniform Resource Locator*) odnosno adrese web stranica, koje korisnik posjeti, poslužitelju kojim upravlja napadač. U drugoj fazi/koraku zloćudni program prati kriptrirani promet web stranice za Internet bankarstvo. Takav se promet presreće i šalje prema napadače vom poslužitelju. U trećem koraku napadač analizira promet i utvršuje u kojoj banci žrtva ima račun. Zatim šalje žrtvinom računaru drugi program koji presreće pritiske tipki na tastaturi u trenutku kada ona pristupa stranicama za Internet bankarstvo. Na opisani način napadač saznaje informacije o

[156] Vidi CARNet HRVATSKA AKADEMSKA ZAJEDNICA i ISTRAŽIVAČKA MREŽA,Bankarski zločudni programi, NCERT+(www.cert.hr) u suradnji sa LS&S (www.LSS.hr), strana 9 i 10..

žrtvinom bankovnom računu, broju računa, lozinku i slično. Nakon treće faze/koraka napadač ima sve što mu je potrebno za nezakonito korištenje žrtvinog računa. Kao prevencija je veoma bitno spriječiti prvu fazu/korak napadača upotrebom nekog od antivirusnih programa koji sprečavaju preuzimanje malignih programa sa suspektnih stranica[157].

3.10.7. Lažno predstavljanje

U napadima lažnim predstavljanjem uvijek postoje tri glavna učesnika: (1) banka kao davalac usluga (2) žrtva kao korisnik usluga banke (3) napadač. Da bi banka kao davalac usluga osigurala isključivo autorizirani pristup svojim uslugama ona prije dozvole pristupa svojim uslugama obavlja autentifikaciju. Zbog toga ona dodjeljuje korisnicima svojih usluga korisničke račune. Napadač da bi koristio usluge banke mora ukrasti lične podatke i korisnički račun korisnika. On za to koristi kanal (tzv. napadački kanal) prema žrtvi radi preuzimanja podataka i vrši napad na korisnika lažnim predstavljanjem. Postoje više načina za izvođenje napada lažnim predstavljanjem. Tipični premijeri su *phising* i lažno predstavljanje upotrebom za praćenje unosa znakova sa tastature. *Phishing* napadi podrazumijevaju aktivnosti kojima napadač upotrebom lažnih poruka elektroničke pošte i lažnih web stranica banaka pokušava korisnika navesti na otkrivanje njegovih „bankarskih ličnih podataka“. Pri tome mislimo na podatke kao što je broj kreditne kartice, korisničko ime, lozinka, PIN i slično. Riječ *phishing* dolazi od engleske riječi „fishing“ kojom se metaforički opisuje postupak kojim neovlašteni korisnici namamljuju korisnike Interneta kako bi „ svojevoljno“otkrili lične podatke[158].

3.11. Trendovi cyber kriminala i pranja novca u 2012.godini

Na temelju Cisco[159] izvještaja za 2011.godinu i prognoza za 2012.godinu te izvještaja PandaLabs-a[160] za 2011.godinu i predviđanje trendova u 2012.godini daju se identificirati trendovi u okviru kojih će na društvenim mrežama dominirati tehnika napada korisnika preko socijalnog inženjeringa, a kao mamac će se koristiti Olimpijske igre ili predsjednički izbori u SAD, broj *malware* će se idalje povečavati eksponenciojalno jer će ih *cyber* kriminalci intenzivno koristiti u svojim napadima, kao i trojance koji su najčešći izbor *cyber* kriminalaca. Prema prognozama trendi će biti i mobitel *malware* koje bi mogle prerasti u epidemiju sa uklonom prema Android-ima na koje napadi neće biti tako masovni kao u 2011. Posebna meta Trojanaca bi mogao da bude novi sistem mobilnog plaćanja putem NFC metode.Također, mete napada Internet kriminalaca bi trebali biti i male i srednje kompanije zbog toga što ista nisu toliko posvećena sigurnosti podataka sa kojima raspolažu. Pored navedenog za očekivati je da se popularni operatvni sistem u novembru 2012. godine lansirati sljedeću verziju Windowsa 8 koji će biti svojevrsni izazov cyber kriminalcima i stvaranje novog zlonamjernog softvera. S obzirom na navedena predviđanja dalje ekspanzije cyber kriminala logično je da će se potrebe za „mulama“-ljudima koji otvaraju posebne bankovne račune ili koriste vlastite kako bi kriminalcima „oprali“ novac (*money mulling*) značajno rasti.

[157] Vidi više CARNet HRVATSKA AKADEMSKA ZAJEDNICA i ISTRAŽIVAČKA MREŽA,Bankarski zločudni programi, NCERT+(www.cert.hr) u suradnji sa LS&S (www.LSS.hr), strana 12.
[158] Vidi CARNet HRVATSKA AKADEMSKA ZAJEDNICA i ISTRAŽIVAČKA MREŽA, Bankarski zločudni programi, NCERT+ (www.cert.hr) u suradnji sa LS&S (www.LSS.hr), strana 12.
[159] http://www.cisco.com
[160] http://pandalabs.pandasecurity.com

Također cyber kriminalci će pri napadima pored tehnologije i dalje eksploatirati sedam ljudskih slabosti, a to su: seksipl, pohlepa, taština, povjerenje, lijenost, suosjećanje i hitnost.

Prema podacima iz izvještaja cijene za neke od najpopularnijih oblika cyber kriminala su iznenađujuće niske.Npr.podaci o bankovnim računima sa šestocifrenim saldom koštaju od 80 pa do 700 USD. Cijena dizajniranja i postavljanja lažne internet prodavnice je od 30 do 300 USD. Cijena mašine/uređaja za kloniranje kreditnih kartica kreće se od 200 do 1.000 USD,a cijena lažnog bankomata koji krade podatke o platnim karticama korisnika iznosi skromnih 3500 USD. Sve ovo upućuje na veoma intenzivnu kriminalnu aktivnost *cyber* kriminala u tekućoj godini sa ogromnim direktnim i indirektnim štetama.

3.12. Novac mazga (money mule)/pranje novca

Radi ilustracije procesa regrutovanje "novac mazgi"kao jedne od vrsta socijalnog inženjeringa poslužit ćemo se sljedećim primjerom: Inozemna kompanija je poslala e-mail u čijem sadržaju, koji je odaslan nekoliko hiljada e-mail adresa, se mladim i obrazovanim ljudima diljem svijeta nudi sjajan posao (finansijski agent) i brza enormna zarada.

Ako ili kada potencijalne žrtve prihvati e-mail ponudu inozemne kompanije moguće je da se pri obavljanju posla sukobe sa zakonom i postane nešto što je u teoriji i praksi poznato kao "novac mazga"- nesvjesni akteri kriminalne sheme pranja novca.. Kako za sjajan posao i enormnu zaradu nisu potrebna nikakva ulaganje ponuda djeluje vrlo primamljivo, a shema prilično jednostavno:"novac mazga" prima uplatu sa ukradenog računa na svoj bankovni račun i u skladu sa instrukcijom "kompanije" transferiše novac na bankovni račun druge "novac mazge" koristeći vlastiti bankovni račun, pri tome iznosa svakog transfera koji izvrši umanjuje za proviziju. Moguća je i varijacija da: "novac mazga" prima uplatu sa ukradenog računa na svoj bankovni račun, nakon toga "novac mazga" diše gotovinu i šalje preko Western Union servisa na bankovni račun druge ili drugih "novac mazgi" i tako nekoliko desetina puta. U navedene sheme i njihove brojne i složene varijacije mogu se uključiti i "lažne kompanije""on line kladionice","on line aukcije","on line kockarnice", *off shore* banke, lažni uposlenici i sl..

Da bi kriminalci izbjegli otkrivanje od strane vrlo strogih i savremenih mehanizama za sprečavanje pranja novca u banci, "novac mazga" bankovni računi se koriste ograničen broj puta u određenom vremenskom periodu, a tansferi sa i na račun "novac mazgi" su pod njihovom rigoroznom kontrolom i pored činjenice da su unaprijed pažljivo dizajnirani.

Nažalost, postoje brojni načini kojim potencijalnim "novac mazgama" „muljatori" mogu pristupiti. To može biti kućna shema ili e-mail ponuda slična Nigerijskoj prevari, oglasi o zapošljavanju na web stanicama, oglasi o iznajmljivanju nekretnina, instant poruka ili na bilo koji drugi način koji podrazumijeva davanje podatke o svom bankovnom računu.

3.13. Cyber mafija

Ono što je nesporno je da je *cyber* kriminal više vezan za aktivnosti pojedinaca, a kriminal vezan za kompjuterske mreže je dominantno djelo grupa i to organizovanih, profesionalizovanih pa sve češće i strogo specijalizovanih. Ove grupe su, s jedne strane, "tradicionalne" grupe organizovanog kriminala koje su se usavršile i osavremenile primjenom informaciono komunikacione tehnologije i pripremile za "izlazak" na cyber scenu. S druge strane, javljaju se i posebne organizovane cyber grupe odnosno *cyber mafija.*

Cyber mafija ima svoja pravila, drugačiji način ponašanja od konvencionalne mafije, kao što ima i specifično virtualno okruženje, informaciono oružje i specijalizovano znanje i vještine. Internacionalizam, transnacionalnost, multidimanzionalnost samo su neka od karakteristika cyber mafije. Njihova organizaciona struktura nije toliko jednostavna, ustaljena i jednoobrazna kao što je to slučaj sa konvencionalnim oblicima organizovanog kriminala što ih još više čini posebnim i društveno opasnim.

3.14. Mjere prevencije za sprečavanje krivičnog djela pranja novca

Mjere sprečavanja krivičnog djela pranja novca obuhvataju brojne aktivnosti preventivnog karaktera koje poduzimaju obveznici[161] i Finansijsko obavještajna jedinica radi sprečavanja pranja novca i predupređenja brojnih štetnih posljedica ove nedopuštene aktivnosti po pojedinca i društvo i njegove demokratske tečevine. Za potrebe ovog modela u nastavku prezentiramo nacionalne mjere prevencije u kontekstu međunarodnih standarda zasnovanih na Četrdeset preporuka 2003 i Devet Specijalnih preporuka za finansiranje terorizma 2001 Finansijske Akcione radne grupe (FATF), dopunjenih – zbog specifičnog obima evaluacija koje je izvršila Komisija – pitanjima koja su povezana sa Direktivom 2005/60/EC Evropskog Parlamenta i Savjeta od 26. oktobra 2005 o sprečavanju korištenja finansijskog sistema u svrhu pranja novca i finansiranja terorizma (u daljem tekstu "Treća EU Direktiva" i Direktiva 2006/70/EC "implementirajuća Direktiva", čiju su usklađenost ocijenili evaluatori u toku njihove terenske posjete Bosni i Hercegovini u periodu 24. maj do 10. juna. 2009. godine.

3.14.1. Procjena rizika

Rizik pranja novca I finansiranje terorističkih aktivnosti je rizik da će klijent iskoristiti finansijski sistem ili djelatnost obveznika za počinjenje krivičnih djela pranja novca ili finansiranja usluga ili proizvod biti direktno ili indirektno upotrjebljeni za pomenuta krivična djela.

Sadržajem odredaba Zakona o sprečavanju pranja novca pored definisanja pojmova koji se koriste u zakonu, utvrđeni su obveznici provođenja mjera za otkrivanje i sprječavanje pranja novca i finansiranje terorističkih aktivnosti kao i njihove obaveze i zadaci koji se odnose ne procjena rizika klijenta ili grupe klijenata, poslovnog odnosa, transakcije ili proizvoda u vezi sa mogućnošću zloupotrebe u svrhu pranja novca i finansiranja terorističkih aktivnosti (član 5.);

3.14.2. Identifikacija i praćenje klijenta

Identifikacija i praćenje klijenta je fundamentalni dio sistema suprotstavljanja pranju novca. Identifikacijom i praćenjem klijenta stvaraju se uslovi za uspostavljanje sistema protiv pranja novca, mogućnost rekonstrukcije pojedinačnih transakcija i stvaraju se osnovi za dolaženje do informacija o potencijalnim izvršiocima krivičnog djela pranja novca.

Sadržajem odredaba člana 6. do 26. Zakona o sprečavanju pranja novca I finansiranje terorističkih aktivnosti utvrđene su mjere identifikacije i praćenja klijenta za sve obveznike iz člana 4. u slučajevima :

[161] Vidi Zakona o sprečavanju pranja novca i finansiranja teroristićkih aktivnosti, član 4.

- ✓ identifikacije klijenta i praćenja klijenta prilikom uspostavljanja poslovnog odnosa sa klijentom;
- ✓ obavljanja transakcija u iznosu od 30.000 KM ili više bez obzira da li je transakcija obavljena u jednoj operaciji ili u nekoliko evidentno povezanih transakcija;
- ✓ postojanje sumnje u vjerodostojnost i adekvatnost prethodno dobivenih informacija o klijentu ili stvarnom vlasniku.

Izuzetan značaj pri realizaciji mjera za suprotstavljanje pranju novca i utvrđivanju identiteta klijenta ima princip "upoznaj svog klijenta". Primijena ovog principa prevazilazi prostu identifikaciju klijenta i dozvoljava, odnosno zahtijeva da institucija poznaje i razumije svoju stranku i njene poslovne aktivnosti. Banke ovaj princip primjenjuju u prevenciji operativnih I reputacijskih rizika. Pored ostalog, implementacija ovog principa pruža dragocjeno sredstvo za identifikovanje sumnjivih i neobičnih transakcija, čime se stvara osnova za proaktivno djelovanje u suprotstavljanju pranju novca. Četrdeset preporuka Grupe za finansijske akcije uspostavljaju temelje primjene ovog principa u preporukama broj 10.,11. i 12.

Radi posebnosti ovog edukativnog modela valja posebno naglasiti već pomenute odredba člana 21. koja tretira korenspnodenski odnos s kreditnim instirucijama sa sjedištem u inozemstvu i člana 26. koje se odnose na elektronski prenos novca.

3.14.3. Ograničenja/zabrane u poslovanju sa klijentom kao mjera za sprečavanje pranja novca

S ciljem preveniranja pranja novca zakonom su propisana ograničenja kojim se obveznicima nalaže zabranu otvaranje i posjedovanje skrivenih računa, štednih knjižica i drugih proizvoda koji omogućavaju skrivanje identiteta klijenta. Pored navedene zabrane obvezniku se zabranjuje uspostavljanje veza korespondentnog bankarstva sa korespondentnim bankama koje posluju ili mogu poslovati kao banke školjke[162].Također, licima koja nisu stipulirana u odredbama člana 4.zakona,a koja obavljaju djelatnost prodaje roba i usluga, zabranjen prihvaćanje plaćanja u gotovini od kupaca ili trećih lica pri kupovini pojedinačnih dobara i usluga ako prelazi 30.000 KM ili nekoliko povezanih transakcija gotovinom ako njihova vrijednost prelazi 30.000 KM.

3.14.4. Obavještavanje o sumnjivim transakcijama

Obavještavanje o transakcijama čini jedan od temelja suprotstavljanja pranju novca i kao takav je ugrađen u odredbe člana 30. i 31. Zakona. U okviru zakonom uspostavljenog sistema obavještavanja obveznik iz člana 4. je dužan FOO-u (FIU-u) u rokovima utvrđenim sadržajem odredaba člana 31. Zakona dostaviti podatke iz člana 44. stav 1. istog zakona o:

- ✓ svakom pokušaju i obavljenoj transakciji,klijentu ili licu ako postoji sumnja na pranje novca ili finansiranje terorističkih aktivnosti;
- ✓ gotovinska transakcija čija vrijednost iznosi ili prelazi iznos od 30.000 KM;
- ✓ povezanim gotovinskim transakcijama čija je ukupna vrijednost iznosi ili prelazi iznos od 30.000 KM.

[162] Banke školjka u smislu odredaba člana 3.Zakona o sprečavanju pranja novca ži finansiranja terorističkih aktivnosti je strana kreditna ili druga institucija kaoja se bavi istom djelatnošću,kokja je registrirana u državi u kojoj ne obavlja svoju djelatnost i koja nije povezana sa finansijskom grupom koja podliježe nadzoru radi otkrivanja i sprečavanja pranja novca ili finansiranja terorističkih aktivnosti.

Na temelju sadržaja obavještenja o transakcijama identifikuju se sumnjive i neobične aktivnosti pranja novca u različitim oblastima koje daljim oplemenjivanjem i dopunjavanjem doprinose da se:

- ✓ direktno otkriju slučajevi pranja novca na temelju primljenih,obrađenih i analiziranih obavještenja o transakcijama;
- ✓ da posluže kao dodatni izvor informacija u krivičnim i finansijskim istragama;
- ✓ na temelju istih sačine operativne i strateške analize s ciljem identifikovanja trendova i tipologija pranja novca;
- ✓ koriste za definisanje indikatora/pokazatelja[163] pranja novca u različitim oblastima poslovnih aktivnosti.

3.14.5. Obaveze i zadaci lica koja obavljaju profesionalne djelatnosti u provođenju mjera za sprečavanje pranja novca

Odredbama zakona, kao obveznici provođenja mjera sprečavanja pranja novca i finansiranja terorističkih aktivnosti, tretirana i pravna i fizička lica koja obavljaju profesionalne djelatnosti (advokati, advokatska društva, notari, samostalni revizori i revizorska društva, pravna i fizička lica koja obavljaju računovodstvene usluge i usluge poreskog savjetovanja). Za ovu vrstu obveznika su propisani zadaci ,obaveze i utvrđeni izuzetci [164] kao i procedure za identifikaciju i praćenje klijenata pri uspostavljanju poslovnog odnosa i/ili obavljanju transakcije kao i prikupljanje podataka odnosno elemenata za njihovu identifikaciju i praćenje.[165] Također, zakonom je i za ovu vrstu obveznika propisana je obaveza obavještavanja Finansijsko obavještajne jedinice u svim slučajevima kada prilikom obavljanja svojih poslova utvrde da u vezi sa poslovnim odnosom, transakcijom ili određenim licem postoji razumna sumnja da se radi o pranju novca i finansiranje terorističkih aktivnosti, izuzeci od propisane obaveze i obaveza sačinjavanja liste indikatora za prepoznavanje lica i transakcija za koje postoji razumna sumnja u vezi sa pranjem novca i finansiranjem terorističkih aktivnosti.[166] Prilikom razmatranja mjera prevencije valja pomenuti da pravna i fizička lica koja obavljaju profesionalne djelatnosti i njihovi regulatori više pažnje usmjeravaju ka poštivanju zakona koji se odnose na njihovu djelatnost, a veoma malo pažnje posvećuju sistemu sprečavanja pranja novca i finansiranju terorističkih aktivnosti što je jedna od temeljnih slabosti sadašnjeg sistema prevencije u Bosni i Hercegovini.

3.14.6. Uloga Finansijsko obavještajne jedinica u provođenju mjera sprečavanja pranja novca

Finananšijsko obavještajna jedinica je odgovarajućim odredbama[167] u okviru zakona pozicionirana kao državna jedinica za sprečavanje, istraživanje i otkrivanje operacija pranja novca koja je organizacioni dio Državne agencije za istrage i zaštitu sa obavezom da prima, prikuplja, evidentira, analizira istražuje i proslijeđuje tužiocu informacije, podatke i dokumentaciju primljenu u skladu sa zakonom i drugim propisima BiH o sprečavanju pranja

[163]Vidi Zakon o sprečavanju pranja novca i finansiranja terorističkih aktivnosti ,člana 37.
[164]Vidi Zakon o sprečavanju pranja novca i finansiranja terorističkih aktivnosti, člana 39.
[165] Vidi Zakon o sprečavanju pranja novca i finansiranja terorističkih aktivnosti, člana 40
[166] Vidi .Zakon o sprečavanju pranja novca i finansiranje terorističkih aktivnosti,član 41.,42. i 43
[167] Vidi Zakona o sprečavanju pranja novca i finansiranja terorističkih aktivnosti, člana 45.,46.,47.,48.,49.,50.,51., i 52.

novca I finansiranja terorističkih aktivnosti i ostvaruje međunarodnu suradnju na polju sprečavanja pranja novca i finansiranja terorističkih aktivnosti. [168]

U obavljanju zakonima propisanih obaveza Finansijsko obavještajna jedinica može ako sumnja u pranje novca ili finansiranje terorističkih aktivnosti u vezi sa nekom transakcijom ili licem od obveznika u pismenoj zahtijevati informacije navedene u odredbama člana 44. Zakona, informacije o vlasništvu, o bankovnim depozitima tog lica i ostalu relevantnu dokumentaciju. Pored navedenog Finansijsko obavještajna jedinica može izdati nalog za privremenu obustavu transakcije ili transakcija u trajanju od naviše pet radnih dana. Nalog za privremenu obustavu sumnjive transakcije ili transakcija Finansijsko obavještajna jedinica može izdati na zahtjev agencija za sprovođenje zakona bosne I Hercegovine, drugih organa i institucija u Bih navedenih u članu 51. stav 1. Zakona kao i stranih finansijsko obavještajnih jedinica.

I pored toga što međunarodni standardi zahtijevaju operativnu i finansijsku samostalnost Finansijsko obavještajnih jedinica njena pozicija u okviru organizacione strukture i sistema rukovođenja Državne agencije za istrage i zaštitu (SIPA), te odredbe člana 45. i 51. st. 5. Zakona koje dodatno kompromituju primjenu međunarodnih standarda u Bosni i Hercegovini su bez ikakve dileme Finansijsko obavještajnu jedinicu uskratili za operativnu I finansijsku samostalnost i time u značajnoj mjeri oslabili efikasnost i efektivnost ukupnog sistema sprečavanja pranja novca i finansiranja terorizma.

Napomena edukatoru

U okviru uloge Finansijsko obavještajne jedinice u kontekstu uspostavljenih međunarodnih standarda operativne i finansijske samostalnosti prezentirati prijedlog Izmjena i dopuna Zakona o sprečavanju pranja novca i finansiranju terorističkih aktivnosti koji se još uvijek nalazi u parlamentarnoj proceduri i objasniti njegove osnovne intencije.

3.14.7. Međunarodna suradnja

U okviru odredbi zakona kojim se uređuje međunarodna suradnja Finansijsko obavještajne jedinice sa finansijsko obavještajnim jedinicama i međunarodnim organima, organizacijama i institucijama uključenim u sprečavanje pranja novca i finansiranje terorističkih aktivnosti u pogledu prikupljanja i ustupanju podataka, informacija i dokumentacije koja se odnosi na poslovni odnos, transakciju ili transakcije i lica vezane za pranje novca i finansiranje terorizma na njihov zahtjev ili na vlastitu inicijativu u skladu sa zakonom i pod uslovom da je osigurana povjerljivost i predhodna autorizacija za njihovo dalje ustupanje i korištenje.

3.14.8. Kontrola prenosa gotovog novca preko državne granice

Kontrola prenosa gotovog novca preko državne granice je također značajna mjera u suprotstavljanju pranja novca. Naime, dobrim sistemom kontrole prenošenja gotovog novca preko državne granice omogućava se praćenje novčanih tokova i stvara se slika o veličini i pravcima tih tokova. Također, na taj način se otkriva nelegalna priroda ovih tokova ukoliko

[168] Vidi Zakona o Državnoj agenciji za istrage i zaštitu („Službeni glasnik BiH“, broj:27/04, 63/04,35/05 i 49/09), član 11. i 13.

postoje i inicira poduzimanje mjera na otkrivanju i razjašnjavanju konkretne kriminalne djelatnosti. Osnovni cilj poduzimanja kontrole prenosa gotovog novca preko državne granice jeste otkrivanje njihove nelegalne prirode, a ne ograničavanje kretanja novca van teritorije Bosne i Hercegovine. Najčešći način prenosa gotovog novca preko državne granice je krijumčarenje. Krijumčarenjem se prenosi novac iz zemlje u kojoj je stečen na nelegalan način, koje načešće imaju stroge propise po pitanju prijave porijekla novca pri njegovom ulaganju u finansijski system,radi ubacivanja u finansijski sistem zemalja u kojima postoji visok stepen diskrecionih prava ulagača. Sadržajem odgovarajućih odredbi zakona utvrđena je obaveza Uprave za indirektno oprezivanje Bosne i Hercegovine da Finansijskoj obavještajnoj jedinici dostavi podatke o svakom prenosu gotovog novca preko državne granice u vrijednosti od 10.000 KM ili više, najkasnije u roku od tri dana od prenošenja.

3.14.9. Interna kontrola, revizija i nadzor nad radom obveznika u vezi sa provođenjem mjera za sprečavanje pranja novca

Jedna od najznačajnijih komponenti implementacije mjera za sprečavanje pranja novca predstavlja stvaranje sistema provjere sprovođenja mjera od strane finansijskih, nefinansijskih i drugih institucija i djelatnosti. Proces provjere implementacije mjera za sprečavanje pranja novca sastoji se sastoji se od sprovođenja mjera interne kontrole i revizije kao i mjere nadzora kao oblika eksterne kontrole. Ovako definisani sistem provjere omogućava uspostavljanje efikasnog sistema sprečavanja pranja novca. Minimum mjera interne kontole utvrđen je preporukom br. 19 u dokumentu Četrdest preporuka Grupe za finansijske akcije i odnosi se na:

- ✓ razvoj internih politika, procedura i kontrola uključujući postavljanje stručnih službenika na nivo menadžmenta i adekvatne procedure nadzora da bi se osigurali visoki standardi prilikom zapošljavanja radnika,
- ✓ stalni program obuke zaposlenih ,
- ✓ funkciju revizije za testiranje sistema mjera za sprečavanje pranja novca.

Slijedom sadržaja odredaba člana 36. i 37. Zakona, radi ocjene usklađenosti poslovanja obveznika sa odredbama zakona o sprečavanju pranja novca i finansiranja terorističkih aktivnosti, procjene adekvatnosti njegovih politika i procedura, adekvatne obuke ovlaštenih I odgovornih lica u kontekstu prihvaćenih standarda za sprečavanje pranja novca i finansiranje terorizma, svaki obveznik je dužan osigurati redovnu internu kontrolu i reviziju obavljanja poslova sprečavanja pranja novca i finansiranja terorističkih aktivnosti.

Primarni metod nadzora u sprovođenju mjera za sprečavanje pranja novca je inspekcijski nadzor (Porezne uprave, Finansijska policija, Finansijsko obavještajna jedinica i sl). Međutim, mogući su i drugi oblici nadzora kao i mjere eksterne kontrole, i to provođenjem postupka supervizije najčešće od strane regulatora (Agencije za bankarstvo, Komisije za vrijednosne papire/hartije od vrijednosti, Ured za nadzor osiguravajućih društava). Eksterna kontrola mjera za sprovođenje mjera za sprečavanje pranja novca najčešće je samo segment u zakonom definisanom polju djelovanja inspecijskih i regulatornih organa i agencija. Inspekcijski organi u okviru svojih zakonskih definisanih nadležnosti realizuju različite aktivnosti preventivnog i represivnog karaktera, kao što su: utvrđuju nedostatke u sistemu sprečavanja pranja novca, pružaju stručnu pomoć, sagledavaju cjelishodnosti, osnovanosti i potpunosti pojedinih podzakonskih akata u domenu svoje nadležnosti i poduzimaju aktivnosti za otklanjanje uočenih nedostataka. U okviru represivnog djelovanja inspekcijskih organa i agencija u zavisnosti od zakonskih rješenja mjere se kreću od usmenih opomena i upozorenja

za otklanjanje uočenih nedostataka do donošenje rješenja kojim se nalažu radnje za otklanjanje nedostataka do podnošenja prekršajnih prijava i izvještaja o postojanju osnova sunje o počinjenju krivičnog djela pranja novca.

Eksternom kontrolom bez obzira na to u kom se obliku realizuje kontroliše se sprovođenje mjera na realizaciji interne kontrole i revizije i primjena zakonom definisanih procedura protiv pranja novca. Kontrola se najčešće realizuje metodom slučajnog odabira periooda,poslovnih odnosa ili transakcija i učesnika koji obuhvačeni odgovarajućim evidencijama kontrolisanog obveznika.Na fonu,navedenog, provođenje nadzora nad radom obveznika u vezi sa primjenom odredba zakona I drugih zakona kojim se propisuju obaveze provođenja mjera za sprečavanje pranja novca je regulisano odredbama člana 68. do 71. kao i kaznene sankcije kao opšti i posebni oblici prevencije koje se utvrđene odredbama člana 72. i 73. Zakona.

3.14.10. Stručno obrazovanje, osposobljavanje i usavršavanje

Stručno obrazovanje, osposobljavanje i usavršavanje zaposlenih predstavljaju veoma važne segmente sistema za sprečavanje pranja novca .Kontinuirano educiranje tužilaca, pripadnika agencija za sprovođenje zakona ,regulatora i supervizora obavezno treba da obuvata i segment sprečavanja pranja novca. Naime planovi i programi organizovane edukacije bi trebali trebalo bi da uvrste aktualne sadržaje koji u užem i širem smislu tretiraju problematiku suprotstavljanja pojavnim oblicima pranja novca. Također, bilo bi poželjno i angažovanje eksperata iz oblasti suprostavljanja pranja movca i njihovo uključivanje u provces edukacije. Za potrebe stručnog usavršavanja u oblasti suprostavljanja pranju novca koriste se različiti metodi kao što su: kružna pisma, periodični izvještaji, video zapisi, bilteni, brošure, posteri, časopisi, seminari, okrugli stolovi, dijaloške emisije i sl. U novije vrijeme finansijsko obavještajne jedinice i jedinice za finansijske istrage vode web stranice na kojima se javnosti prikazuju podaci vezani za suprostavljanje pranju novca. Nažalost navedeni trendovi iz ove oblasti, iz više razloga, još uvijek nisu postali praksa Finansijsko obavještajne jedinice Bosne i Hercegovine. Jedan od veoma zanimljivih metoda za stručno usavršavanje u oblasti suprotstavljanja pranju novca su interaktivni CD rom-ovi,koje koriste njemačke banke u obuci svog osoblja za primjenu mjera za sprečavanje pranja novca[169]. Ovi CD-ovi sadrže multimedijalne informacije kojima se pristupa preko računara,u ovom slučaju korisnik pred sobom ima virtualnog predavača koji ga vodi kroz program obuke. Potreba stručnog obrazovanja, osposobljavanja i usavršavanja je prepoznata i ugrađena kroz odredbe člana 35 zakona kojim je utvrđena da je za blagovremeno, stručno i kvalitetno provođenje preventivnih mjera za sprečavanje pranja novca neophodno je da svaki obveznik iz zakona osigura kontinuirano stručno obrazovanje,osposobljavanje i usavršavanje zaposlenika koji vezani za poslove sprečavanja pranja novca. U tom smislu je dužan izraditi program godišnjeg stručnog obrazovanja, osposobljavanja i usavršavanja zaposlenih.

Saradnja i koordinacija na unutrašnjem planu u sprovođenju mjera sprečavanja pranja novca

Saradnja i koordinacija na unutrašnjem planu su veoma važni elementi sistema za suprotstavljanje pranju novca. Naime,dobro uspostavljen sistem koordinacije i saradnje omogućava objedinjavanje djelovanja različitih elemenata sistema suprotstavljanja pranju

[169] Reviev of FATF Anti-Many Laundering Systems and mutal Evalution Procedures 1992. do 1999.godina, 2001.,p.24.

novca i poboljšava efikasnost tog sistema. Saradnju i koordinaciju neophodno je uspostaviti na nekoliko nivoa i to između:

- ✓ različitih nadležnih državnih i nedržavnih organa, agencija i institucija na operativnom nivou,
- ✓ nadležnih državnih organa i finansijskih, nefinansijskih institucija i profesionalnih djelatnosti kao i njihovih profesionalnih udruženja,
- ✓ svih subjekata u oblasti suprotstavljanju pranja novca na strateškom nivou.

Saradnja i koordinacija na operativnom nivou podrazumijeva objedinjavanje djelovanja različitih nadležnih organa u istragama pranja novca. Ovakav pristup u istragama omogućava stvaranje kompletne slike pojedinih shema pranja novca, kvalitetno prikupljanje relevantnih podataka, informacija i dokumentacije iz različitih izvora i značajno doprinosi efikasnosti, efektivnosti i potpunosti finansijske istrage.

Koordinacija i saradnja između nadležnih državnih organa i finansijskih i nefinansijskih institucija i profesionalnih djelatnosti omogućava ostvarivanje povratne informacije u odnosu na primjenu mjera za suprotstavljanje pranju novca. Povratne informacije doprinose blagovremenoj adaptaciji mjera suprostavljanja pranju novca i njihovim tendencijama u ovim institucijama i djelatnostima.

Saradnja i koordinacija na stratečkom nivou podrazumjeva izradu strteškog plana u kome bi bili predstavljeni opšti i posebni ciljevi kao i plan aktivnosti za ostvarenje tih ciljeva za uspostavljanje i razvoj efikasnog sistema protiv pranja novca.

Kvalitetan sistem koordinacije i saradnje na svim nivoima omogućava stvaranje kompaktnog i cjelovitog odgovora na aktualne izazove u oblasti suprotstavljanja pranju novca i drugim oblicima kriminalnih aktivnosti. Značaj međuinstitucionalne saradnje je skromno i vrlo reducirano artikuliran kroz odredbe članova 51. i 52. Zakona.

3.15 Krivično djelo pranja novca u međunarodnom pravu

Kao dio cjelovite strategije suprotstavljanja pranju novca na međunarodnom nivou, međunarodna zajednica se opredijelila za normiranju ove pošasti novog vremena, radi iznalaženja najkorisnijih metoda, mjera i sredstava za suprotstavljanju pranju novca. U tom smislu donijeto je nekoliko međunarodnih pravnih akata koji predstavljaju osnovu za suprotstavljanje pranju novca u međunarodnim okvirima, kako slijedi:

1. Konvencija Ujedinjenih nacija protiv nedozvoljenog prometa opojnih droga I psihotropnih supstanci (Beč 1988.godine);
2. Konvencija Savjeta Europe o pranju,traganju,privremenom oduzimanju I oduzimanju prihoda stečenih krivičnim djelom (Strazbur 1990.godine);
3. Direktiva Savjeta Europe za sprečavanje korištenja finansijskog sistema u svrhe pranja novca (Luksemburg 1991.godine);
4. Konvencija Ujedinjenih nacija o borbi protiv transnacionalnog organizovanog kriminaliteta (Palermo 2000.godine);
5. Konvencija Savjeta Europe o pranju, traženju, zaplijeni i oduzimanju prihoda stečenih kriminalom i o finansiranju terorizma (Varšava 2005.godine);
6. Direktiva 2005/60/EZ o sprječavanju korištenja financijskog sistema u svrhu pranja novca i financiranja terorizma.

Sadržajem odredbi navedenih međunarodnih propisima obavezuju se države potpisnice da u nacionalnim zakonodavstvu kao krivično djelo uvedu slijedeća djela, ako su učinjena sa umišljajem [170]:

- ✓ Konverzija ili prijenos imovine za koju se zna da predstavlja nezakonit prihod ,sa svrhom prikrivanja ili maskiranja nezakonitog porijekla takve imovine ili pomaganja bilo kojoj osobi uključenoj u izvršenje glavnog krivičnog djela da izbjegne zakonske posljedice ovog djela;
- ✓ Prikrivanje ili maskiranje prave prirode, porijekla, mjesta, raspolaganja, premještanja te postojanja prava ,odnosno vlasništva na imovinu za koju se zna da predstavlja nezakonit prihod,u skladu sa svojim ustavnim načelima i osnovnim konceptima svog pravnog sistema;
- ✓ Stjecanje, posjedovanje ili upotreba imovine za koju se zna da je u vrijeme primanja, da je predstavljala nezakonit prihod;
- ✓ Sudjelovanje u izvršenju,uzdržavanje ili zavjera radi izvršenja, pokušaja izvršenja I pomaganje,poticanje,olakšavanje I davanje savjeta u izvršenju bilo kojeg od djela navedenih u prethodnim alinejama.

3.16. Kriminalizacija pranja novca u BIH

U Krivičnom zakonu BiH pranje novca je kriminalizovano sadržajem odredaba člana 209. Krivičnog zakona BiH koji glasi:

Pranje novca
Član 209.

(1) Ko novac ili imovinu za koju zna da su pribavljeni učinjenjem krivičnog djela primi, zamijeni, drži, njima raspolaže, upotrijebi u privrednom ili drugom poslovanju, ili na drugi način prikrije ili pokuša prikriti, a takav je novac ili imovina veće vrijednosti ili to djelo ugrožava zajednički ekonomski prostor Bosne i Hercegovine ili ima štetne posljedice za djelatnosti ili finansiranje institucija Bosne i Hercegovine,

kaznit će se kaznom zatvora od šest mjeseci do pet godina.

[170] Član 3.Konvencije Ujedinjenih nacija protiv nedozvoljenog prometa opojnih droga I psihotropnih supstanci (Beč 1988.godine); član 6. Konvencikje Savjeta Europe o pranju, traganju, privremenom oduzimanju i oduzimanju prihoda stečenih krivičnim djelom (Strazbur 1990.godine);član 6 Konvencija Ujedinjenih nacija o borbi protiv transnacionalnog organizovanog kriminaliteta (Palermo 2000.godine).

(2) Ako vrijednost novca ili imovinske koristi iz stava 1. ovog člana prelazi iznos od 50.000 KM,učinitelj će se kazniti kaznom zatvora od jedne do deset godina.

(3) Ako je pri učinjenju krivičnog djela iz stava 1. i 2. ovog člana učinitelj postupio nehatno u odnosu na okolnost da su novac ili imovinska korist pribavljeni krivičnim djelom, kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.

(4) Novac i imovinska korist iz stava 1. do 3. ovog člana će se oduzeti.

Krivični zakoni dva entiteta BiH I Brčko Distrikta Bosne I Hercegovine sadrže sasvim slična krivična djela što se tiče kriminalizacije pranja novca. Ova krivična djela se mogu naći u članu 272. Krivičnog zakona FBiH[171], članu 280. Krivičnog zakona RS[172] i članu 265. Krivičnog zakona Brčko Distrikta[173].

Komisija eksperata za evaluaciju mjera protiv pranja novca i finansiranja terorizma (MONEYVAL) je u Nacrtu izvještaja o trećem krugu detaljne procjene za Bosnu I Hercegovinu kao najozbiljniji nedostatak režima borbe protiv pranja novca identificirala slijedeće .

1. Nijedan o četiri definicije krivičnog djela pranja novca sadržana u sva četiri krivična zakona (KZ BIH, KZ F BiH, KZ RS I KZ BD BiH),u pogledu materijalnih elemenata nije u potpunosti usklađena sa članom 3. Bečke Konvencije i članom 6. Konvencije iz Palerma;

2. Krivičnom legislativom, legislativom koja uređuje vrijednosne papire niti ostalom legislativom Brčko Distrikta BiH nije kriminalizirao tržišnu manipulaciju i na taj način propustio da obuhvati predikatnih krivičnih djela za pranje novca sadrže sve potrebne kategorije krivičnih djela u svim relevantnim oblicima.

3. Opseg krivičnih djela pranja novca nije u potpunosti razdvojem, djelimično zbog neusklađenosti vrijednosnih pragova u krivičnim djelima na državnom i nedružavnom nivou i isuviše nejasnih uslova iz člana 209. st. 1. Krivičnog zakona BiH;

4. Generalna percepcija pranja novca na svim nivoima nadležnosti u Bosni I Hercegovini , ne ide izvan pranja dobiti od evazije poreza. Jedva da je i jedna pravosnažna sudska presuda za pranje novca povezana sa nekim drugim predikatnim djelom osim poreskog kriminala (posebno organizovanog kriminala, finansijski kriminal, ,korupcija, intelektualno vlasništvo itd.).[174] Rezulat toga je da dobit od organizovanog i ostalih oblika kriminala ostaje neotkrivena;

5. Značajan nedostatak na državnim sudovima i u tužilaštvima zbog obimne radne norme, manjka osoblja, nedostatka specifične ekspertize kao i problemi dokazivanja u procesuiranju;

6. Iako takav slučaj u zakonu postoji na državnom nivou, još uvijek postoji nesigurnost među stručnjacima da li se namjerni element pranja novca može zaključiti iz objektivnih činjeničnih okolnosti, što može kompromitovati efikasnost sistema spriječavanja pranja novca.

[171] Vidi "Službene novine FBiH" broj: 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11,
[172] Vidi "Službeni glasnik RS" br. 49/03, 108/04, 37/06, 70/06, 73/10,
[173] Vidi Službeni glasnik Brčko Distrikta BiH" br. 10/03, 48/04, 06/05, 12/07, 14/07, 21/07)
[174] U toku izrade Edukativnog modela"Cyber crime,pranje novca i finansijske istrage"ostvaren je neposredni uvid u presude Suda Bosne i Hercegovine kako je navedeno u dopunskoj literaturii modela.

7. Usprkos adekvatnom zakonskom okviru ‚procesuiranje rijetko ima‚za metu pravna lica (*shell* preduzeća, itd) umješane u slučajeve pranja novca.

Napomena edukatorima:

- ✓ ***U okviru prezentacije Edukativnog modela sa kandidatima iz reda tužilaca I agencija za sprovođenje zakona kroz formirane grupe argumentima za I protiv elaborirati svaki od takstativno navedenih nedostataka,***
- ✓ ***Posebno pažnju usmjeriti na argumentaciju koja se tiće generalne percepcije pranja novca na svim nivoima političko-teritorijalnog organizovanja.***
- ✓ Argumentirano raspraviti da li se i u kojoj mjeri namjerni element pranja novca mogu zaključiti iz objektivnih činjeničnih okolnosti.

3.17. Kriminalističke mjere i metodi otkrivanju, razjašnjavanju i dokazivanju krivičnog djela pranja novca

Efikasan i efektivan sistem metoda i mjera u suprotstavljanju pranju novca kao jednom od savremenih oblika kriminala minimiziraju se mogućnosti kriminalcima i organizovanim kriminalnim grupama da zadrže kriminalom stečenu imovinu i urušava njihovu ekonomsku moć kao motiv njihovih budućih kriminalnih aktivnosti. Stoga u nastavku edukativnog modela dajemo kratak pregled metoda i mjera koje se primjenjuju u postupku otkrivanja, razjašnjavanja i dokazivanja krivičnog djela pranja novca.

3.17.1. Otkrivanje krivičnog djela pranja novca

Otkrivanje krivičnog djela pranja novca u direktnoj je funkciji sa posebnostima ovog krivičnog djela koje u potpunosti određuje i mogućnosti za njegovu blagovremenu, efikasnu i kvalitetnu detekciju. Pri tome pod posebnosti krivičnog djela pranja novca podrazumijevamo:

1. sticanje, posjedovanje, korištenje, skrivanje, pretvaranje nelegalno stečenom imovinom direktna je posljedica prethodnih/predikatnih kriminalnih aktivnosti;
2. da bi što više maskirale veze i prikrio trag između nezakonito stečene imovine i predikatnog krivičnog djela i njegovog počinioca odnosno stvarnog vlasnika nezakonito stečene imovine kriminalci pristupaju procesu pranja novca koristeći se brojnim ‚a u posljednje vrijeme pažljivo visokoprofesionalno osmišljenih i vrlo sofisticiranim shemama za pranje novca;
3. Temelj svih manje i više složenih shema pranja novca čine tri uobičajene faze pranja novca(polaganje, prikrivanje i integracija);

U svakoj fazi postupka tužilac i pripadnici agencija za sprovođenje zakona trebaju voditi računa o navedenim posebnostima krivičnog djela pranja novca.

3.17.2. Kako se dolazio do saznanja da je izvršeno krivično djelo pranja novca

Do saznanja da je izvršeno krivično djelo pranja novca najčešće se dolazi na tri načina.

Prvi, operativnom djelatnošću Finansijsko obavještajne jedinic koja svakodnevno prikuplja, evidentira, analizira, istražuje i proslijeđuje Tužiocu informacije, podatke i dokumentaciju primljenu u sa Zakonima i drugim propisima BIH o sprječavanju pranja novca i finansiranja terorističkih aktivnosti. Također, preko Finansijsko obavještajna jedinica se može doći do saznanja i kroz međunarodnu suradnju i istrage pranja novca I finansiranja terorističkih aktivnosti koje Finansijsko obavještajna jedinica ostvaruje.

Drugo, Finansijskom istragom osumnjičenog kao posredni izvor saznanja da je izvršeno krivično djelo pranja novca;

Treće, kriminalističko obavještajnom i kriminalističko istražnom operativnom djelatnošću agencija za sprovođenje zakona.

Četvrto, na temelju informacija iz otvorenih izvora(televizije, radija, web portala, web stranica, štampanih medija, sapštenja pres službi, fotografija, informacija, izvještaja, istraživanja, rezultata provednih anketa, diskusija, brošura) te prijava pravnih lica i građana (anonimne i pseudonimne) i sl.

Najčešće se do saznanja da je počinjeno krivično djelo se dolazi kroz primjenu odredaba Zakona o sprečavanju pranja novca i finansiranja terorističkih aktivnosti. U postupku primjene odredaba ovog zakona obveznici iz člana 4. Zakona, su dužni Finansijskoj obavještajnoj jedinici prijaviti i dostaviti podatke iz člana 44. Zakona o:

- ✓ Svakom pokušaju i obavljenoj transakciji, klijentu ili licu ako postoji sunja na pranje novca ili finansiranje terorističkih aktivnosti;
- ✓ Gotovinsku transakciju čija vrijednost iznosi ili prelazi sumu od 30.000,00 KM;
- ✓ Povezanim gotovinskim transakcijama čija ukupna vrijednost iznosi ili prelazi sumu od 30.000,00 KM.

U okviru navedenih obaveza i aktivnosti ne treba zaboraviti ulogu finansijskih regulatora i supervizora čija je uloga veoma bitna za funkcionisanje cjelokupnog sistema sprečavanja pranja novca i finansiranja terorističkih aktivnosti u Bosni I Hercegovini.

Ne rijetka, ali veoma značajana je primjena odgovarajućih kriminalističko-taktičkih mjera i radnji (prikupljanje obavještenja, opservacija, provjera alibija, prikupljanje izjava, kriminalistička kontrola, lišavanje slobode i zadržavanje, kriminalistička obrada itd.) i operativno-taktičkih metoda i sredstava pri neposrednom otkrivanju krivičnog djela pranja novca. Za uspješno otkrivanje ovog krivičnog djela potrebno je stalno praćenje identifikovanih načina njegovog izvršenja i seriozna analiza svih otkrivenih krivičnih djela pranja novca. Ovakvim načinom rada stvara se indicijalna osnova za uočavanje pojedinih načina/tipologija pranja novca koja omogućava blagovremeno i kvalitetno planiranje aktivnosti na razjašnjavanju i dokazivanju ovog krivičnog djela.

Slučajevi kada se kao izvor saznanja za izvršeno krivično djelo pranja novca pojavljuju otvoreni izvori (televizijske informacije ,informacije sa radija, web portala, web stranica, štampanih medija, saopštenja pres službi, fotografija, informacija ,izvještaja, istraživanja,

rezultata provednih anketa, diskusija, brošura) te prijava pravnih lica i građana (anonimne i pseudonimne) i sl. su vrlo često dragocjeni. U svim pobrojanim i nepobrojanim slučajevima potrebno je primjenom operativno-taktičkih i tehničkih mjera i radnji svaki slučaj pažljivo provjeriti.

3.17.3. Razjašnjavanje i dokazivanje krivičnog djela pranja novca

Razjašnjene i dokazivanje krivičnog djela krivičnog djela pranja novca predstavlja veoma značajan segment suzbijanja pranja novca. U ovoj fazi se razjašnjavaju, utvrđuju i dokazuju svi bitni elementi krivičnog djela pranja n ovca,što predstavlja neophodan uslov za dalje uspješno vođenje krivičnog postupka. Radi toga u ovoj fazi operativnu djelatnost treba planirati i usmjeriti tako da omogući prikupljanje činjenica, podataka i okolnosti na osnovu kojih će se razjasniti slijedeća pitanja:

1. Da li je novac i/ili druga imovina pribavljena krivičnim djelom?
2. Vrsta krivičnog djela kojim je pribavljena imovina koja je predmet pranja novca;
3. Da li je riječ o novca ili nekoj drugoj imovini?
4. Kolika je vrijednost imovine pribavljene krivičnim djelom?
5. Da li je počinitelju ta činjenica bila poznata?
6. Mjesto,vrijeme i način pranja novca;
7. Da li počinitelj imao pomagače?
8. Da li su se počinitelj i saučesnik udružili radi vršenja krivičnog djela?
9. Da li je riječ o počinitelju koji je izvršio ili bio saučesnik u izvršenju krivičnog djela kojim je pribavljena imovina i koji nakon počinjenja krivičnog djela vrši pranje novca ili počinitelju koji samo vrši pranje novca, a drugo lice je počinitelj krivičnog djela kojim je pribavljena imovina?
10. Da li je počinitelj lice koje se specijaliziralo za krivična djela pranja novca?
11. Koja i kakva kriminalna djelatnost i prošlost počinitelja?
12. Da li pranje novca vrši za neku organizovanu kriminalnu grupu?
13. Koja je to organizovana grupa,od kada djeluje i na kom teritoriju?
14. Kakva je organizacije, hijerarhija, sastav, vrsta, obim i intenzitet djelovanja organizovane kriminalne grupe kojoj počinitelj pripada?
15. Da li organizovana kriminalna grupa održava veze sa pripadnicima institucija vlast (sudska, zakonodavna i izvršna) i medija ?
16. Koje su to institucije i mediji i pojedinci u njima?
17. Da li počinitelj pri izvršenju krivičnog djela postupao s umišljajem ili iz nehata?
18. Kakav je finansijska pozicija počinitelja krivičnog djela pranja novca?

Za sve odgovore na navedena orijentaciona pitanja neophodno je osigurati vjerodostojne materijalne i lične dokaze. Od materijalnih dokaza poželjno je osigurati dokumentaciju koja omogućava praćenje traga novca svih potencijalnih osumnjičenih za krivično djelo pranja novca. Na temelju dokumentacije moguće je vršiti rekonstrukciju poslovnih događaja u bliskoj prošlosti. Posebnu pažnju treba posvetiti obradi svake informacije koja ima dokazujuću vrijednost ,a koja može biti prikupljena, uskladištena ili prenesena u digitalnom obliku.

Dokumentacija i evidencija prikupljena iz navedenih izvora može da sadrži dokazne i indicijalne činjenice koje imaju izuzetan značaj za usmjeravanje operativne obrade i dokazivanje krivičnog djela pranja novca. Stoga se u okviru plana operativne djelatnosti planiraju I mjere za pronalaženje navedene dokumentacije. Te mjere se odnose na primjenu

operativno-taktičkih mjera i radnji pregleda i uvida u dokumentaciju, i na primjenu radnji dokazivanja kao što su pretresanje i privremeno oduzimanje. Oduzeta dokumentacija podliježe adekvatnom vještačenju, čime se stvaraju mogućnosti za obezbjeđenje materijalnih dokaza u odnosu na krivično djelo i učinioca.[175]

Ako postoji razumna sumnja da je počinitelj prao novac kroz neki "biznis" (galerije, mjenjačnice, zlatare, trgovine stilskim namještajem, trgovine nakitom od plemenitih meta, turističke agencije, osiguranja, taksi službe, fitnes klubovi i sl) neophodno je izvršiti uvid u knjigovodstvene isprave, poslovne knjige i finansijske izvještaje tog ili tih pravnih lica s ciljem utvrđivanja činjenice da li je u poslovanju tog ili tih pravnih lica u tretiranom periodu bilo miješanja nelegalnih i legalnih sredstava. U okviru tih operativnih aktivnosti neophodno je izvršiti horizontalnu i vertikalnu analizu finansijskih izvještaja do i od počinjenja krivičnog djela pranja novca i utvrditi kada,kako i koliko je nelegalnih sredstava ubačeno u pravna lica i kako se to reflektiralo na finansijsko stanje pravnog lica i kategorije koje se iskazuju u finansijskim izvještajima. Posebnu pažnju je neophodno obratiti na kupce i dobavljače te izvršiti komparaciju količina i jedinične cijene roba i usluga iskazanih u ulaznim i izlaznim fakturama i analizu novčanog toka.

U okviru ovih aktivnosti neophodno je da istražitelji posebnu pažnju posvete licima kojima su poznate ili bi mogle biti poznate neke od činjenica vezane za počinitelja i konkretno krivično djelo. Sa takvim licima je uputno obaviti razgovor kako bi se blagovremeno osigurati kvalitetni izvori ličnih dokaza i stvorile pretpostavke da se ta lica saslušaju kao svjedoci u krivičnom postupku.

Kao nužan uslov za uspješno okončanje kriminalističke obrade odnosno otkrivanje počinitelja i dokazivanje njegove kriminalne djelatnosti jeste saradnja svih nadležnih organa, timski rad, stručnost, znanje iskustvo i poštivanje principa zakonitosti tokom predkrivičnog i krivičnog postupka[176].

3.18. Pranje novca I finansijske istrage

Cilj mjera za sprečavanje i otkrivanje pranja novca, koje u interakciji provode obveznici, regulatori i finansijsko obavještajne jedinice, jeste praćenje i analiza poslovnih odnosa odnosno finansijskih transakcija i otkrivanje shema pranja novca. Na temelju obavještenja o sumnjivoj transakciji vrši se otkrivanje,razjašnjavanje i dokazivanje krivičnog djela pranja novca. Na drugoj strain, cilj finansijske istrage je identifikacija, traganje, privremeno oduzimanje i trajno oduzimanje prihoda u gotovo isto vrijeme kada se vodi krivična istraga krivičnog djela koje je za posljedicu imalo imovinsku korist. U brojnim slučajevima obavještenje o sumnjivoj transakciji dovelo je i do finansijske istrage, a i obrnuto, jer su u bliskoj prošlosti zabilježeni praktični primjeri da se preko finansijske istrage došlo do osnova sunje o počinjenju krivičnog djela pranja novca. Stoga u nastavku edukativnoga modela u kontekstu *cyber* kriminala i pranja novca uz pomoć i podršku *cyber* bankarstva i *cyber* plaćanja u svjretli međunarodnih stsandarda i nacionalnog zakonodavstva tretirat ćemo finansijske istrage kao jedan od najmočinijih alata za identifikaciju, traganje, privremeno oduzimanje i oduzimanje prihoda stečenih krivičnim djelom.

[175] Vidi Goran Boošković,Pranje novca,BeoCing,Beograd,2005.str.142
[176] Vidi Goran Boošković, Pranje novca, BeoCing, Beograd, 2005.str.143.

4. FINANSIJSKA ISTRAGA

Upotreba informaciono-komunikacijskih tehnologija i korištenje usluga eksperata iz različitih oblasti (informatičara, računovođa, revizora, poreskih i investicijskih savjetnika, bankara, pravnika, i dr.) u nezakonitim aktivnostima, doprinijeli su da kriminal, a posebno organizirani, danas postane izuzetno sofisticiran, te da umnogome suzi mogućnosti otkrivanja njegovih aktivnosti. Potreba adekvatnog suprotstavljanja različitim kriminalnim aktivnostima organizovanih kriminalnih grupa sve više upućuje na korištenje savremenih dostignuća nauke u praktičnom djelovanju državnih organa nadležnih za suzbijanje ove vrste kriminala. Jedna od efikasnijih metoda svakako je finansijska istraga, koja omogućava otkrivanje finansijskih aktivnosti organizovanog kriminala, lociranje nezakonito stečenih sredstava i stvaranje osnova za pokretanje postupka oduzimanja nezakonito stečenih sredstava. Efikasnim finansijskim istragama i sistemom mjera oduzimanja nelegalno stečene imovine, podriva se ekonomska moć kriminalnih organizacija i onemogućava se infiltracija nelegalno stečene imovine u finansijski sistem i sprječava kontrolisanje političkih i ekonomskih tokova.

Savremeni koncept borbe protiv imovinski motivisanog kriminala, posebno organizovanog kriminala, upućuje na potrebu kontinuiranog usavršavanja postojećih i uvođenje novih istražnih metoda u kriminalističkom radu. On podrazumijeva i stalno praćenje novih naučnih i tehničkih dostignuća i njihovo inkorporiranje u postojeće procedure i metode, s akcentom na primjeni metoda finansijskih istraga kada je riječ o suprotstavljanju organizovanom kriminalu koji je sve više prisutan u globalnom *cyber okruženju.*

Finansijske istrage su postale jedan od najznačajnijih alata agencija za sprovođenje zakona i tužilaštva za efikasno suprotstavljanja imovinski motivisanom kriminalu, posebno organizovanom, s obzirom na činjenicu da omogućavaju praćenje i lociranje „tragova“ nezakonito stečenog novca. Međutim, pri tome treba imati na umu da finansijske istrage zahtijevaju posebna znanja i vještine da bi se njima prikupili podaci potrebni za identifikaciju, osiguranje, dokazivanje i oduzimanje imovinske koristi pribavljene krivičnim djelom.

Izvorno, neke od metoda finansijske istrage preuzete su iz postupaka poreskih službi koji se poduzimaju s ciljem utvrđivanja neprijavljenih prihoda i izbjegavanja plaćanja poreza, da bi kao takve bile prilagođene potrebama borbe protiv organizovanog kriminala. Historijski posmatrano, najpoznatije primjere daju američki sudovi. Do šire primjene metoda finansijske istrage u borbi protiv organizovanog kriminala u SAD-u dolazi sa donošenjem Zakona o organizacijama koje se bave reketom i korumpiranjem (*Racketeer Influenced and Corruption Organization Act* – RICO) iz 1970. godine, kojim su ove metode prihvaćene kao važno sredstvo za borbu protiv organizovanog kriminala, prije svega u dokazivanju nezakonitih prihoda .

4.1. Pojam i cilj finansijske istrage

Finansijska istraga predstavlja skup kriminalističko istražnih aktivnosti,vještina i tehnika koje se u pravilu provode sinhronizovano sa krivičnom istragom imaju za cilj da otkriju prihod stečen krivičnim djelom, utvrdi imovinu koja se može oduzeti i privremeno osigurati (privremeno oduzeti) imovina kako bi se omogućilo kasnije konačno oduzimanje. Uspješnim otkrivanjem i privremenim oduzimanjem imovine sprječava se njeno prikrivanje i raspolaganje i omogućava efikasno konačno oduzimanje na kraju krivičnog postupka.

4.2. Međunarodni akti kojim su uspostavljena načela i standardi za vođenje finansijskih istraga i oduzimanje, odnosno konfiskaciju imovine stečene kriminalom.

Brojni su međunarodni akti koji se odnose na problematiku oduzimanja, odnosno konfiskaciju imovine stečene kriminalom.

4.2.1. Konvencije UN protiv nezakonitog prometa opojnih droga i psihotropnih supstanci

Može se reći da je razvoj nove koncepcije u ovoj oblasti na međunarodnom planu započeo donošenjem Konvencije *UN protiv nezakonitog prometa opojnih droga i psihotropnih supstanci (UN Convention Against Illicit Traffic Narcotic Drugs and Psyhotropic substances, Viena,19.12.1988).* Svrha ove konvencije je unaprijeđenje saradnje među stranama potpisnicama kako bi se mogle efikasnije boriti protiv brojnih aspekata nezakonitog prometa opojnim drogama i psihotropnim supstancama koji imaju međunarodnu dimenziju. Odredbama Konvencije je uvedena obaveza državama potpisnicama da usvoje mjere kojim bi se omogućila pljenidba dobiti koja potiče od krivičnih djela vezanih za droge ili imovine čija vrijednost odgovara vrijednosti takve dobiti kao i mjere koje će nadležnim organima omogućiti identifikaciju, otkrivanje, zamrzavanje ili privremeno dobiti, imovine i sredstava u svrhu konačnog oduzimanja uključujući pristup bankarskim, finansijskim i komercijalnim evidencijama. Konvencijom su također, utvrđena i pravila međunarodne suradnje uključujući priznavanje i izvršenje naloga za oduzimanje. Odredbe Bečke konvencije sugerišu državama potpisnicima konvencije da razmotre obrat u teretu dokazivanja u vezi sa legitimnošću dobiti ili drugog vlasništva koje podliježe pljenidbi,u mjeri u kojoj je takva radnja u skladu sa principima njihovih zakona te s prirodom sudskih i drugih postupaka.

4.2.2. Konvencija o pranju novca, istragama, zaplijeni i konfiskaciji dobiti od kriminala

Nakon Bečke konvencije su doneseni i drugi propisi, od kojih se posebno izdvajaju *Konvencija o pranju novca, istragama, zaplijeni i konfiskaciji dobiti od kriminala (Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, Strasbourg, 1990).* Ova konvencija je potpisana od strane Bosne i Hercegovine 30.03.2004. godine kada je i ratifikovana, stupila je na snagu 01.07.2004. godine. Cilj ove konvencije je olakšati međunarodnu suradnju i uzajamnu pomoć u istraživanju krivičnih djela te pronalaženju, privremenom oduzimanju i oduzimanju dobiti stečene krivičnim djelom te pomoći državama potpisnicama u postizanju sličnog stepena efikasnosti čak i u odsutnosti potpune zakonodavne usklađenosti. Države potpisnice (stranke) Konvencije, posebno su se obavezale kažnjavati pranje dobiti stečene krivičnim djelom, oduzimati izvršenja i dobit i/ili imovinsku vrijednosti koja odgovara takvoj dobiti), zbog čega državna tijela moraju poduzeti sve potrebne mjere radi oduzimanja posebnih dijelova imovine koji predstavljkaju imovinsku korist ostvarenu krivičnim djelom ili sredstva kojim je krivično djelo počinjeno, kao i oduzimanje imovinske koristi koja se sastoji u zahtjevu za vračanjem novčanog ekvivalenta te koristi. Pristupajući Konvenciji Bosna I Hercegovina je ispunila obaveze da u svom krivičnom zakonodavstvu inkriminira pranje novca.

Konvencija posebno naglašava da se prekogranične organizirane kriminalne aktivnosti zahtijevaju međunarodnu suradnju na svim razinama I utvrđuje načela,standarde, oblike, pravila međunarodne krivičnopravne pomoći kao restriktivne osnove I eventualne razloge za eventualno odbijanje I odgodu suradnje za pružanje pravne pomoći.

4.2.3. Krivičnopravna konvencija o korupciji (Criminal Law Convention on Corruption, Strasbourg 1999),

Sadržajem odredaba ove Konvencije su obavezane države potpisnice da usvoje zakonodavne i druge potrebne mjere koje će im omogučiti izvršavanje konfiskacije ili na drugi način oduzimanje sredstava i koristi stečenih činjenjem krivičnih djela ustanovljenih Konvencijom ili imovine u vrijednosti koja odgovara stečenoj korist (član 19. st. 3.).Također državne potpisnice su se obavezale da usvoje zakonodavne i druge potrebne mjere, uključujući i one koje dozvoljavaju upotrebu posebnih istražnih radnji, u skladu sa domaćim pravom, da omoguće skupljanje dokaza vezanih za krivična djela predviđena članovima 2. do 14. Konvencije i da identificiraju, uđu u trag, fiksiraju i oduzmu instrumente i korist pribavljenu korupcijom, ili imovine u vrijednosti te koristi. Uključujući pri tome pristup bankovnim evidencija I njihovo oduzimanje. Konvencija, također, preporučuje državama potpisnicama da bankarska tajna ne bude prepreka realizaciji navedenih mjera.

4.2.4. Međunarodna konvencija o suzbijanju finansiranja terorizma (International Convention for the Suppression of the Financing of Terrorism, New York 1999),

Sadržajem odredaba člana 8. Konvencije sve države potpisnice se obavezuju da poduzmu odgovarajuće mjere u skladu sa nacionalnim zakonskim principima, s ciljem da identifikuju, otkriju,zamrznu ili zaplijene eventualna sredstva koja se koriste ili su određena u svrhu činjenja krivičnih djela iz člana 2. Konvencije kao i sredstva stečena činjenjem takvih krivičnih djela. Također,odredbama Konvencije se sugeriše da razmotre zaključivanje sporazuma o podjeli sa drugim državama potpisnicama, redovno ili od slučaja do slučaja, sredstva stečena zaplijenom kao i uspostavljanje mehanizama kojim će se sredstva stečena zapljenom koristiti za obeštećenje žrtava krivičnih djela pomenutih u članu 2. st. 2. t. (a) i (b) ili njihovih porodica.

Međutim odredbama član 12. st. 2. Konvencija je značajno umanjila efikasnost I efektivnost međusobne pravne pomoći država potpisnica, dajući im mogućnost da mogu odbiti zahtijeva međusobnu pravnu pomoć po osnovu bankarske tajne.

4.2.5. Konvencija UN protiv transnacionalnog organizovanog kriminala (UN Convention Against Transnational Organized Crime, Palermo 2000),

Sadržajem odredaba ove Konvencije je obuhvaćeno više krivičnih djela kao što je učestvovanje u organizovanoj kriminalnoj grupi radi izvršenja teškog krivičnog djela (član 5.), pranje novca sa obuhvatom što više prediktnih krivičnih djela (član 6.), koruptivna krivična djela (član 8.) kao i krivičnu ili nekrivičnu odgovornost pravnih lica (član 10.) i ometanje pravde kao krivično djelo (član 23.). Također, odredbama članova 12. do 14. Konvencije utvrđuju se nephodne mjere, koje će koje će omogućiti konfiskaciju dobito stečene izvršenjem krivičnih djela obuhvaćenih Konvencijom ili imovine čija vrijednost odgovara vrijednosti te dobiti kao i imovine opreme ili drugih instrumenata korištenih ili namijenjenih za korištenje u vršenju krivičnih djela navedenih u Konvenciji.Pored navedenog kroz odredbe Konvencija su stipulirane mjere koje bi trebale usvojiti države potpisnice, a tiču se jurisdikcije nad krivičnim djelima iz članova 5., 6., 8. i 23. Konvencije, uslove i postupak ekstradicije, uzajamnu pravnu pomoć (član 18.), mogućnosti vođenja zajedničke istrage i posebnih istražnih radnji (članovi 19. i 20.), djelotvorne zaštite svjedoka (član 24.) i mjere za suradnju, unapređenje saradnje sa organima unutrašnjih poslova (članovi 26. i 27.) i prikupljanje,razmjenu i analizu informacija o prirodi organizovanog kriminala (član 28.).

Kroz sadržaj Protokola za prevenciju, suzbijanju i kažnjavanju trgovine ljudskim bićima, naročito ženama i djecom (član 5.), Protokola protiv krijumčarenja imigranata kopnom, morem i vazduhom (član 6.) i Protokola protiv nezakonite proizvodnje i trgovanja vatrenim oružjem, njegovim dijelovima i komponentama te streljivom (član 5.) koji dopunjava Konvenciju UN protiv transnacionalnog organizovanog kriminala su određena druga krivična djela.

4.2.6 Konvencija UN protiv korupcije (United Nations Convention against Corruption, Merida 2003).

Sadržajem odredaba članova 15. do 25. ove Konvencije su navedena koruptivna krivična djela koja bi države potpisnice prema sadržaju odredaba člana 42. Konvencije trebale inkriminisati u svojim zakodavstvima. Pored navedenog Konvencija državama potpisnicima preporučuje utvrđivanje odgovornosti pravnih lica za učeće u krivičnim djelima iz Konvencije (član 26.), nalaže poduzimanje neophodnih mjera radi identifikacije, trganja, zamrzavanja ili zaplijene bilo čega iz člana 1. tačka (a) i (b) u cilju konačne konfiskacije te primjereno upravljanje nadležnih organa zamrznutom, zaplijenjenom ili konfiskovanom imovinom, dostupnosti bankarskih, finansijskih i komercijalnih podataka bez pozivanja na bankarsku tajnu kao primjenu obrnutog tereta dokazivanja (člana 31). Također odredbama člana 44. do 50. Konvencije se reguliše međunarodna saradnja u krivičnim stvarima ,a odredbama člana 51. do 59. Konvencije detaljno se razrađuje načelo vračanje dobara od kojih je posebno interesantna odredba o raspolaganju sredstvima/imovinom. Naime prema sadržaju odredaba člana 57. Konvencije zamoljena strana ima obavezu da izvrši povraćaj oduzete imovine strani moliocu u slučajevima pronevjere javnih sredstava ili pranja takvih sredstava u slučajevima kada strana molilac osnovano utvrdi prethodno vlasništvo. Zamoljena strana može zadržati sredstva za pokriće razumnih troškova.

4.2.7. Plan aktivnosti Savjeta Europe: Sprječavanje i kontrola organizovanog kriminala: Strategija Evropske uniju za početak novog milenijuma

Plan aktivnosti Savjeta Europe: Sprječavanje i kontrola organizovanog kriminala: Strategija Evropske uniju za početak novog milenijuma iz 2000. godine je posvečena i otkrivanju, zamrzavanju i trajnom oduzimanju imovinske koristi od krivičnog djela. Sadržaj preporuke broj 17. tretira potrebu i mogućnost uspostavljanja specijaliziranih jedinica, a Preporuke 19., 20. i 21. bave se instrumentom tereta dokazivanja radi trajnog oduzimanja i oduzimanjem bez prisustva učinioca krivičnog djela radi "pokrivanja" u krivičnim slučajevima kada je učinilac nestao ili umro. Pored navedenog, preporukama se zahtijeva razmatranje instrumenata o razmjeni ili vračanju imovine među državama članicama.

Noviji razvoj međunarodnopravne regulative i standarda u oblasti konfiskacije imovine stečene kriminalom sublimiran je kroz sadržaje:

4.2.8. Konvenciji Savjeta Europe o pranju, otkrivanju, zaplijeni i konfiskaciji prinosa kažnjivih djela i finansiranja terorizma iz 2005. godine (Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, Warsaw, 2005),

Krajem 2003.godine Savjet Europe je odlučio da revidira, ažurira i proširi svoju Konvenciju o privremenom oduzimanju i oduzimanju prihoda stečenog krivičnim djelom iz

1990.godine.Proces revizije je doveo do Konvenciji Savjeta Europe o pranju, otkrivanju, zaplijeni i konfiskaciji prinosa kažnjivih djela i finansiranja terorizma koja je usvojena 16. maja 2005. godine na trećem sastanku na vrhu šefova država i Vlada Savjeta Europe u Varšavi. Konvencija predstavlja prvi međunarodni sporazum koji obuhvata i prevenciju i kontrolu pranja novca kao i finansiranje terorizma. U tekstu Konvencije je naglašena potreba brzog pristupa finansijskim informacijama ili informacijama o sredstvima u posjedu organizovanog kriminala, uključujući i terorističke grupe, ključ uspješnosti preventivnih i represivnih mjera.

Konvencija dopunjava definicije pojmova koji nerijetko radi prevoda na jezik domaćeg prva upotrebljavaju pogrešno i prave nepotrebne dodatne konfuzije u međunarodnoj saradnji; upućuje na potrebu usvajanja zakonodavnih i drugih mjera koje će omogućiti trajno oduzimanje sredstava i prihoda ili imovine čija vrijednost odgovara tim prihodima ili opranoj imovini; potiče na usvajanje zakonodavnih i drugih mjera koje će omogućiti da se brzo identifikuje, uđe u trag, zamrzne ili zaplijeni imovina koja podliježe konfiskaciji prema članu 3. Konvencije; preporučuje usvajanje zakonskih i drugih mjera koje će omogućiti državama potpisnicama da valjano upravljaju zamrznutom ili zaplijenjenom imovinom u skladu sa članom 4. i 5. Konvencije; mjera koje će omogućiti sudovima i drugim nadležnim organima obezbijede potrebna ovlaštenja kako bi mogli naložiti bezuslovno stavljanje na uvid bankarske, finansijske i komercijalne dokumentacije ili njihovu zapiljenu kako bi se mogle provesti radnje iz člana 3., 4. i 5.

Konvencije; mjere koje će omogućiti zainteresovanim stranama na koje se odnose radnje iz članova 3., 4. i 5. djelotvorne pravne lijekove kako bi zaštitili svoja prava; mjere koje će onemogućiti da dijela (počinjena sa namjerom) iz člana 9. stav 1. tačka (a), (b), (c) i (d) u nacionalnom pravu kvalifikuju kao krivična djela. Mjere koja će omogućiti da se pravna lica smatraju odgovornim za krivična djela pranja novca u smislu odredaba člana 10. Konvencije; mjere koje će omogućiti uspostavljanje FIU onako kako je definisano Konvencijom; mjere sprečavanja pranja novca; mjere za odlaganje/suspenziju sumnjivih transakcija, opšta načela i mjere međunarodne saradnje; mjere obaveznog pružanja pomoći u identifikaciji sredstava,prihoda i druge imovine stečene kriminalom koja podliježe konfiskaciji, kao i ulaženje u trag tim sredstvima, prihodima i imovini; mjere koje su neophodne za odgovor na međunarodni zahtjev druge strane potpisnice, da li fizičko ili pravno lice koje je predmet krivične istrage posjeduje ili kontroliše jedan ili više računa u bilo kojoj banci koja sa nalazi na njenoj teritoriji i da pribavi detaljne podatke o idetifikovanim računima i transakcijama te nadzire tokom određenog perioda bankarske transakcije preko jednog ili više računa i rezultate tog nadzora dostavi strani molitelju; mjere spontanog informisanja (bez zahtijeva) bez dovođenja u pitanje sopstvene istrage i postupaka; privremene mjere; mjere konfiskacije; odbijanje i odlaganje saradnje, međusobno obavještavanje i zaštita prava trećih lica; priznanje stranih sudskih odluka; procesna i druga pravila; saradnja između finansijsko-obavještajnih jedinica, mehanizam nadzora i rješavanje sporova i završni dio sa dodatkom .

4.2.9. Okvirna odluka Vijeća EU o konfiskaciji prihoda, sredstava i imovine povezane sa kriminalom (Council Framework Decision on Confiscation of Crime-Related Proceeds, Instrumentals and Property)14,

Evropsko vijeće je donijelo Odluku da uzajamno priznavanje, nasuprot uzajamnoj pomoći, treba da postane temelj saradnje pravosuđa država članica Evropske unije. Evropski nalog za hapšenje je prvi međunarodnopravni instrument koji je usvojen nakon ovog pristupa. Okvirna odluka o zamrzavanju je drugi međunarodnopravni instrument koji obuhvata i zamrzavanje

dokaza i zamrzavanja imovine sa namjerom da se ista konfiskuje. Identificirane su važne razlike u odnosu na Konvenciju o privremenom oduzimanju i oduzimanju prihoda stečenog krivičnim djelom iz 1990. godine. Prva, više ne postoji sistem postavljanja i prijema zahtijeva za uzajamnu pomoć kojin obuhvata državu molioca i zamoljenu državu. Kao supstitut toga sada postoji sistem u kojem država izdavalac izdaje naredbu o zamrzavanju i šalje tu naredbu drugoj državi, državi izvršiocu. Na taj način se izbjegava odgovor na zahtijev koji dolazi iz inostranstva već se u pravilu izvršava nalog koji dolazi iz inostranstva. Druga, prostor za razložno odbijanje izvršenja naloga je ograničen. Spisak osnova za odbijanje je jasan, kratak i detaljan.

4.3. Zašto je potrebno provesti finansijske istrage

Jedan od osnovnih motiva vršenja "teških" krivičnih djela, kao i krivičnih djela organizovanog kriminala je finansijska korist. Organizovane kriminalne grupe nezakonito stečenu finansijsku korist preko pranja novca nastoje legalizirati i pridružiti demokratskim vrijednostima/ tekovinama tih društava s ciljem jačanja ekonmskog i političkog uticaja u društvu. Radi toga oduzimanje finansijske koristi/prihoda stečenih krivičnim djelom se sve više priznaje kao efikasno sredstvo u borbi protiv kriminala, a osebno protiv organizovanog kriminala, jer član ili vođe kriminalne grupe/organizacije koji se samo osudi na zatvorsku kaznu obično u uspostavljenoj kriminalnoj strukturi zamjeni neko drugi I njegovim zatvaranjem aktivnosti kriminalne organizacije ne prestaju.

Istovremeno,oduzimanjem nezakonito stečene imovine/sredstava ostvaruje se princip da niko ne može imati korist od krivičnog djela. Svrha ovog principa nije samo prevencija već i zaštita interesa oštećene strane ,te radi toga nije dostatno/dovoljno počinitelja krivičnog djela samo (pr)oglasiti krivim i osuditi na kaznu zatvora, a pri tome mu ostaviti svu stečenu imovinsku korist na raspolaganju

4.4. Koji su efekti oduzimanja nezakonito stečene imovine?

Oduzimanje imovine stečene krivičnim djelom ima brojne efekte od kojih posebno treba izdvojiti:

- ✓ Vrši se prevencija (opšta i posebna), jer je imovinska korist razlog, motiv i cilj za većinu izvršilaca krivičnih djela;
- ✓ Sprečava integraciju nezakonito satečenog prihoda i penetraciju korupcije u legalne ekonomske tokove,
- ✓ Eliminiše/dokida sredstva za buduće činjenje krivičnih djela;
- ✓ Pomaže da se dođe do vrha kriminalne organizacije,
- ✓ Osnažuje vladavinu zakona I moralnog principa da niko ne može imati korist od krivičnog djela.

4.5. Oduzimanje imovinske koristi stečene krivičnim djelom

Oduzimanje imovine pribavljene krivičnim djelom ne spada u krivične sankcije u našem krivičnom zakonodavstvu. To je posebna krivično pravna mjera čiji se osnov nalazi u opštem pravnom principu sadržanom u odredbama člana 110. stav 2. Krivičnog zakona Bosne i Hercegovine,[177] da niko ne može zadržati imovinsku korist pribavljenu krivičnim djelom.

[177] „Službeni glasnik BiH",broj: :3/03,32/03,37/03,54/04,61/04,30/05,53706,55/06,32/07 i 8/10

Ovo je krivičnopravna mjera, jer je vezana za izvršenje krivičnog djela, i izriče se sudskom odlukom kojom je utvrđeno da je krivično djelo učinjeno,pod uslovima propisanim Krivičnim zakonom Bosne i Hercegovine,odnosno Krivičnih zakona F BiH,RS i BD BiH.

4.6. Prošireno oduzimanje imovinske koristi stečene krivičnim djelom

Shodno odredbama člana 110. Krivičnog zakona Bosne i Hercegovine kada se krivični postupak vodi za krivična djela iz glava XVII, XVIII, XIX, XXI a i XXII tog Zakona, sud može odlukom kojom je utvrđeno da je krivično djelo učinjeno ,po uslovima ovog zakona oduzeti I onu imovinsku korist za koju tužilac pruži dovoljno dokaza da se opravdano vjeruje da je takva imovinska korist pribavljena izvršenjem krivičnih djela, a počinilac nije pružio dokaze da je korist pribavljena zakonito.

Dakle, za prošireno oduzimanje neophodno je: (1) da se vodi krivični postupak za djela iz glava XVII,XVIII,XIX,XXI A I XXII, (2) da je donesena osuđujuća presuda, (3) da postoji dovoljno dokaza za opravdano vjerovanje da imovina potiče iz krivičnog djela za koje se vodi postupak, (4) da optuženi nije pružio dokaze o zakonitom sticanju. Prošireno oduzimanje predstavlja redukciju dokaznog standarda koji se primjenjuje pri utvrđivanju nezakonitog porijekla imovine, te inverziju ili podjelu tereta dokazivanja nezakonitog porijekla imovine između tužioca i okrivljenog[178].Međunarodni standard za uvođenje proširenog oduzimanja očigledno nije sporan. Postavlja se pitanje da li je ova mogućnost u skladu sa načelima domaćeg prava i prirodom sudskih postupaka, kako to predviđa Konvencija UN iz 2000. godine?

Napomena edukatoru:

Republika Srpska donijela je Zakon o oduzimanju imovine stečene izvršenjem krivičnog djela 2010. godine. Zakon usvaja koncept privremenog i trajnog oduzimanja imovine stečene krivičnim djelom, ali ne i imovine koja potiče iz kriminogene djelatnosti (prošireno oduzimanje). Prijedlog u oba slučaja podnosi tužilac, a odluku donosi sud. Zahtjev za trajno oduzimanje tužilac može podnijeti nakon potvrđivanja optužnice, a najkasnije u roku od godinu dana po pravosnažnom okončanju krivičnog postupka. Stvari se komplikuju ako vlasnik na glavnom pretresu ospori zahtjev tužioca. U tom slučaju odluka se donosi u posebnom postupku koji se mora okončati u roku od dvije godine od pravosnažnosti presude kojom je okrivljeni oglašen krivim. Ovakvo rješenje otvara nekoliko problema. S obzirom na brojne nejasniče i kontraverze nephodno je da edukatori pokušaju razjasne dilemu koji je poseban postupak zakonodavac ima u vidu: da li je to krivični ili neki drugi postupak, po kojim pravilima se provodi, da li pred vijećem ili sudijom pojedincem i ko odlučuje o žalbi. Osim toga,potrebn je da argumentiraju tvrdnju da je vezivanje oduzimanja imovine za osuđujuću presudu nije konzistentan pristup jer ne daje odgovor za slučaj smrti optuženog u toku postupka i zastaru krivičnog gonjenja koja nastupi u toku postupka. Takođermna fonu sadržaja ovog modela nephodno je argumentirati tvrdnu da je suštinski nedostatak ovog modela je izbjegavanje proširenog oduzimanja oduzimanja imovinske koristi.

Pažljivom analizom ove odredbe KZ BiH može se zaključiti da je inicijativa za primjenu instituta "obrnutog tereta dokazivanja" na postupajućem tužiocu koji treba pružiti dokaze koji

[178] Vidjeti opširnije: Elizabeta Ivičević Karas: Kaznenopravno oduzimanje imovinske koristi, Hrvatski ljetopis za kazneno pravo I praksu, br.2/2007, str.683.

ukazuju na sumnju da se radi o koristi koja je stečena izvršenjem kataloga navedenih krivičnih djela. Ukoliko nadležni sud prihvati prijedlog tužioca, teret dokazivanja je i na počinitelju jer je tužilac već sudu prezentirao dokaze koji ukazuju na sumnju da se radi o nezakonito stečenoj imovini/imovinskoj koristi od strane počinitelja. Počinitelj bi trebao da pruži dokaze da je imovinska korist stečena na zakonit način. Na opisani način zakonodavac je podijelio tereta dokazivanja između tužioca koji zastupa javni interes i počinitelja krivičnog djela. Ukoliko počinitelj i pored toga što mu je omogućeno korištenje svih raspoloživih dokaznih sredstava ne uspije dokazati da je imovinska korist stečena na zakonit način, sud na osnovu slobodnog uvjerenja može odlukom kojom je utvrdio da je krivično djelo počinjeno naložiti oduzimanje imovinske koristi od počinitelja.

4.7. Način oduzimanja imovinske koristi pribavljene krivičnim djelom

Krivičnim zakonom BiH je propisano da je predmet oduzimanja svaki oblik stečene imovinske koristi. Što se tiče utvrđivanja iznosa imovinske koristi koju treba oduzeti, uvriježena je praksa sudova da se primjenjuje tzv ”neto načelo, prema kojem je iznos nezakonito pribavljene imovinske koristi jednak prihodu od koje se odbijaju nastali troškovi.Za razliku od navedene prakse sudova u BiH, eksperti Savjeta Europe[179] preferiraju tzv. ”bruto načelo” koje ne dozvoljava oduzimanje troškova koje je počinitelj imao pri činjenju krivičnog djela.

U slučaju da nije moguće oduzeti imovinsku korist za koju je utvrđeno da je nastala izvršenjem krivičnog djela počinitelj je dužan isplatiti novčani iznos koji je razmjeran pribavljenoj imovinskoj koristi. Poseban problem pri identificiranju imovinske koristi, koja se na temelju sudske odluke treba oduzeti, predstavlja situaciju u kojoj je ista prenesena na treće lice. U pravilu se oduzimanje imovinske koristi vrši i od trećih osoba na koju je prenesena,osim u slučajevima kada se dokaže da su te osobe nastupale *bona fide* prema takvoj imovinskoj koristi.

Prema odredbama našem zakonodavstvu imovinska korist oduzima se i od trećih osoba na koje je prenesena bez naknade ili uz naknadu koja ne odgovara stvarnoj vrijednosti. Zakonski uslov za oduzimanje takve koristi od trećih osoba je činjenica da je treća osoba znala ili mogla znati da se radi o imovinskoj koristi pribavljenoj krivičnim djelom. Ovim je omogućena zakonska zaštita osoba koje su u dobroj vjeri došle u posjed određene imovine za koju u vrijeme njenog pribavljanja nisu znale ili mogle znati da se radi o nezakonito stečenoj imovini[180].

Također, jedan od načina prikrivanja imovinske koristi pribavljene krivičnim djelom je i njeno sjedinjavanje sa zakonito stečenom imovinom. U tim i takvim slučajevima zakon je predvidio oduzimanje I te imovine, ali u mjeri koja ne premašuje procijenjenu vrijednost imovinske koristi pribavljene krivičnim djelom[181].Pored navedenog moguće je da imovinska korist stečena krivičnim djelom bude izvor prihoda ili neke druge koristi odnosno da se takav prihod ili korist ostvaruje iz imovine sa kojom je nezakonito stečena imovinska korist sjedinjena ili u koju je pretvorena. U svim takvim slučajevima se takav prihod ili korist

[179]Robert Golobinet, Priručnik za pripadnike policije i pravosuđa,Finansijske istrage i oduzimanje imovine stečene krivičnim djelom,Savjet Europe,CARDS regionalni program 200272003-Projekt:Razvoj pouzdanih i funkcionalnih policijskih sistema i jačanje borbe protiv glavnih kriminalnih aktivnosti i jačanje policijske saradnje(CARPO),strana 32,

[180] Vidi Krivični zakon BiH,član 111.,stav 1.

[181] Vidi Krivični zakon BiH,član 111.stav 2.

oduzimaju na način i u mjeri kao da se radi o imovinskoj koristi pribavljenoj krivičnim djelom[182]. Krivičnim zakonom BiH je prihvaćeno načelo supsidijarnosti institute oduzimanja imovinske koristi stečene krivičnim djelom spram imovinskopravnih zahtijeva oštećenog.[183]

4.8. Postupak oduzimanja imovinske koristi pribavljene krivičnim djelom

Imovinska korist pribavljena krivičnim djelom utvrđuje se u krivičnom postupku po službenoj dužnosti. U tom postupku posebnu rekao bih ključnu ulogu ima tužilac koji pored ostalog ima pravo i obavezu da utvrđuje činjenice potrebne za odlučivanje o imovinskopravnom zahtjevu,odnosno,o oduzimanju imovinske koristi stečene krivičnim djelom[184].Prema tome, tužilac je dužan prikupljati dokaze I izviđati okolnosti koje su važne za utvrđivanje pribavljene imovinske koristi.[185] Međutim takve obaveze ima i Sud pa se na taj način u procesnom smislu ostvaruje načelo da niko ne može zadržati protivpravno stečenu imovinsko pravnu korist. Sud će, shodno zakonskim odredbama, vrijednost imovinske koristi procjenjivati na osnovu vlastite procjene, ako bi procjena na drugačiji način dovela do nesrazmjernih teškoća ili bi došlo do značajnijeg odugovlačenja postupka.[186] Na temelju navedenog slijedi logičan zaključak, da eventualne poteškoće u postupku utiču samo na postupak, odnosno način utvrđivanja imovinske koristi, a nikako i na obavezu Suda da utvrdi imovinsku korist. Sud je u svakom slučaju, bez obzira na način utvrđivanje, dužan da utvrdi imovinsku korist i izrekne mjeru oduzimanja. Također, se da zaključiti, da će se imovinska korist utvrđivati u svakom krivičnom postupku, izuzev ako je priroda krivičnog djela takva da je očigledno da njegovim izvršenjem nije pribavljana imovinska korist. Ako je oštećeni podnio imovinsko pravni zahtjev u smislu povrata predmeta pribavljenog krivičnim djelom,odnosno novčanog iznosa koji odgovara vrijednosti premeta, imovinska korist, će se utvrditi samo u onom djelu koji nije obuhvaćen imovinskopravnim zahtjevom, čime se prihvata supsidijarni odnos oduzimanja imovinske koristi spram imovinskopravnog zahtijeva[187].

Također, valja istaknuti imovinska korist se oduzima od optuženog bez obzira na njegovu materijalnu situaciju. Pri tome je potrebno naglasiti da je zakonom uspostavljen mehanizam osiguranja od otuđenja imovine koja je predmet postupka oduzimanja. U tom smislu ,Sud će pored utvrđivanja vrijednosti imovinske koristi slobodnom procjenom ,po službenoj dužnosti odrediti privremene mjere osiguranja,po odredbama koje važe po Zakonu o izvršnom postupku[188].U odnosu na prisutne dileme u vezi vrste odluke kojom se nalaže oduzimanje imovinske koristi, treba posebno naglasiti da je zakonom određeno da se oduzimanje može izvršiti presudom u kojoj se optuženi oglašava krivim,ili rješenjem o sudskoj opomeni,rješenjem o primjeni odgojne mjere, kao i presudom kojom se utvrđuje da je djelo izvršeno u stanju neuračunljivosti ili smanjene uračunljivosti[189]. Izmjenama propisa u ovoj oblasti ,moguće je pod određenim uslovima izricati ovu mjeru I u okviru skraćenog postupka izdavanja kaznenog naloga. Zakonom je propisano da tužilac može u optužnici zatražiti od Suda da izda kazneni nalog u kojem će optuženom izriči određenu krivičnopravnu sankciju ili mjeru bez provođenja glavne rasprave. U tom i takvom postupku tužilac pored ostalih, može

[182] Vidi Krivični zakon BiH,član 111.stav 3.
[183] Vidi Krivični zakon BiH,član 112.
[184] Vidi Zakon o izmjenama i dopunama Zakona o krivičnom postupku BIH,(„Službeni glasnik BiH“,broj 58/08)
[185] Vidi Zakon o krivičnom postupku BiH,član 392.stav 2.
[186] Vidi Zakon o krivičnom postupku BiH,član 394.
[187] Vidi Zakon o krivičnom postupku BiH,član 396.stav 1.
[188] Vidi Zakon o krivičnom postupku BiH,član 395.
[189] Vidi Zakon o krivičnom postupku biH,član 396.stav 1.

zatražiti i izricanje mjere oduzimanja imovinske koristi pribavljene krivičnim djelom. Uslov za to je da se postupak za krivična djela sa propisanom kaznom zatvora do pet godina ili novčanom kaznom kao glavnom kaznom,a za koje je tužilac prikupio dovoljno dokaza koji pružaju osnov za tvrdnju da je osumnjičeni učinio krivično djelo.[190] Konsultujući materijalnopravne odredbe kojim su propisane sankcije za koruptivna krivična dijela (glava XIX) da se zaključiti da se skraćeni postupak za izdavanje kaznenog naloga kojim se može zatražiti i izricanje mjere oduzimanja imovinske koristi pribavljene krivičnim djelom može voditi samo za određena krivična djela[191].

Što se tiče zakonskih ovlaštenja za prikupljanje podataka o pribavljenoj imovinskoj koristi,treba naglasiti da se tužilac i ovlaštene službene osobe[192] mogu koristiti sve zakonom propisane mjere, radnje i postupke dokazivanja opšteg i posebnog tipa. Tako, tužilac može predložiti Sudu da izda naredbu banci ili drugoj pravnoj osobi koja vrši finasijsko poslovanje, kojom će se ta ili te pravne osobe obavezati da dostave podatke o bankovnim depozitima i drugim finansijskim transakcijama i poslovima te osobe (osobe za koju postoje osnovi sumnje da je počinila krivično djelo koje je povezano sa sticanjem imovinske koristi) kao i osoba za koje se osnovano vjeruje da su uključene u te finansijske transakcije ili poslove osumnjičenog ako bi takvi podaci mogli biti dokaz u krivičnom postupku.[193]

Pored navedenih zakon poznaje I druge radnje koje se mogu poduzeti ovlaštene službene osobe I tužilac ,a koje služe utvrđivanju stvarnog porijekla imovine za koju se sumnja da je pribavljena krivičnim djelom kao što su: pretresanje stana , prostorija I osoba[194], privremeno oduzimanje predmeta I imovine[195], Ispitivanje osumnjičenog[196], saslušanje svjedoka[197], vještačenje[198] I posebne istražne radnje[199].

4.9. Kada treba početi sa finansijskom istragom?

Imajući na umu činjenicu da je svrha financijske istrage omogućiti oduzimanje prihoda stečenih krivičnim djelom, ona treba početi dovoljno rano kako bi se spriječilo počinitelja kaznenog djela da eventualno proda imovinu ili na neki drugi način raspolaže imovinom.
Pravo vrijeme za započinjanje financijske istrage jest odmah nakon otkrivanja osumnjičenog ili više njih, a prije provođenja radnji na temelju kojih osumnjičenik saznaje da se protiv njega vode istraga (npr. pretresanje stana , prostorija i osoba, ispitivanje osumnjičenog i sl.). Financijskom istragom i analizom transakcija može se proširiti krug osumnjičenih, a kod prikupljanja kriminalističko-obavještajnih podataka prije pokretanja finansijske istrage također je potrebno voditi računa o ciljevima vođenja financijske istrage. Dakle, da bismo bili efikasni i efektivni u prevenciji i borbi protiv počinitelja krivičnih djela kojima je osnovni motiv koristoljublje, moramo se usmjeriti kako na otkrivanje krivičnih djela i počinitelja, tako i na otkrivanje, zamrzavanje, privremeno i trajno oduzimanje prihoda od izvršenog krivičnog djela, jer ćemo jedino ako počinitelj dobije zasluženu sankciju i ako mu oduzmemo korist

[190] Vidi Zakon o izmjenam,a i dopunama Zakona o krivičnom postupku BiH,član 112 („Službeni glasnik, biH“,broj 58/08),
[191] Vidi Krivični zakon BiH,član 217.stav 2.,član 218. i član 219.stav 1. i 2.
[192] Vidi Zakon o krivičnom postupku BIH,član 20 stav 1 tačka g).
[193] Vidi Zakon o krivičnom postupku BiH,član 72.
[194] Vidi Zakona o krivičnom postupku BiH, član 51.,52.,53.,54.,55.,56.,57.,58.,59.,60.,61.,62.,63. i 64.
[195] Vidi Zakona o krivičnom postupku BiH, član 65. i 66
[196] Vidi Zakona o krivičnom postupku BiH, član 77.,78.,79. i 80.
[197] Vidi Zakona o krivičnom postupku BiH, član 77.,78.,79. i 80.
[198] Vidi Zakona o krivičnom posttupku BIH, član 95.,96.,97.,98.,99.,100.,101.,102. i 111
[199] Vidi Zakona o krivičnom postupku BiH, član 116

stečenu kaznenim djelom postići svrhu vođenja krivičnog postupka. Na temelju navedenog slijedi zaključak ,da eventualne poteškoće u postupku utiču samo na postupak, način utvrđivanja,a nikako I na obavezu Suda da utvrdi imovinsku korist.

4.10. Postupak provođenja finansijske istrage

U postupku provođenja istrage krivičnog djela organizovanog, koruptivnih, finansijskog i tzv. klasičnog kriminala i prikupljanja dokaza o elementima krivičnog djela, učiniocu i saučesnicima (posrdni izvršilac) odnosno podstrekačima i pomagačima nephodno je provesti finansijsku istragu u svim slučajevima kada krivično djelo ima za posljedicu ostvarenu imovinsku korist.

Apstraktno posmatrano, za ostvarivanje ciljeva svake organizacije, pa bila ona i kriminalna, potrebna su finansijska sredstva – ona se pribavljaju kroz vršenje određenih djelatnosti (zakonitih ili nezakonitih), zatim se evidentiraju, ulažu i transferišu, pri čemu kao rezultat takvih finansijskih aktivnosti nastaju određeni **„**papirnati**“** tragovi kroz razne forme dokumentacije , evidencije,poslovnih knjiga i finansijskih izvještaja.

Takvi tragovi se mogu otkriti upotrebom istražnih tehnika koje suštinski izviru iz finansijske dokumentacije i knjigovodstva odnos no računovodstva. Kriminalističke obrade organizovanog, kao i drugih vrsta imovinski motivisanog kriminala, mogu se poboljšavati selektivnom upotrebom različitih metoda finansijske istrage, kojima kao savremenim dostignućem kriminalističke nauke, dolazi do informacija i dokaza o:

- ulaganju nezakonito stečenih sredstava u legalno poslovanje;
- privrednim subjektima koji se koriste kao **„**paravan**“** za kriminalne djelatnosti;
- dokazima sadržanim u dokumentaciji koja prati ekonomsku aktivnost kriminalnih organizacija;
- postojanju ili skrivanju protivzakonito stečene imovine;
- prethodno nepoznatim poslovima kriminalnih organizacija ili pojedinaca;
- svjedocima za koje se nije znalo, kao i drugim lica i privrednim subjekatima uključenim u kriminalnu djelatnost;
- izvršenju drugih krivičnih djela, koje mogu pomoći da se rasvijetle šire kriminalne djelatnosti pojedinaca i kriminalnih organizacija;
- međunarodnim finansijskim vezama i operacijama između kriminalnih organizacija lociranih u različitim zemljama;
- visokokvalitetnim dokazima sadržanim u različitoj finansijskoj dokumentaciji, na osnovu kojih se mogu utvrditi načini transfera, vrijeme transfera i mjesta ulaganja nezakonito stečenih sredstava;
- mogućnosti da se identifikuje, prati i vrednuje imovina koja može biti predmet oduzimanja;
- primjeni mjera zamrzavanja radi sprečavanja bilo kakvog postupanja, transfera ili odlaganja nezakonito stečene svojine;
- drugim značajnim za kriminalističku obradu slučajeva organizovanog, odnosno imovinski motivisanog kriminala.

Pored zakonskih odredbi o nadležnostima i ulogama agencija koje učestvuju u finansijskoj istrazi potrebno je sa posebnom pažnjom voditi računa i o stvarnim odnosima između odgovarajućih agencija, organa , službi i institucija prvenstveno u pogledu svakog iznesenog

prijedloga, razmjene podataka i donošenja odluke u toku vođenja finansijske istrage.Tim više, jer su finansijske istrage veoma složene i obuvataju finansijske aktivnosti osumnjičenog od nekoliko godina.Zbog toga je nephodna velika umješnost tužioca u sačinjavanju multiagencijskog tima koji će besprijekorno funkcionirati i profesionalno provesti finansijsku istragu.

Finansijska istraga se provodi u više faza koje se logično , funkcionalno i vremenski vežu jedna na drugu sve do okončanja finansijske istrage.

4.10.1. Otkrivanje krivičnog djela i počinioca (krivične istrage)

Treba razlikovati policijski rad na otkrivanju krivičnih djela u skladu sa zakonskim propisima kojima se propisuje temeljni rad policije[200], od procesne uloge tužioca na otkrivanju krivičnih djela. Tužilac poduzima potrebne mjere na otkrivanju krivičnog djela isključivo temeljem postojanja osnova sumnje da je krivično djelo izvršeno. Prikupljanje i pronalazak saznanja i dokaza koji čine osnove sumnje da je djelo izvršeno je isključivo nadležnost policijskih organa u okviru svojih nadležnosti.

Znači da otkrivanje krivičnog djela koje obavlja tužilac predstavlja događajno usmjereno otkrivanje krivičnog djela, odnosno dodatno razotkrivanje krivičnog djela na temelju već stečenog saznanja da postoji događaj koji u sebi nosi osnov sumnje da je počinjeno krivično djelo, za razliku od policijskog otkrivanja krivičnog djela gdje je otkrivanje osnova sumnje da je krivično djelo izvršeno posljedica redovnih aktivnosti koje nisu bile usmjerene na događaj koji u sebi nosi osnov sumnje da je počinjeno krivično djelo.

Navedene nadležnosti tužioca i policije u otkrivanju krivičnog dijela i počinioca se ne isključuju već su sadržajem odredaba člana 218. Zakona o krivičnom postupku BiH su dizajnirane i povezane tako da čine cjelovit funkcionalni sistem u kojem tužilac zavisno od propisane kazne za krivično djelo za koje postoji osnov sumnje da je počinjeno, ima nadzor nad radom ovlašenih lica.

4.10.2. Utvrđivanje prihoda/imovinske koristi stečenih krivičnim djelom (vrsta i iznos)

S obzirom na činjenicu da su rijetki slučajevi da se preko direktnih dokaza kroz opšte i osebne mjere radnje ipostupke koji se poduzimaju u okviru krivičnu istragu utvrdi prihod koji je osumnjičeni stekao počinjenjem krivičnog djela i da se isti oduzme.

U pojedinim situacijama, na stepen osnova sumnje da je izvršeno krivično djelo iz oblasti imovinski motivisanog kriminala, mogu da utiču i spoljnje manifestacije, što je posljedica djelovanja materijalne koristi nastale izvršenjem krivičnog djela na učinioca.

[200] Vidi Zakon o policijskim službenicima BiH („Službeni glasnik“,broj 27/04, 63/04, 5/06, 33/06, 58/06, 15/08, 63/08 i 35/09), Zakon o policijskim službenicima („Službeni glasnik“,broj 43/10) i Zakon o policijskim službenicima F BiH („Službene novine F BiH“,broj 27/05) kao i Zakon o Državnoj agenciji za istrage i zaštitu („Službeni glanik BiH“,broj:27/04, 63/04, 35/05. i 49/09), Zakon o graničnoj policiji Bosne i Hercegovine („Službeni glasnik BiH“,broj: 50/04, 27/07, 59/09), Zakon o unutrašnjim poslovima („Službeni glasnik RS“,broj 48/03), Zakon o policiji Brčko Distrikta BiH („Službeni glasnik BD BiH“,broj 31/09, 60/10, 31/11), Zakon o unutrašnjim poslovima F BiH („Službeni glasnik BiH“,broj 49/05).....

Ove spoljne manifestacije mogu da posluže kao indicije za postavljanje verzija/hipoteza o izvršenom krivičnom djelu (promjena ponašanja, nekontrolisano trošenje novca, kupovina skupocjenih stvari, kockanje, i sl.). Temeljna mjera koja se primjenjuje u takvim slučajevima je *finansijska istraga* osumnjičenog, koja, između ostalog, obuhvata procjenu da li način njegovog života ukazuje na „pošten život". Takva finansijska istraga se može obaviti na tri načina – prvi je u teoriji i u praksi poznat kao rekonstrukcija neto vrijednosti i novčanog toka i ona se primjenjuje u slučajevima kada imamo dostupnu i pouzdanu dokumentaciju na raspolaganje iz koje se može retroaktivno utvrditi početno stanje i svi ili većina poslovnih događaja vezanih i bitnih za Finansijski kapacitet osumnjičenog, drugi kao *analiza neto vrijednosti* i koristi se u slučajevima kada osumnjičeni ima imovinu koja privlači pažnju, dok se treći definiše kao *analiza izvora i primjene sredstava,* i primjenjuje se kada osumnjičeni ima vidno/ekstremno izražene potrošačke navike.

Da bi se tačno, pravilno i blagovremeno utvrdili finansijsko stanje osumnjičenog poželjno bi bilo da istražitelji koji provode finansijsku istragu posjeduju znanja i vještine koje bi im omogućile da:

- pravilno kategoriziraju svaki poslovni događaj za osumnjičenog u periodu koji je obuhvaćen istragom.
- pravilno identificiraju vrstu dokumenata koji su relevantan dokaz da se taj poslovni događaj desio (npr. neplaćena faktura za utrošak električne energije je dokument o obavezi osumnjičenog, uplatnica kojom je plaćena faktura za električnu energiju je dokaz o trošku osumnjičenog),
- znaju značenje dokumenta,njegove veze sa drugim dokumentima i njegov uticaj na finansijski položaj i kapacitet fizikog i pravnog lica,
- znaju locirati mjesto-a gdje se taj dokument generisao, njegov hodogram(unutrašnji I vanjski) , mjesto gdje se isti čuva (npr. podaci o ispostavljenim, plaćenim i neplaćenim fakturama, opomenama, tužbama, presudama i sudskim izvršenjima za utrošak električne se evidentiraju u poslovnim knjigama javnih preduzeća, zavisno o vrsti plaćanja (gotovinsko ili bezgotovinsko plaćanje) ista se mogu dokumentovati knjigovodstvenim ispravama koje su evidentirane u poslovnim knjigama poslovne banke
- znaju propisane rokove za čuvanje knjigovodstvenih isprava, poslovnih knjiga, finansijskih izvještaja i popisa;
- kao i da poznajemo procedure kroz koje se na zakonit način mogu steći potrebni dokazi o finansijskoj sposobnosti osumnjičenog odnosno visini nelegalnih prihoda koje je ta osoba stekla u periodu koji je obuhvaćen finansijskom istragom ;

4.10.3. Ekonomske kategorije poslovnih događaja koje određuju finansijski položaj pojedinca

U toku finansijske istrage pažnja tužitelja i finansijskih istražitelja agencija za provođenje zakona je skocentrisana na četiri ekonomske kategorije koje određuju finansijsku poziciju svakog od pojedinaca. Na temelju analitičkih podataka i dokumentacije o prihodima, troškovima, imovini i obavezama može se izvršiti se potpuna rekonstrukcija finansijskog stanja osumnjičenog koja ponekada seže i po nekoliko godina unazad. Stoga je veoma bitno da istražitelji ovaj posao urade brzo, temeljito i odgovorno kako ne bi ostavili prostora osumnjičenom da ometa i prolongira istragu.

Stoga za potrebe edukativnog modela je neophodno razjasniti šta podrazumijeva i obuhvata svaka od navedenih kategorija , koji su kriteriji za njihova međusobna razgraničenja te kako i na temelju koje dokumentacije se za potrebe finansijske istrage utvrđuje i iskazuje njihova vrijednost .

4.10.3.1.. Prihod odnosno neto prihod

Prihod koji čine sva lična primanja u novcu i/ili stvarima koristima, protuuslugama,i/ili u vidu premija sl. na koja su prethodno plaćene pripadajuće obaveze.

Prihodi se kao i troškovi evidentiraju i utvrđuju po načelu blagajne. Načelo blagajne znači da se za pojedinca prihod smatra stvarno primljenim prihodom u času kada mu je stavljen na raspolaganje i/ili kada je primljen u njegovu korist, a rashodi se smatraju rashodima kada su plaćeni.

U prihode ubrajamo neto plaća koju uposleniku isplaćuje poslodavac po osnovu ugovora o radu odnosno radnog odnosa ili daje u dobrima, koristima, protuusluga, i/ili u vidu premija i drugih prihoda; dodatni neto prihodi po osnovu naknada, potpora i sl. koje poslodavac isplatio uposlenicima; neto prihodi od samostalnog obavljanja djelatnosti (obrt, poljoprivreda, šumarstvo, slobodna zanimanja i sl.); prihodi po osnovu sudjelovanja u raspodijeli dobiti privrednih društava (dividende ili udjeli); penzije/mirovine rezidenta bilo da je stečena u inozemstvu ili Bosni i Hercegovini; potpore i druga primanja ostvarena po osnovu posebnih propisa i pravima ratnih vojnih invalida i civilnih žrtava rata; socijalne potpora; dječji dodatak i novčana sredstva za opremu novorođenčeta; prihodi od prodaje imovine; naknada štete načinjene na imovini; osiguranje ili druga naknada štete načinjene na imovini, u iznosu koji je rabljen za zamjenu ili popravak oštećene imovine; nagrade svih vrsta; prihodi po osnovu naknade za vrijeme nezaposlenosti i spriječenosti za rad; prihodi invalidnih osoba koje su uposlene u privrednom društvu, ustanovi ili radionici za radno i profesionalno osposobljavanje i rehabilitaciju; prihodi po osnovu naknade za tjelesno oštećenje, umanjenu radnu sposobnost i naknada za pretrpljene neimovinske štete; prihodi po osnovu naknade štete uposlenicima po osnovu posljedica nesreće na radu; naknade osuđenim osobama za vrijeme odsluženja kazne u odgojno-popravnim, odnosno kazneno-popravnim ustanovama; prihodi po osnovu stipendija učenika i studenata na redovnom školovanju; prihodi koje ostvare učenici i studenti putem učeničkih i studentskih udruženja; dobitci ostvareni sudjelovanjem u nagradnim igrama i igrama na sreću; prihodi po osnovu kamate po viđenju i/ili na štednju u bankama, štedionicama i štedno-kreditnim zadrugama,bankovnim računima (žiro račun,devizni račun i dr.) i kamate na državne obveznice, prihodi po osnovu nasljedstva; prihodi od imovinskih prava ostvarenih otuđenjem odnosno prodajom, ustupanjem ili zamjenom ili drugim prijenosom uz naknadu autorskih prava, patenata, licenci, franšiza i ostale imovine koja se sastoji od prava …….

4.10.3.2. Troškovi

Troškovi su novčani izraz upotrjebljenih resursa koji se koriste u svrhu postizanja određenog cilja/ciljeva i /ili ostvarenja učinaka. Uglavnom su to plaćanja za stanovanje, odjeću, obuću, ishranu, održavanje i servis, ličnu higijena, kozmetiku, rehabilitaciju i liječenje, školovanje i usavršavanje, komunalije, energiju, ptt usluge, zabavu, kulturu, sport, odmor, rekreaciju, prevoz, rate za kredite, kamate, članarine, novčane kazne, takse, premije osiguranja, pretplata na RTV, časopise i knjige, pokloni i sl. Kao što je navedeno kod kategorije prihoda i troškovi se za potrebe finansijske istrage evidentiraju , iskazuju i tretiraju po načelu blagajne

u vrijednosti izvršenog plaćanja. Načelo blagajne znači da se troškovi pojedinca smatraju troškovima tek kada su plaćeni.

4.10.3.3. Imovina

Imovina privrednom smislu je skup dobara koje posjeduje određeni subjekt i sa njima nesmetano raspolaže. U pravnom smislu imovina je skup subjektivnih imovinskih prava predstavljenih jednim nositeljem, a u knjigovodstvenom smislu imovina je skup subjektivnih prava i obaveza predstavljenih jednim nositeljem.Za potrebe edukativnog modela imovinu ćemo tretirati kao skup dobra/resursa i subjektivnih prava koje posjeduje predstavljenih jednim nositeljem koji sa njima nesmetano raspolaže. Imovina su stvari ili prava koje pojedinac posjeduje ili ima pravo na njih i koje se mogu pretvoriti u novac. Pod imovinom za potrebe ovog modela podrazumijevamo novac (žiro računi, tekući računi, posebni računi, gotovina, gotovina u sefu, devizni računi, oročeni depoziti te debitne kartice u vezi sa tekućim računom) i novčani ekvivalente, hartije od vrijednosti, zemljište, šume, građevinski objekti niskogradnje I visokogradnje (izgrađeni i neizgrađeni), transportna sredstva svih vrsta, zrakoplovi plovila potraživanja, namještaj, oprema i uređaji, imovinska prava (autorskih prava, patenata, licenci i franšiza) i ostale imovine koja se sastoji od prava. Imovina se potrebe modela ne iskazuje po tržišnoj vrijednosti već se uvijek iskazuje po vrijednosti iskazanoj na fakturi u trenutku nabavke.

4.10.3.4. Obaveze

Obaveza je pravni odnos (ugovorni ili zakonski) između dvije strane na osnovu kojeg jedna strana ovlaštena da zahtijeva od druge strane određeno davanje, činjenje ili uzdržavanje od nečega što bi inače imala pravo da čini,a druga strana je dužna da to ispuni. Obaveze možemo grubo podijeliti na zakonske i ugovorne.Za potrebe praćenja neto vrijednosti obavezama se smatraju sva dugovanja pojedinca.

Napomena edukatorima

Bilo bi uputno da se učesnicima edukacije prezentira praktičan primjer koji sadrži poslovne događaje koji se trebaju kategorizirati u sve četri navedene ekonomske kategorije, a odnose se na osumnjičenog.Nakon prezentacije učesnici bi trebali sačiniti ogledne obrazce (kontrolne liste) te u njima izvršiti kategorizaciju poslovnih događaja, a nakon toga svoje uradke uz odgovarajuća objašnjenja elaboriraju edukatorima.

4.10.4. Metoda rekonstrukcije novčanog toka i neto vrijednosti

Metoda rekonstrukcije neto vrijednosti i novčanog toka zasniva se također na podacima o prihodima, rashodima, obavezama i imovini sadržanim u dokumentaciji i evidencijama i poslovnim knjigama koji se odnose na finansijske transakcije osumnjičene osobe.Ova metoda se primjenjuje u slučajevima kada imamo dostupnu i pouzdanu dokumentaciju na raspolaganje iz koje se može retroaktivno utvrditi početno i krajnje stanje i svi ili većina poslovnih događaja vezanih i bitnih za finansijski položaj i kapacitet osumnjičenog. Ova metoda podrazumijeva precizno i dokumenovano utvrđivanje četiri ekonomske kategorije koje određuju finansijski kapacitet osumnjičenog: (1) imovina (2) obaveze, (3) prihodi (4) rashodi, ostvareni na dan početka finansijske istrage. Ova metode se primjenjuje u svim slučajevima kada nema dovoljno neposrednih dokaza o neprijavljenim, odnosno nezakonitim

prihodima, ili su evidencije neodgovarajuće ili netačne, pri čemu je evidentno da se imovina i/ili obaveze i/ili troškovi osumnjičenog uvećavaju.

4.10.4.1. Rekonstrukcija novčanog toka

Rekonstrukcijom i analizom prihoda i troškova po vrsti iznosu u određenom vremenskom periodu može se precizno utvrditi u kojem apsolutnom i relativnom iznosu pojedinac uspijeva da plati dospjelih obaveza (troškovi). Ovakav način tretiranja prihoda i troškova odnosno onog što je legalno zarađeno i onoga što je potrošeno naziva se rekonstrukcija novčanog toka. Praćenjem novčanog toka u određenom periodu utvrdit ćemo da li je neto prihod u određenom vremenskom periodu bio veći i u kojem iznosu od troškova i obrnuto. Ovdje treba napomenuti da su u pravilu izvori prihoda po vrsti znatno uži od vrste troškova. Upravo zbog toga je sve troškove pojedinca veoma teško, ali ne i nemoguće identificirati i dokumentovati. Detaljna analiza identificiranih prihoda i troškova prvi je korak u definiranju finansijske pozicije/profila pojedinca koji je predmet finansijske istrage.

4.10.4.2. Rekonstrukcija neto vrijednosti/kapitala vlasnika

Paralelno sa rekonstrukcijom i analizom novčanog toka neophodno je pratiti analitički i sintetički i neto vrijednost .Neto vrijednost (Nv) je razlika između imovine (Ip) i obaveza pojedinca (Op). Neto vrijednost može biti pozitivna, neutralna i negativna. Pozitivna je ako je imovina veća od obaveza, neutralna je ako je imovina identična obavezama i negativna ako je imovina manja od obaveza.

Nakon izvršene rekonstrukcije novčanog toka i neto vrijednosti istog perioda vrši se komparativna analiza prikupljanih podataka.

Ukoliko osumnjičeni u utvrđenom periodi ima pozitivan novčani tok to znači da mu je preostao određeni iznos novca koji automatski predstavlja povećanje njegove finansijske imovine. Preostali novac iz novčanog toka pojedinac je mogao koristiti za plaćanje obaveza ili za "kupnju" nove imovine. Ukoliko ostatkom pozitivnog novčanog toka vratimo/platimo dug/obaveze to znači da će se smanjiti njegovi troškovi u novčanom toku što za posljedicu ima veći pozitivan rezultat novčanog toka. Ako pak odluči da preostali novac investira u neki od oblika finansijske imovine ta će nam imovina u kratkomi i/ilisrednjem i/ili dugom roku stvarati dodatni neto prihod što će u uslov zadržavanja troškova istog perioda za posljedicu opet imati pozitivan rezultat u novčanom toku. Smanjenjem obaveza ili kupovinom imovine postepeno se povećava neto vrijednost pojedinca. Ako je novčani tok negativan, onda će se dogoditi suprotno od navedenog. S vremenom će pojedinac morati prodavati svoju imovinu ili posezati za stvaranjem novih obaveza u skladu sa prevelikim troškovima. Ovaj proces će smanjiti njegovu neto vrijednost i staviti ga u lošu finansijsku poziciju iz koje treba da nađe izlaz. Nažalost, jedan od izlaza je njegovo pristupanje kriminalnoj organizaciji u okviru koje počinje da se bavi nedozvoljenim aktivnosti koje mu osiguravaju nelegalni prihod.

Model retroaktivne rekonstrukcije podataka o imovini, obavezama, prihodima I troškovima osumnjičenog s ciljem utvrđivanja nezakonitih prihoda je veoma zahtijevan model koji ukoliko se temelji na tačnim polaznim podacima za sve četiri kategorije i na podacima iz relevantne dokumentaciji daje vrlo precizne podatke o nezakonitim prihodima odnosno njihovoj vrsti visini pa čak I cjelokupnom periodu sticanja.

Prikupljanje ličnih dokaza usmjereno je na vođenje razgovora sa osumnjičenim i licima kojima su mogle biti poznate pojedine činjenice koje se odnose na konkretnu kriminalističku obradu. Radi izbjegavanja nesporazuma, na početku razgovora osumnjičenom treba predočiti šta se podrazumijeva pod pojmom sredstva(npr.gotovina), imovina (imovinska prava),prihod (npr.isplačena dividenda)i trošak(npr.plaćena rata za lombarni kredit) jer osumnjičeni kasnije može da stvari koje je izostavio iz iskaza, ili ih lažno saopšti, pripiše nerazumijevanju pojma navedenih kategorija. U svakom konkretnom slučaju treba preduzeti mjere da bi se saznalo nešto više o bilo kakvom pisanom tragu o postojanju nekog od pojavnih oblika navedenih ekonomskih kategorija.

Dokazivanjem na osnovu metoda (retroaktivne) rekonstrukcije podrazumijevaju da se sva uvećanja imovine za koja ne postoji odgovarajuća dokumentacija, svrstavaju u kategoriju neprijavljenih, odnosno nezakonitih prihoda, zavisno od prirode finansijske istrage.

U cilju što kvalitetnije prezentacije i razumijevanja cjelokupnog postupka primjene ovog metoda, preporučljivo je korištenja priloga u obliku kontrolnih lista, tabelarnih prikaza i grafičkih priloga. Prilozima se objašnjava cijeli slučaj, a poželjno je da budu organizovani na takav način da služe postizanju određenog cilja, odnosno izračunavanju neprijavljenog ili nezakonitog prihoda. Prilozi se mogu koristiti i u pojedinim fazama krivičnog postupka, za bolje razumijevanje primijenjenih metoda i dokazivanje pojedinih činjenica relevantnih za krivični postupak.

4.10.5. Metod dokazivanja na osnovu neto vrijednosti

Metod dokazivanja na osnovu neto vrijednosti zasniva se također na podacima o prihodima, rashodima, obavezama i imovini sadržanim u dokumentaciji i evidencijama i poslovnim knjigama koji se odnose na finansijske transakcije osumnjičene osobe[201]. Primjenjuje se u poreskim i drugim finansijskim istragama, pri čemu treba napomenuti da se u slučajevima poreskih istraga utvrđuju neprijavljeni prihodi, dok su u ostalim finansijskim istragama predmet istrage nezakoniti prihodi.

Dokazivanjem na osnovu neto vrijednosti mjeri se povećanje, odnosno smanjenje neto vrijednosti sredstava kojima jedna osoba raspolaže, pri čemu se sva uvećanja imovine za koja ne postoji odgovarajuća dokumentacija, svrstavaju u kategoriju neprijavljenih, odnosno nezakonitih prihoda, zavisno od prirode istrage.

Historijski posmatrano, organizovana primjena ovog metoda javlja se tridesetih godina XX vijeka, kada agencije za provođenje zakona u SAD-u nisu imale uspjeha u procesuiranju šefova raznih mafijaških udruženja koja su se bavila organizovanim kriminalom. Posredne metode dokazivanja nezakonitih djelatnosti prvi su razvili specijalni agenti Poreske uprave SAD (*Internal Revenue Service-IRS*), za potrebe krivičnog gonjenja čelnih ljudi organizovanog kriminala, i to zbog kršenja poreskih zakona. Koristeći ove metode, na osnovu dokumentacije su dokazivali da su prihodi članova kriminalnih organizacija bili dovoljno visoki za obaveznu poresku prijavu, odnosno da članovi kriminalnih organizacija nisu prijavljivali sve svoje prihode. Na taj način su šefovi gangsterskih porodica odlazili u zatvor, ali ne zbog ubistava, ucjena ili drugih krivičnih djela za koja su sumnjičeni, nego prvenstveno zbog utaje poreza na prihod.

[201] Vidi više George A.Manning,Ph.D.C.F.E.,E.A.Taylor&Francis Group,Boca Rata-London-Singapore, 2005:page 119-143).

Metod dokazivanja na osnovu neto vrijednosti zasniva se na činjenici da onaj ko posjeduje novac isti može potrošiti, uložiti ili sačuvati (tzv. sef,slamarice i sl.). Koristeći ovaj metod moguće je izračunati koliko je određena osoba potrošila novca, koliko je uložila u određene poslove, a koliko je, pak, sredstava eventualno sačuvala za određeni vremenski period. Ovi iznosi se potom upoređuju sa poznatom vrijednošću imovine/sredstava kojom je to lice raspolagalo u određenoj godini, pri čemu se eventualni višak imovine/sredstava smatra neprijavljenim, odnosno nezakonitim prihodom, u zavisnosti od vrste istrage.

Ovaj metod se primjenjuje u slučajevima kada nema dovoljno neposrednih dokaza o neprijavljenim, odnosno nezakonitim prihodima, ili su evidencije neodgovarajuće ili netačne, pri čemu je evidentno da se imovina osumnjičenog uvećava. Uspješna primjena metoda dokazivanja na osnovu neto vrijednosti zavisi od pouzdanosti informacije o polaznoj neto vrijednosti osumnjičenog lica, koja uključuje sva sredstva i sve obaveze (odnosno prihode i rashode) u određenom trenutku. Polazna neto vrijednost je osnovica (polazna tačka) od koje će se računati buduće promjene sredstava ili obaveza. Prilikom primjene metoda dokazivanja na osnovu neto vrijednosti izuzetno je važno da se utvrdi tačna neto vrijednost imovine/sredstava osumnjičenog na početku, tj. u osnovnoj ili polaznoj godini.

Metod dokazivanja na osnovu neto vrijednosti zahtjeva primjenu matematičkih operacija određenih formulom za izračunavanje neto vrijednosti[202]. Sama formula za izračunavanje neto vrijednosti glasi:

I (imovina i sredstva*)* **– D (**dugovanja) = **Nv (**neto vrijednost**) - Np (**Neto vrijednost početne godine = **N** (povećanje ili smanjenje neto vrijednosti) + **Lt** (Lični troškovi) **+Lg** (lični gubici) **= Us** (Ukupna sredstva) **– Lp** (Legalni prihodi**) =Nn** (Neprijavljeni ili nezakoniti prihodi)

Imovina i sredstva obuhvataju gotovinu, novac na računima, hartije od vrijednosti, vozila, nekretnine, lične predmete, antikvitete, opremu i sredstva koja se koriste u poslovanju, i dr. (već navedeno) Finansijske obaveze obuhvataju kredite, pozajmice, dospjele obaveze po ispostavljenim računima, stanja na računima (minus), hipoteke, dospjele rate za otplatu, i dr. Troškovi amortizacije su uključeni u model odnosno njegovu matematičku formulu. Da bi se utvrdila početna neto vrijednost osumnjičenog, treba detaljno analizirati sve stavke koje se svrstavaju u grupu imovina/sredstva, uz korištenje dostupne dokumentacije. Jedan od mogućih problema prilikom utvrđivanja početne neto vrijednosti može da bude i utvrđivanje iznosa gotovog novca koji osumnjičeni posjeduje. Prilikom upotrebe svake indirektne metode dokazivanja, jedan od najznačajnijih elemenata koje treba utvrditi jeste iznos gotovine. Ona se određuje obavljanjem razgovora sa osumnjičenim i potencijalnim svjedocima, pregledom dokumentacije, primjenom tehnike izvora i upotrebe izvora sredstava i sl.

Nakon gotovog novca i sva ostala imovina se uključuje u formulu, kako bi se smanjila mogućnost greške. Krajnje stanje na računima do određenog datuma računa se za svaki postojeći bankovni račun, što uključuje štedne uloge, račune za kredite, račune u kreditnim zadrugama, gotovinu koja se drži kod brokerskih kuća i svaki drugi oblik štednih uloga. Takvo stanje mora da odgovara svakoj uplati, polog ili isplati koji je prošla kroz taj račun. Dokazi o zaključnom/finalnom stanju na računima na kraju godine obuhvata i izvode tih računa sa pratećom dokumentaciju o otvaranju tih računa.

[202] George A.Manning,Ph.D.C.F.E.,E.A.Taylor&Francis Group,Boca Rata-London-Singapore, 2005:page 98).

Vrijednost bilo koje hartije od vrijednosti računa se u odnosu na njenu vrijednost na kraju godine, dok svih drugih materijalnih stvari, određuje prema njihovoj cijeni u vrijeme sticanja, ne po tržišnoj cijeni. Dobici ili gubici koji mogu nastati kao rezultat promjena tržišnih cijena se ne oporezuju, niti se mogu odbiti od poreza do trenutka dok se hartije od vrijednosti ne prodaju. Dokumentacija koja se odnosi na hartije od vrijednosti uključuje dokaz o vlasništvu I načinu njihovog sticanja.

Cijena vozila u vrijeme kupovine dodaje se na kraju obračunske godine. Ukoliko je kredit koji je služio za kupovinu vozila osiguran, preostali iznos kredita koji nije otplaćen svrstava se u rubriku dugovanja/obaveza u završnoj matematičkoj formuli. Dokumentacija za vozila može obuhvatati bilo koji oblik dokumentacije, auto kuće, društva za lizing, agencije ili pojedinaca koji su prodali vozilo, kao i bilo koji drugi oblik pisanog dokaza o registraciji ili prenosu vlasništva koji se nalazi u posjedu državnog organa. Kao i kod vozila, i cijena nekretnine u vrijeme kupovine uračunava se na kraju godine. Kao i u prethodnom slučaju, ako je kredit za kupovinu nekretnine bio osiguran, on se posebno računa pod stavkom dugovanja.

Dokumentacija o nekretninama trebalo bi da obuhvati kupovnu cijenu, dokaz o dobivanju kredita (ukoliko je postojao zahtjev za njegovo dobivanje), način isplate i pravni status nekretnine. Pored dokumentacije koja dokazuje kupovinu nekretnine, treba doći i do dokaza o kontinuiranosti vlasništva nad nekretninom kroz provjeru plaćanja poreza na godišnjem nivou za nekretninu.

U slučajevima kada je preduzeće pravni subjekt odvojen od osumnjičenog, imovina preduzeća se neće izračunavati pri procjeni neto vrijednosti imovine. Imovina preduzeća se može računati samo u slučajevima kada je osumnjičena osoba jedini vlasnik preduzeća. U takvim situacijama postoji preplitanje lične imovine sa imovinom preduzeća, zbog čega je potrebno izračunati neto vrijednost imovine preduzeća. Sredstva osumnjičenog u preduzeću moraju se uračunati u svojoj prvobitnoj ili prilagođenoj vrijednosti, pri čemu se vrijednost amortizacije i smanjenja vrijednosti sredstava preduzeća moraju posebno navesti pod stavkom dugovanja. Poslovna imovina najčešće obuhvata poslovni namještaj i opremu, nekretnine, sredstva za proizvodnju i potraživanja.

Slijedeći korak u formuli izračunavanja neto vrijednosti imovine predstavljaju dugovanja. Kao i u slučaju imovine i sredstava, iznos koji se duguje na kraju godine uključuje se u formulu. U dugovanja se svrstava svako zaduživanje subjekta, uključujući i dug koji se odnosi na zaduženja za lični kredit, kredite za kupovinu opreme, zaduženje za kredit dobiven za nekretninu, zaduženje po kreditnoj kartici ili bilo koji drugi oblik zaduženja. Poslovna zaduživanja mogu da uključe nagomilane otplate na računima i račune za naplatu. Dokumentacija o dugovanjima koja se odnose na imovinu i sredstva uključuje razne fakture, zahtjeve za odobrenje kredita, poreske prijave i druga dokumenta.

Neto vrijednost obuhvata samo novac potrošen za kupovinu sredstava ili smanjenje dugovanja. Pojedinac troši novac i za lične životne troškove, koji uključuju izdatke za hranu, komunalije, školarinu, osiguranje, plaćanje poreza, benzin i druge potrebe. Ove stavke se također moraju uzeti u obzir prilikom utvrđivanja ukupno potrošenih sredstava. Lični troškovi smanjuju dio razlike do nezakonite ili neprijavljene dobiti. Također, neuključivanje ličnih gubitaka u formulu za neto vrijednost poremeti će već izračunate podatke i neće predstavljati cjelokupan iznos neprijavljene dobiti ili nezakonito stečene dobiti. Lični gubici mogu biti kapitalni, zatim gubici nastali prilikom prodaje ličnih predmeta i sl. Zatim sledi

utvrđivanje sredstava iz poznatih izvora. Krediti ovdje nisu poznati izvori, budući da se prilikom izračunavanja neto vrijednosti označavaju kao dugovanja.

Gotovinu možemo odrediti kao novčana sredstva koja se nalaze u posjedu neke osobe. Ta sredstva se mogu nalaziti u stanu ili kancelariji nekog pojedinca, mogu da budu povjerena trećoj osobi ili pohranjena u nekom sefu. Gotovina ne uključuje novac koji se nalazi na bilo kom računu kod finansijskih institucija. Finansijska analiza je usmjerena ka gotovini kojom je neko raspolagao određenog datuma prethodne godine, ili godine prije početka istrage (osnovna godina) i na gotovinu kojom se raspolaže istog datuma tekuće godine u kojoj se kriminalistička obrada sprovodi.

U postupku utvrđivanja iznosa gotovine kojom je lice raspolagalo u osnovnoj godini koja služi za poređenje, i tekućoj godini ili godinama koje su obuhvaćene istragom, treba prikupiti lične i materijalne dokaze. Prikupljanje ličnih dokaza usmjereno je na vođenje razgovora sa osumnjičenim i licima kojima su mogle biti poznate pojedine činjenice koje se odnose na konkretnu kriminalističku obradu. Radi izbjegavanja nesporazuma, na početku razgovora osumnjičenom treba predočiti šta se podrazumijeva pod pojmom gotovina, jer osumnjičeni kasnije može da stvari koje je izostavio iz iskaza, ili ih lažno saopšti, pripiše nerazumijevanju pojma gotovine. U svakom konkretnom slučaju treba preduzeti mjere da bi se saznalo nešto više o bilo kakvom pisanom tragu o postojanju gotovine. Kada je riječ o različitim kriminalnim aktivnostima, najčešće se vodi neka vrsta evidencije (dnevna prodaja opojne droge i ostvarena zarada). Ona se vodi po principu jednostrukog knjiženja i može da sadrži značajne podatke o količini novca koji je osumnjičeni zaradio. Također, treba prikupiti i svu dokumentaciju koja može da opovrgne postojanje gotovine, a odnosi se na sve djelatnosti kojima je gotovina stečena.

Metod dokazivanja na osnovu neto vrijednosti svoje začetke i najširu primjenu ostvario je u SAD-u. Da bi službe za sprovođenje zakona ove zemlje primijenile jedan takav istražni metod, potrebno je da budu ispunjena tri zahtijeva: 1) pouzdano utvrđivanje početne neto vrijednosti za osnovnu godinu; 2) negirati razumna obrazloženja osumnjičenog koja pobijaju njegovu krivicu; 3) utvrditi da li je rast neto vrijednosti rezultat dohotka koji se oporezuje prema važećim propisima, ili je posljedica nezakonitih poslova. Metod dokazivanja na osnovu neto vrijednosti temelji se na posrednim dokazima i predstavlja primarni metod dokazivanja neprijavljenih i nezakonitih prihoda, koji se primjenjuje kada se ne može primijeniti metod istrage specifičnih stavki, ili kada nije moguć uvid u knjige ili evidencije, a očigledno je da osumnjičeni akumulira imovinu i sredstva.

U cilju što bolje prezentacije i razumijevanja cjelokupnog postupka primjene ovog metoda, preporučljivo je korištenja priloga u obliku tabelarnih prikaza i grafičkih priloga. Prilozima se objašnjava cijeli slučaj, a poželjno je da budu organizovani na takav način da služe postizanju određenog cilja, odnosno izračunavanju neprijavljenog ili nezakonitog prihoda. Prilozi se mogu koristiti i u pojedinim fazama krivičnog postupka, za bolje razumijevanje primijenjenih metoda i dokazivanje pojedinih činjenica relevantnih za krivični postupak.

4.10.6. Metod dokazivanja na osnovu troškova

Metod dokazivanja na osnovu troškova je posredan metod dokazivanja neprijavljenih ili nezakonitih prihoda i u osnovi je sličan metodu dokazivanja na osnovu neto vrijednosti[203]. Naime, oba metoda predstavljaju određene varijacije procedura koje izviru iz finansijske dokumentacije i računovodstva. Metod dokazivanja na osnovu troškova primjenjuje se kada pojedinac/osumnjičeni većinu svojih prihoda troši, tj. ima izražene potrošačke navike, dok se metod dokazivanja na osnovu neto vrijednosti, kao što sam već objasnio, primjenjuje kada pojedinac stiče/akumulira znatnu količinu imovine u određenom periodu.

Praktična primjena metoda dokazivanja na osnovu troška počinje procjenom stanja neto vrijednosti poreskog obveznika na početku poreskog perioda.[204] U tom smislu, on može posjedovati imovine/sredstava u rasponu od mnogo do ništa. Nakon što utvrdima imovinu pojedica/osumnjičenika ide se na slijedeči korak utvrđivanje troškova I prihoda pojedica/osumnjičenika za određeni period. Ukoliko u posmatranom periodu njegovi troškovi prelaze iznos prijavljenih prihoda, a njegova neto vrijednost krajem tog perioda ostane ista kao na početku može se zaključiti da su u njegovoj poreskoj prijavi (navedena primanja koja su nerealna, odnosno niža od stvarnih. Metod je prvi put primenjen u slučajevima poreza na prihode poreskih obveznika čija je osnovica bila gotovina, gde su poreski obveznici imali zakonit izvor sredstava (firmu ili platu) ili su bili bez vidljivih sredstava za život, dok se danas primenjuje kako za istragu slučajeva utaje poreza na prihod, tako i za finansijske istrage izvršenih krivičnih dela imovinskog kriminala. S obzirom da je reč o posrednom metodu dokazivanja, njegova primena dolazi u obzir kada[205]:

- osumnjičeni ne vodi poslovne knjige , evidencije i dokumentciju;
- knjige, evidencija i dokumentacija nisu dostupne;
- knjige , evidencija i dokumentacija nisu potpuni i ažurni;
- osumnjičeni onemogućava, zadržava ili ometa uvid u poslovne knjige , evidenciju i dokumentaciju.

Računovodstvo se bazira na koncepciji da je vrijednost imovine ili sredstava jednaka zbiru vrijednosti finansijskih obaveza i vlasničkog kapitala. Dokazivanje na osnovu neto vrijednosti zasniva se na promijeni vrijednosti vlasnikovog kapitala iz godine u godinu, podrazumijevajući utvrđivanje stanja na svakom od računa, te imovine i rashoda na kraju osnovne godine, kao i svih onih godina koje su pod istragom. Dokazivanje na osnovu troškova se primjenjuje kada se većina prihoda troši, umjesto da se sredstva akumuliraju, odnosno da se iskoriste za smanjenje finansijskih obaveza. Sredstva se, na primjer, mogu trošiti za nabavku droge, za putovanja, kupovinu poklona, kockanje, lične troškove života i sl. U slučajevima kada se u kriminalističkoj obradi uspješno dokažu svi zakoniti izvori prihoda, odnosno sredstava (uključujući kredite, poklone, nasljedstvo i dr.), ostaje samo jedan mogući izvor prihoda nezakonite djelatnosti.

---

[203] Vidi više George A.Manning,Ph.D.C.F.E.,E.A.Taylor&Francis Group,Boca Rata-London-Singapore, 2005:page 143-167).

[204] Vidi više James R.Richards,Transnatinal Criminal Organizations,Cybercrime,and Money Laundering CRC PRESS,Boca Raton-London-New York-washington,D.C. 1999: 215).

[205] James R.Richards,Transnatinal Criminal Organizations,Cybercrime,and Money Laundering CRC PRESS,Boca Raton-London-New York-washington,D.C. 1999: page 98.

[205] Vidi više George A.Manning,Ph.D.C.F.E.,E.A.Taylor&Francis Group,Boca Rata

Zahtjevi za primjenu metoda dokazivanja na osnovu troškova, koji se primjenjuju u američkom pravnom sistemu, slični su zahtjevima koji se odnose na primjenu metoda dokazivanja na osnovu neto vrijednosti. U slučajevima primjene metoda dokazivanja na osnovu troškova treba najprije, sa razumnom pouzdanošću, utvrditi početnu neto vrijednost imovine/sredstava osumnjičenog. Prilikom primjene ovog metoda ne moraju se prikazati tačni iznosi za svaki pojedini račun na strani prihoda i rashoda za osnovnu godinu, ili za godine koje su pod istragom. Međutim, treba uzeti u obzir sve račune sa kojih se mogu utvrditi podignuti novčani iznosi. Sljedeći korak je utvrđivanje vjerojatnog izvora viška sredstava. U istrazi treba predstaviti dokaze kojima se dokumentira da se u periodu na koji se istraga odnosi osumnjičeni bavio nekom nezakonitom djelatnošću. Dokazi uključuju i svjedočenja o umiješanosti osumnjičenog u nezakonite poslove. Zatim, veoma je važno da se provjere svi dokazi u slučajevima koji se ne odnose na konkretno krivično djelo, a dokazuju zakonite izvore sredstava osumnjičene osobe.

Metod dokazivanja na osnovu troškova zasniva se na posrednim dokazima, tako da će, ukoliko se ne uračuna neki oblik zakonitog izvora sredstava, to uticati na vjerodostojnost rezultata do kojih se dođe njegovom primjenom. Osnov ove metode je upoređivanje izvora imovine/sredstava sa njihovim korištenjem, pri čemu treba napomenuti da postoji više različitih izvora imovine/sredstava osumnjičene osobe tokom godine. U slučajevima kada se vrijednost imovine/sredstava smanjuje, to može da znači da su imovina, odnosno sredstva pretvoreni u gotovinu. Također, kada postoji povećanje finansijskih obaveza (rashodi), to znači da su od finansijskih ustanova, pojedinaca ili drugih osoba uzimana novčana sredstva na kredit, koja su zatim polagana na neki drugi račun ili su potrošena.

Imovina/sredstva mogu biti zakoniti ili nezakoniti, odnosno oporezivi ili neoporezivi. Specifični podaci koji se odnose na imovinu/sredstva mogu ukazati na smanjenje imovine, povećanje rashoda i zakonite prihode. Smanjenje imovine podrazumijeva umanjenje gotovog novca, stanja na bankovnim računima, zaliha, stanja na računima potraživanja, u opremi i drugo. Povećavanje finansijskih obaveza/rashoda može biti prouzrokovano povećanjem glavnica kredita, povećanjem računa dospjelih na naplatu i drugo. Zakoniti prihodi mogu biti plate, poslovna dobit, iznajmljivanje nekretnina, dobit na osnovu prodaje lične imovine, pokloni, nasljedstvo, isplate polisa osiguranja i krediti. Trošenje sredstava označava novac koji je osumnjičena osoba potrošila za godinu dana. Povećanje imovine, smanjivanje finansijskih obaveza i lični životni troškovi zahtijevaju trošenje akumuliranih sredstava ili ostvarene dobiti. Sredstva se mogu trošiti za različite namjene, a najčešće je to povećanje imovine, smanjenje finansijskih obaveza, lični životni troškovi, gubici na prodaji imovine i slično. Povećanje imovine se najčešće odnosi na povećanje sredstava, stanja na bankovnim računima, uvećanje zaliha, potraživanja, poslovnu opremu, nekretnine i ličnu imovinu. Smanjenje finansijskih obaveza uglavnom se odnosi na smanjenje plativih računa i otplatu glavnica kredita.

Postupak analize troškova odvija se u tri osnovne faze. Prva obuhvata svrstavanje/razvrstavanje svih transakcija u kategoriju upotreba/trošenje ili izvora sredstava. Druga podrazumijeva utvrđivanje ukupnih troškova i poznatih izvora sredstava za svaku godinu koja je predmet istrage. U trećoj se od ukupnih troškova za posmatrani period oduzimaju ukupni poznati izvori sredstava, te dobiva vrijednost neprijavljene ili nezakonite dobiti. U tom smislu, formula za analizu troškova glasi:

Nd (Neprijavljena ili nezakonita dobit) = **Ut** (Ukupni troškovi) –**Upi/Up** (poznati izvori sredstava/prihoda)[206]

I metod dokazivanja na osnovu troškova zasniva se na posrednim dokazima. Riječ je o primarnom metodu dokazivanja nezakonitih prihoda i neprijavljenih oporezivih prihoda, koji se primjenjuje kada organu za provođenje zakona I tužiocu ne stoje na raspolaganju dokumentacija, evidencija ili poslovne knjige, dok osumnjičena osoba nekontrolisano troši sredstva i ne akumulira/uvećava imovinu. U takvim slučajevima treba uporediti potrošene vrijednosti sa poznatim izvorima sredstava.

Prvo se mora utvrditi polazna tačka, zatim ukupne troškove i vjerovatan izvor i visinu prihoda, a potom treba istražiti finansijske tragove i navode osumnjičenog, kako bi se došlo do relevantnih informacija. Preporučljivo je koristiti grafičke i tabelarne prikaze finansijskih informacija u pojedinim fazama krivičnog postupka, kako bi se bolje razumjele primijenjene metode i lakše dokazale činjenice relevantne za krivični postupak.

Napomena edukatorima

Na praktičnim primjerima prezentirati dobre i manje dobre strane svakog od navedenih metoda finansijske istrage. U okviru tog zadatka pokušati formirati timove kojim bi rukovodili tužioci.Zadatak tih timova bi bio da sačine plan provođenja istrage, vrstu materijalnih dokaza koje se trebaju prikupiti, lični dokazi i njihovo značenje, mjesta na kojima se ti dokmenti nalaze, značenje prikupljenih materijalnih dokza, način njihove analize, tumačenje i prezentacija dobivenih rezltata, sačinjavanje finsalnog izvještaja i predlaganje daljih mjera tužiocu.

4.11. Zakonski osnovi za primjenu metoda finansijske istrage u bosanskohercegovačkom zakonodavstvu

U okviru sadašnjeg državnog i nedržavnog krivično-procesnog zakonodavstva ne postoje smetnje da se finansijska istreaga provedu po sva tri navedena načina/metoda. Tvrdnju temeljimo na sadržaju odredaba člana Finansijska istraga se u procesnom smislu temelji na odredbama člana 35.,197. i 392[207]. Zakona o krivičnom posatupku BiH na kojima se temelji finansijska istraga u procesnom smislu.

4.12. Intervju/uzimanje izjava kao podrška u vođenju finansijske istrage

Radi izvršenja zadataka iz člana 218[208]. (Zakona o krivičnom postupku BiH), ovlaštena službena osoba može prikupljati izjave od osoba. Pri prikupljanju izjava od osoba, ovlaštena službena osoba će postupiti u skladu nsa članom 78.[209] odnosno u skladu sa članom 86.[210]

[206] George A.Manning,Ph.D.C.F.E.,E.A.Taylor&Francis Group,Boca Rata-London-Singapore, 2005:page 98).

[207] Zakon o krivičnom postupku Bosne i Hercegovine ("Službeni glasnik BiH",broj 3/03, 32/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08,58/08,12/09,16/09, 93/09).,

[208] Zakon o krivičnom postupku Bosne i Hercegovine ("Službeni glasnik BiH",broj 3/03, 32/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08,58/08,12/09,16/09, 93/09).,

[209] Zakon o krivičnom postupku Bosne i Hercegovine ("Službeni glasnik BiH",broj 3/03, 32/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08,58/08,12/09,16/09, 93/09).,

[210] Zakon o krivičnom postupku Bosne i Hercegovine ("Službeni glasnik BiH",broj 3/03, 32/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08,58/08,12/09,16/09, 93/09).,

ZKP BIH. U tom slučaju se zapisnici o prikupljenim izjavama mogu upotrijebiti kao dokazi u krivičnom postupku.

Iz sadržaja navedenih odredbi se da zaključiti da je uzimanje izjava (u nastavku teksta intervju) od osoba veoma važan dio kvalitetne krivične i finansijske istrage koji je neophodno temeljito i kvalitetno planirati, pripremiti i realizirati. Intervju treba provoditi profesionalno i sa visokim stepenom formalnosti. Intervju u pravilu počinje sa jasnim i preciznim opomenama i upozorenjima koje osobi koja se intevijuiše, u smislu sadržaja odredaba člana 86. st.1., daje ovlašteno službeno lice. Nakon toga slijedi identifikacija osobe i identifikacija predmeta. Veoma je bitno da ovlaštena službena osoba snima cijeli tok intervjua audio,a po mogućnosti i audio-vizuelnim sredstvima jer bi ti snimci mogli biti od veoma velike koristi za analizu intervjua i dalje razvijanje slučaja kao i u sudskom postupku kao podsjećanje svjedoka na sadržaj njihove izjava u toku postupka.Također,ovlaštena službena osoba je dužna da uz predhodnu autorizaciju tužioca intervjuisati svakog svjedoka koji je povezan sa slučajem koji je predmet krivične odnosno finansijske istrage.Dosadašnja terorija,i praksa je izdiferencirala je tri vrste svjedoka: (1) prijateljski (2) neutralni (3) nerijateljski svjedok. (1) Prijateljski/kooperativni svjedok je svjedok koji je više nego voljan da daje informacije i on je najčešće i žrtva. Međutim kooperativni svjedok ne iznosi samo činjenice nego ih nerijetko mješa sa svojim neobjektivnim mišljenjem. Prijateljske svjedoke treba ocjenjivati veoma pažljivo. Oni možda i nisu pogodni svjedoci zbog predrasuda ili nedostatka objektivnosti. (2) Neutralni svjedoci u pravilu nemaju nikakav ili veoma mali interes za slučaj. Iako oni mogu dati najbolje svjedočenje oni uvijek ne pružaju sve neophodne činjenice i dokaze o slučaju. Mnogi od njih nikada nisu videjeli subjekt i ponekad imaju teškoće u pronalaženje dokaza koje posjeduju, a relevantni su za slučaj.

(3) Neprijateljski svjedok je veoma težak za intervijusanje. Svjedok koji u pravilu ne govori istinu ili postaje nekoopertivan može indicirati nepoštene namjere ili usku povezanost sa predmetom istrage.

Pravilno planiranje intervjua je veoma bitno. Ovlaštena službena osoba-ispitivač mora imati generalnu ideju o onome što svjedok zna, ono što može pružiti i njegova veza sa subjektom. Prije svakog intervjua ispitivač treba da pregleda sve informacije i podatke koji se oednose na slučaj. Takve informacije se mogu podijeliti na tri opšte kategorije:

1. informacije koje se mogu dokumentovati, a o kojima je potrebno razgovarati ,
2. informacije koje je moguće dokumentovati, ali je potrebno o njima razgovarati,
3. informacije koje se moraju razvijati kroz svjedočenje.[211]

Ispitivač treba da pripremi "registrator" koji sadrži dokumentaciju, podatke I /ili informacije koje su složene redoslijedom kojim će se odvijati intervju. Ispitivač treba da odredi svrhu ili cilj ispitivanja i to pretoči u tzv. razgovornik. Razgovornik bi treba da sadrži samo onu informaciju koja je relevantna i materijalna uključujući i rekla-kazala informacije. Važne teme treba istaći ,a srodne teme postaviti u pravilan i logičan slijed. Ispitivač bi trebao da tzv. specifična pitanja svede na minimum jer ona mogu reducirati fleksiblinost ispitivača, svjedoka i osumnjičenog. Ispitivač treba da pokrije što je moguće više informacija. Razgovornik intervjua treba da obuhvati minmalno:

[211] George A.Manning,Ph.D.,C.F.E.,E.A.FINANCIAL INVESTIGATION and FORENSIC ACCOUNTING (Second Edition),Taylor&Francis Group,Boca Ration,London,Singapur,2005.p.372

1. Veza (vrsta i intenzitet) svjedoka sa subjektom/osumnjičenim,
2. Sve eventualne sastanke,e-mail poruke, telefax, sms, mms i telefonske i druge kontakte sa subjektom/osumnjičenim,
3. Dokumenti koji se odnose na poslovne aktivnosti osumnjičenog,
4. Identifikaciju svih ostalih potencijalnih svjedoka,
5. Finansijsko poslovanje pravnih lica sa kojima je vlasnički poveza osumnjičeni,
6. Finansijske transakcije koje su vezana osumnjičenog, posebno one koje su identificirane kao suspektne,
7. Informacije o historiji/prošlosti i pozadini osumnjičenog,
8. Sve ostale relevantne materijalne ili lične informacije ili dokaze[212].

4.12.1. Tehnika i taktika vođenje intervjua

U toku intervjua ispitivač morate biti u stanju da shvati svaku informaciju bez obzira na njenu prirodu I treba biti spreman da je razvijete u cjelosti. Ako ispitivač nije fleksibilan možete potrošiti puno vremena I postaviti brojna nepotrebna pitanja što može rezultirati obimnom izjavom sa malo ili bez ikakve vrijednosti. Iako se može učiniti da je jednostavnije da se ispitivač pridržava fiksnog modela intervjuiranja ili da se oslanjate na serije pitanja ili tema , rigidno pridržavanje bilo kojim zabilješkama ili razgovorniku će ozbiljno umanjiti fleksibilnost. Razgovornik ili podsjetnik treba da posluži samo kao vodič, a ne kao zamjena za originalno i spontano postavljanje pitanja.

Pažljivo planirani razgovornik intervjua će pružiti dovoljno prostora kako bi ispitivač imao mogućnost da se bolje nosi sa situacijom koja se može desiti. Uspostavljanje dobre komunikacije ispitivača sa svjedokom u toku inicijalnog intervjua je esencijalno jer pruža mogućnost dobivanja informacije koja mu možda ne bi bila dostupna kasnije.

Vješti ispitivač vodi intervju tako da dobije što je moguće više informacija. Ispitivač potiče svjedoka da razgovara o sebi, svojoj porodici, hobijima, finansijskoj historiji i odnosima sa drugim uključujući subjekt istrage. Poslije inicijalnog kontakta neki svjedoci mogu postati manje komunikativni stoga ispitivači I njihovi rukovodioci treba planiraju i vode inicijalni intervju tako da dobiju što je moguće više informacija. Ispitivač treba pustiti svjedoka da govori;Ispitivač treba budite dobar slušalac.

Očigledna činjenica koja se odnosi na intervjuiranje da ono podrazumijeva komunikaciju između dvije ili više osoba. To je posebna profesionalna vrsta konverzacije koja zahtijeva sva sredstva I instrumente dobrog govora i komunikacije. Tehnike treba da budu razvijene tako da navode svjedoke da odgovaraju na željena pitanja. Ispitivač treba da stekne jasnu predodžbu o stilu života I finansijskim operacijama svjedoka i/ili osumnjičenog. Izjave koje su dali svjedok ili osumnjičeni se kasnije mogu koristiti kao test njihove istinitosti i tačnosti. Ispitivač treba da je uvijek spreman na indikacije prevare od strane svjedoka ili subjekta. Svjedoci ili osumnjičeni su mogli imati neobično dobru ili lošu sreću u životi i/ili biznisu ,ispitivač im treba dozvolite da nesmetano razgovaraju o svojim pogreškama ili uspjesima. Ispitivač treba nastaviti sa postavljanjem pitanja sve dok ne dobije sve informacije koje je realno očekivao.

[212] George A.Manning,Ph.D.,C.F.E.,E.A.FINANCIAL INVESTIGATION and FORENSIC ACCOUNTING (Second Edition),Taylor&Francis Group,Boca Ration,London,Singapur,2005.p.372i 373.

Neki od prijedloga koji slijede će vjerovatno pomoći ispitivaču da dobije potpune I tačne odgovore u toku intervjua.

1. Koristite kratka pitanja koja se odnose na jednu temu koja su mogu jasno I jednostavno razumjeti.
2. Postavljajte pitanja koja zahtijevaju narativne odgovore;izbjegavajte "da" I "ne" odgovore kad god je to moguće;
3. Pitajte svjedoka kako zna da je ono što navodi činjenica;
4. Od subjekta se također može tražiti da pruži činjeničnu osnovu za bilo koji zaključak koji je naveden;
5. Kad god je to moguće izbjegavajte pitanja koja sugeriraju dio odgovora-vođena pitanja;
6. Budite spremni da spriječite svjedoka da besciljno luta u odgovorima. Gdje god je to moguće zahtijevajte direktan odsgovor.
7. Spriječite svjedoka da¸vas udalji od teme.Nemojete dozvoliti svjedoku da vas zbuni odgovorima ili da nedodgovori na neka od osnovnih pitanja;
8. Koncentrirajte se više na odgovore nego na slijedeća pitanja;
9. Da bi ste izbjegli nepotpunu I nevezanu hronologiju, treba da jasno razmijete svaki odgovor i da svaku nejasnoću eliminirate prije nego što nastavite;
10. Kada su sve važne tačke riješene prekinite intervju; ako je moguće ostavite vrata otvorena za slijedeće sastanke.

Svjedok ili subjekt treba da u potpunosti odgovore na slijedeća osnovna pitanja :

1. *Ko.* Treba napraviti potpunu identifikaciju svih osoba kojim se obraćao i sa kojima je bio u kontaktu u vezi sa slučajem. Ovo podrazumijeva opis, adresu, državljanstvo, nadimak, reputacija I saradnici;
2. *Šta*. Potpune detalje koji se odnose na ono što se desilo odnosno dešavalo. Pitanja treba da se odnose na događaje, metode I sisteme. Treba dobiti potpun odgovor. Pratiti svaki bitan poslovni ili drugi događaj od njegovog nastanka do završetka.
3. *Gdje*. Kompletne pojedinosti koje se odnose na finansijsku dokumentaciju, evidencije,poslovne knjige I finansijske izvještaje I poslove, uključujući njihovu lokaciju, klijente, svjedoke, kupci, dobavljače I sl.

4.13. Posebne istražne radnje kao podrška finansijskoj istrazi

U postupku finansijske istrage poseban značaj ima primjena posebnih istražnih radnji koje zbog specifičnosti finansijske istrage i teškoća u prikupljanju materijalnih I ličnih dokaza zauzima posebno mjesto. Posebne istražne radnje kojima se privremeno ograničavaju ustavna prava i slobode građana radi pribavljanja saznanja i dokaza važnih za krivični postupak, koristan su instrument u borbi protiv najtežih oblika kriminala. Posebne istražne radnje su u krivičnoprocesnom zakonodavstvu situirane kao posebno sredstvo koje se mogu koristiti protiv osoba za koje postoji sunja da je sama ili sa drugim osobama učestvovala ili učestvuje u učinjenju krivičnog djela iz člana 117[213]. Zakona o krivičnom postupku BiH, ako se na drugi način ne mogu pribaviti dokazi ili bi njihovo prikupljanje bilo povezano sa nesrazmjernim teškoćama. Posebne istražne radnje predviđene u krivičnoprocesnom zakonodavstvu Bosne i Hercegovine su:

[213] Zakon o krivičnom postupku Bosne i Hercegovine ("Službeni glasnik BiH",broj 3/03, 32/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08,58/08,12/09,16/09, 93/09).,

1. nadzor i tehničko snimanje telekomunikacija,
2. pristup kompjuterskim sistemima i kompjutersko sravnjenje podataka,
3. nadzor i tehničko snimanje prostorija,
4. tajno praćenje i tehničko snimanje osoba, transportnih sredstava i predmeta koji stoje u vezi s njima,
5. korištenje prikrivenih istražitelja i korištenje informatora,
6. simulirani i kontrolisani otkup predmeta i simulirano davanje potkupnine, i
7. nadzirani prevoz i isporuka predmeta krivičnog djela.

4.13.1. Nadzora i tehničkog snimanja telekomunikacija

Ono što karakteriše sve posebne istražne radnje pa tako posebnu istražnu radnju nadzora i tehničkog snimanja telekomunkacija jeste tajnost, odnosno odvijanje istražne radnje prema osumnjičenom bez njegovog znanja.Ovom komunkacijom može biti obuhvaćena sva komunikacija osumnjičenog ili lica za koju postoje osnovi sumnje da učiniocu, odnosno od učinioca krivičnog djela prenosi informacije u vezi s krivičnim djelom, odnosno da počinitelj koristi telekomunikacijsko sredstvo te osobe, izuzev komunikacije osumnjičenog sa svojim braniocem. Ova posebna istražna radnja vrši se presretanjem komunikacije u momentu dok komunikacija još uvijek traje. U pogledu samog sadržaja dokaza pribavljenih posebnim istražnim radnjama nadzora i tehničkog snimanja telekomunikacija on uglavnom predstavlja razgovor putem sredstava telekomunkacija , koji se može odvijati kako u vrijeme izvršenja krivičnog djela tako I prije i poslije izvršenja krivičnog djela.

Suštinski, po pravilu osumnjičeni je primjenom ove posebne istražne radnje dokaz sam protiv sebe, odnosno posebna istražna radnja nadzora i tehničkog snimanja telekomunikacija za rezultat ima komunikaciju osumnjičenog koja je povezana sa izvršenjem krivičnog djela a koja se može odvijati, prije, u toku i poslije izvršenja krivičnog djela, a koja osumnjičenog dovodi u vezu sa izvršenjem krivičnog djela koje je predmet istražnog postupka.

Karakteristika ove posebne istražne radnje je da se izvodi u realnom vremenu odnosno u stvarnom vremenu odvijanja komunikacije *(tzv. real time ili on line nadzor*), odnosno ova posebna istražna radnja vrši se presretanjem komunikacije u momentu dok komunikacija još uvijek traje, za razliku od klasičnih radnji dokazivanja koje se po pravilu izvode sa vremenskom distancom u odnosu na predmet dokazivanja.

Vrsta telekomunikacije koja se može nadzirati i snimati ničim nije ograničena, međutim najšešće se radi o fiksnoj telefoniji i uređajima koji koriste GSM mreže mobilne telefonije (mobilni telefoni), mada bi ovom posebnom istražnom radnjom mogli biti nadzirani i uređaji satelitske telefonije te svakog drugog oblika telekomunikacije.

Prije predlaganju primjene ove posebne istražne radnje sudiji za prethodni postupak od strane tužioca na način kako je to utvrđeno sadržajem odredaba člana 118[214]. preporučujemo, da se ukoliko okolnosti dozvoljavaju, korištenjem mogućnosti koje daju odredbe člana 72[215]. ZKP BIH prethodno,od operatora telekomunikacija ili drugog pravnog lica koje vrši pružanje telekomunikacionih usluga, pribave podaci o korištenje telekomunikacijskih usluga za lice iz

[214] Zakon o krivičnom postupku Bosne i Hercegovine ("Službeni glasnik BiH",broj 3/03, 32/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08,58/08,12/09,16/09, 93/09).,
[215] Zakon o krivičnom postupku Bosne i Hercegovine ("Službeni glasnik BiH",broj 3/03, 32/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08,58/08,12/09,16/09, 93/09).,

člana 116. st.1.[216] i uz pomoć analitičara i analitičkog softvera analiziraju. Također,veoma je bitno da se postupak analize telekomunikacijskih usluga nastavi I dok traje primjena ove posebne istražne radnje.

Taktički osmišljenim korištenjem ove posebne istražne radnje mogu se prikupiti značajne informacije o kriminalnoj djelatnosti osobe I kriminalne organizacije kojoj pripada na temelju kojih se stvara cjelokupna slika njihovog kriminalnog djelovanja. Ova posebna istražna radnja se u pravilu kombinuje sa drugim radnjama zavisno od vrste kriminalne djelatnosti, kriminalne reputacije i profila kriminalne grupe i njenih članova.

4.13.2. Pristup kompjuterskim sistemima i kompjutersko sravnjenje podataka

Pristup kompjuterskim sistemima i kompjutersko sravnjenje podataka posebna je istražna radnja kojom se dolazi do podataka, odnosno dokaza važnih za krivični postupak, i to „upoređivanjem ličnih podataka građana koji su obrađeni u odgovarajućim bazama/bankama podataka s podacima i registrima koji se nalaze u okviru policijskih evidencija“. Posebna istražna radnja pristup kompjuterskim sistemima i kompjutersko sravnjenje podataka je radnja koja se do sada nije koristila u krivično-sudskom postupku Bosne i Hercegovine od strane tužilaca i agencija za provođenje zakona.

Inače, ova specijalna istražna tehnika se sastoji u automatskom (kompjuterizovanom) pretraživanju identifikacionih podataka određenih lica, koji imaju indicijalni značaj, odnosno sužavaju krug osumnjičenih ili upućuju na eventualnog učinioca krivičnog djela. Tzv.„Raster pročešljavanje“ je korištenje podataka koji se nalaze u privatnim ili javnim bazama/bankama podataka prema unaprijed utvrđenim kriminalističkim kriterijumima (rasteri) u cilju otkrivanja osumnjičenog i pronalaženja drugih lica i predmeta. Povezivanjem različitih baza/banaka podataka, stvaranjem integralnih sistema podataka otvara se i mogućnost pristupanja informacijama različite prirode (nekretnine,udjeli u pravnim licima, zdravstveno osiguranje, poresko stanje, bankovni računi, vojna obaveza, sudski postupci i slično) o građanima i stvaranje kompletne slike o njihovoj ličnosti. Uobičajena forma ove radnje je upoređivanje dostupnih podataka putem automatske obrade sa postojećim podacima ili sa novim podacima koji su nastali programskim pročešljavanjem.

U praksi se razlikuju dvije vrste upoređivanja podataka, negativno i pozitivno. Kod negativnog, dolazi do brisanja polaznog podatka ako se pokaže neka konvergencija u odnosu na podatak sa kojim se vrši upoređivanje, odnosno doprinosi eliminaciji određenih lica iz kruga osumnjičenih automatizovanim pretragama kroz policijske, administrativne i druge evidencije.

U slučaju pozitivnog upoređivanja, stvara se novi podatak na osnovu pronađenih podudarnih podataka, odnosno utvrđivanje kruga osumnjičenih lica na osnovu određenih karakteristika, činjenica ili sposobnosti, koje su zapažene kod nepoznatog učinioca krivičnog djela.

„Raster programom“ se utvrđeni podaci mogu dalje dorađivati i upotpunjavati sa drugim „raster programima“, što služi sužavanju kruga sumnjivih lica. Metod „raster pretraga“ bi po mom sudu unio novi kvalitet u kriminalistički rad, jer se aktivnosti usmeravaju na veliki broj lica koja nisu klasičnim metodama rada policije osumnjičena za izvršeno krivično djelo. Iz

[216] Zakon o krivičnom postupku Bosne i Hercegovine (“Službeni glasnik BiH”,broj 3/03, 32/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08,58/08,12/09,16/09, 93/09).,

prikupljene mase podataka bi osumnjičeni bili izdvojen tek nakon pribavljanja podataka koji ukazuju na indicije u vezi sa žrtvom i/ili predmetima, posredno na učinioca ili na neke okolnosti konkretnog slučaja. S obzirom da se u pravilu radi o obradi ogromnog broja podataka, koji se klasičnim radom policije ne bi ni mogli iskoristiti. „Raster pretraživanja“ su apstraktne prirode i prethode radu usmjerenom na određeno lice. Suštinu ove specijalne istražne tehnike predstavlja omogućavanje slobodnog pristupa policije svim evidencijama, koje se vode automatizovano, što opet odudara od načela zaštite prava na privatnost građana i informatičko samoodređenje.

4.13.3. Nadzor i tehničko snimanje prostorija i tajno praćenje i tehničko snimanje osoba, transportnih sredstava i predmeta koji stoje u vezi sa njima

.

Nadzor i tehničko snimanje prostorija kao posebna istražna radnja ima za krajnji cilj prikupljanje podataka o komunikacijama u određenom prostoru, neovisno od oblika u kojem se one ostvaruju (pisani, zvučni, itd.).U ovu posebnu istražnu radnju spadaju i optičko i akustično snimanje određenog prostora , te dakako aktivnosti koje se u nadziranom prostoru odvijaju, cyber napada na banke, pranja novca poput davanja i primanja mita i sličnih kriminalnih aktivnost.

Tajno praćenje i tehničko snimanje osoba i predmeta “posebna je vrsta kriminalističke opservacije“. *Ratio* upotrebe ove prikrivene posebne istražne radnje jeste prikupljanje podataka o kretanju osoba I transportnih sredstava koje su predmetom nadzora I snimanja, kontaktima koje one ostvaruju, njihovom snimanju radi osiguranja dokaza u postupku, kao i u prikupljanju podataka o postupanju s određenim predmetima. I ova radnju je poželjno kombinirati sa drugim posebnim istražnim radnjama kao što su nadzor i tehničko snimanje telekomunikacija, korištenje prikrivnih istražitelja i korištenje informatora i simulirani i kontrolirani otkup predmeta i simulirano davanje potkupnine. Krimninalne organizacije najčešće anagažuju finansijske i pravne eksperte kao i eksperte za informaciono-komunikacione tehniologije koji svoja znanja koriste da bi olakšali ostvarivanje krajnjeg cilja: onemogućavanja povezivanja nelegalno stečene imovine sa njihovim pravim izvorom. Složene sheme pranja novca sadrže transnacionalne elemente koji podrazumijevaju kretanje “prljavog” novca preko granica više zemalja uglavnom elektronskim transferom. Ove i slične aktivnosti kriminalnih organizacija obavljaju se strogo poštujući princip tajnosti, informacije korisne za finansijsku istragu mogu se pribaviti samo od neposrednih učesnika tih aktivnosti.

4.13.4. Korištenje prikrivennih istražitelja , korištenje informatora , simulirani i kontrolirani otkup predmeta i simulirano davanje potkupnine

Ova posebna istražna radnja je, pored posebne istražna radnja nadzora i tehničkog snimanja telekomunikacija, do sada najeksploatisanija i obzirom na njenu kompleksnost u primjeni i rizike koji su evidentni u njenoj primjeni neophodno ju je napokon početi primjenjivati u duhu nedavno izmijenjenih odredaba člana 116. stav 6.[217]koji glasi ”Prikriveni istražitelj je posebno obučeno ovlašteno službeno lice koje istražuje pod izmijenjenim identitetom. Prikriveni istražitelj smije pod svojim izmijenjenim identitetom učestvovati u pravnom prometu. Ukoliko je to neophodno za formiranje i održavanje identiteta, mogu se izraditi, izmjeniti ili koristiti odgovarajući dokumenti.

[217] Zakon o krivičnom postupku Bosne i Hercegovine (“Službeni glasnik BiH”,broj 3/03, 32/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08,58/08,12/09,16/09, 93/09).,

Prikriveni istražitelj je policijski službenik, koji djeluje tajno ili prikriveno, koji se sa promijenjenim identitetom nastoji uključiti u kriminalnu sredinu, te obavještavati o svim njezinim kriminalnim aktivnostima koje su od značaja za buduće uspješno vođenje krivičnog postupka. Npr. pri razjašnjavanju i dokazivanju krivičnog djela pranja novca značaj primjene ove posebne istražne radnje ogleda se u mogućnosti da se dođe do informacija:

- ✓ Načinu sticanja prljavog novca;
- ✓ Načinu iznošenja novca iz zemlje,
- ✓ Poslovi I imovina u koje se novac ulaže,
- ✓ Bankama I firmama koje koriste kriminalne organizacije u procesu pranja novca,
- ✓ Korumpiranim bankarskim , državnim I policijskim službenicima koji pomažu ovu aktivnost,
- ✓ Finansijskim ICT i pravnim ekspertima i drugim licima koja su uključeni u aktivnosti kriminalne organizacije koja se bavi pranjem novca.

Navedene informacije omogućile bi praćenje finansijski tragova kriminalnih organizacija, identifikovanje učesnika, pronalaženje i oduzimanje krivičnim djelom stečenih sredstava čime se podriva ekonomska moć kriminalnih organizacija.

Opravdanost upotrebe ovog oblika istraživanja, po mom mišljenju ne leži toliko u mogućnosti svjedočenja ovakvog službenika u glavnom dijelu krivičnog postupka, nego ponajprije u stvaranju osnova i smjernice za poduzimanje kriminalističkih, odnosno vanprocesnih aktivnosti. Obzirom da je upotreba prikrivenih istražitelja kompleksan, ozbiljan pothvat, koji zahtijeva kvalitetnu i temeljitu pripremu i nerijetko nosi određeni stupanj opasnosti za onoga koji nastupa u ulozi prikrivenog istražitelja.

Simulirani otkup posebna je istražna radnja koja pogodna za otkrivanje koruptivnih krivičnih djela i krivičnih djela nedopuštene trgovine, neovlaštenog prometa opojnim drogama, itd i uglavnom je realiziraju prikriveni istražitelj uz pomoć informanta. Sastoji se u kupovanju predmeta koji su na bilo koji način povezani sa krivičnim djelom. Za krivična djela za koje je karakterističan visok stupanj tajnovitosti, poput korupcije, čija je daljnja značajka i poseban savez i dogovor počinitelja (i podmititelju i podmićenom dakako da nije u interesu da se sazna za korupcijsku aktivnost), simulirano davanje potkupnine je iznimno značajan i vrijedan istražni postupak. Složenost simuliranog davanja mita se reflektira i u činjenici da je za uspješno izvođenje ove aktivnosti nužno osigurati označene predmete koje su objektom nezakonite transakcije (najčešće, ali ne isključivo, su to novčanice), jer je u protivnom mogućnost pribavljanja fizičkih dokaza (raspolaganje i posjed označenim novčanicama) slaba ili nikakva.

4.13.5. Nadzirani prijevoz i isporuka predmeta krivičnog djela

Kod posebne istražne radnje nadziranog prijevoza i isporuke predmeta krivičnog djela tajno se nadzire prijevoz i isporuka naznačenih predmeta s ciljem otkrivanja svih sudionika (posebice organizatora) nezakonitih/kriminalnih aktivnosti. Posebne istražne radnje simuliranog otkupa predmeta i simuliranog davanja potkupnine te nadziranog prijevoza i isporuke predmeta krivičnog djela ne smiju se izvršavati tako da predstavljaju podstrekavanje na počinjanje krivičnog djela.

U tom slučaju ne vrijedi razlog isključenja protupravnosti, odnosno, npr. onaj ko bi utjecao na stvaranje odluke za primanje mita, riskirao bi da bude krivično odgovoran za sudjelovanje

u počinjenju krivičnog djela primanja mita. Ovo s druge strane isključuje i osnovu za krivični progon podstrekavane osobe za krivično djelo izvršeno u vezi s radnjom podstrekavanja. Ova praktična mogućnost i zamka zbog svoje senzitivnosti i značajnosti u smislu odvraćanja treba da je posebno I u svakom konkretnom slučaju markirana.

4.14. Kako tumačiti i koristiti rezultate finansijske istrage

U praksi je moguća više varijacija dobivenih rezultata profesionalno korektno provedene finansijske istrage podržane ili ne intervjuima i primjenjenim posebnim istražnim radnjama Stoga je veoma bitno da ovlaštena službena lica/istražitelji koji su proveli finansijsku istragu, tužiocu kroz izvještaj i prikupljene dokaze i kroz predhodna i/ili naknadna objašnjenja na razumljiv, koncizan i prihvatljiv način prezentiraju rezultate finansijske istrage.

Radi pravilnog tumaćenja i daljeg efikasnog i efektivnog korištenja rezultata finansijske istrage u daljem postupku pred sudom nephodno je da tužilac sa ovlaštenim službenim osobama u toku i nako provedene finansijske istrage razjasni svaki specifični detalj koji se odnosi na finansijsku istragu i sa ovlaštenim službenim licima sačini taktiku prezentiranja rezultata finansijske istrage i dokaza koji su tom prilikom prikupljeni.

Ukoliko je nephodno, izvještaj ovlaštene službene osobe treba da sadrži i prijedloge za pokretanje privremenih mjera oduzimanja imovine ,mjeru zaplijene ili drugu nephodnu mjeru kako bi se spriječilo njeno korištenje, otuđenje ili raspolaganje.Također,ovlaštena službena osoba će uvijek kada postoji opasnost od odlaganja, privremeno oduzeti imovinu koja se ima oduzeti po KZ BiH, zaplijenti imovinu ili poduzeti druge nephodne privremene mjere kako bi se spriječilo bilo kakvo korištenje,otuđenje ili raspolaganje tom imovinom u skladu sa zakonom[218].

4.15. Modeli međunarodna suradnja u postupcima oduzimanja prihoda/imovine stečenih krivičnim djelima

Nastajanje, razvoj i jačanje organizovanog kriminala u međunarodnim okvirima podrazumijeva razvoj efikasnih modaliteta međunarodne saradnje u toku krivične i finansijske istrage i postupka oduzimanja prihoda stečenih kriminalom. Dokument *Grupe za finansijske akcije-Četrdeset preporuka* u sadržaju preporuke 7. ukazuje na potrebu da države usvoje mjere koje će omogućiti svojim kompetentnim nadležnim institucijama da konfiskuju imovinu/prihod stečen kriminalom.

Takve mjere bi trebalo da uključe ovlaštenja za (1) identifikaciju, praćenje i evaluaciju imovine koja podliježe konfiskaciji (2) poduzimanje privremenih mjera kao što su zamrzavanje i pljenidbu radi sprječavanja bilo kakve prodaje, prenosa ili oslobađanja od takve imovine (3) poduzimanje svih adekvatnih istražnih radnji.

Navedeni vid međunarodne saradnje najčešće se razvija u obliku pomoći u istrazi,zajedničkim istragama i posebne istražne radnje, pomoći u zamrzavanju odnosno privremenom oduzimanju prihoda stečenih kriminalom i pomoći u trajnom oduzimanju, vraćanju ili razmjeni nelegalno stečene imovine koja se nalazi u drugoj državi.

[218] Vidi Zakon o krivičnom postupku BIH,član 72.

4.15.1. Pomoć u istrazi

Pomoć u istrazi ima za cilj pronalaženje i obezbjeđenje dokaza o postojanju porijeklu, transformaciji, miješanju (sa legalnim sredstvima) prebacivanju, razmjenjivanju, lokaciji, pravnom statusu i vrijednosti prihoda stečenih kriminalom.

Za sve navedene činjenice potrebno kroz međunarodnu saradnju na zakonit način osigurati pravno valjane dokaze. Pored prihoda od kriminala koji može biti u različitim oblicima (nekretnine, pokretne stvari, oprema, hartije od vrijednosti, novac i ekvivalenti novcu i sl.) od materijalnih dokaza veoma je važna dokumentacija i evidencije koje omogućavaju praćenje finansijskog traga koji ostavljaju aktivnosti organizovanog kriminala. Za praćenje finansijskog traga potrebno je vraćanje operativne aktivnosti unazad i rekonstrukcija poslovno-finansijskih aktivnosti organizovanog kriminala za što je potrebna različita dokumentacije (dokumentacija o kupovini nekretnina, pokretnih stvari, potvrde mjenjačnice o zamjeni valute, finansijske I revizorske izvještaje, nalozi za međubankarske transfere , nalozi za elektronskih transfera novca, nalozi za isplatu I uplatu, ugovor o posjedovanju sefova, ugovori o sklapanju različitih pravnih poslova, bankarski izvodi i dokumentacija za sve vrste računa, poslovna korespondencija koja uključuje primljene I proslijeđene e-mailove sa identificiranih IP adresa i dr.) i evidencija (podaci o vlasništvu nad motornim vozilima, katastarski podaci, podaci o ostavinskim raspravama, podaci o privatizaciji preduzeća, poreski podaci i dr.).

Navedena i druga dokumentacija i evidencije može da sadrže indicijalne i dokazne činjenice, koje imaju izuzetan značaj za usmjeravanje operativne aktivnosti i dokazivanje krivičnih djela organizovanog kriminala.

Konvencija Savjeta Evrope o pranju, otkrivanju, zaplijeni i konfiskaciji prihoda kažnjivih dela i finansiranja terorizma svojim odredbama određuje da države potpisnice moraju biti u stanju da preduzmu mjere u slučajevima zahtijeva za: *podacima o bankarskim računima* (član 17.) koji se odnose na određivanje da li fizičko ili pravno lice, protiv koga se vodi krivični postupak, posjeduje ili kontroliše jedan ili više računa, *podacima o bankarskim transakcijama* (član 18.) koji se odnose na pružanje detaljnih informacija o bankovnim transakcijama u određenom periodu i *podacima o praćenju bankarskih transakcija* (član 19.) u određenom periodu i saopštavanje rezultata državi koja je uputila zahtjev. Prema sadržaju odredaba člana 20. ove Konvencije države mogu *spontano davati podatke* o nezakonito stečenom prihodu bez prethodnog zahtijeva ne prejudicirajući istražne i sudske postupke u slučajevima kada smatraju da bi pružanje tih podataka pomoglo drugoj državi u pokretanju ili vođenju krivičnih postupaka

4.15.2. Zajedničke istrage i primjena posebnih istražnih

Zajedničke istrage i primjena posebnih istražnih radnji kao poseban oblik uzajamne pomoći država potpisnica kao mogući model međunarodne suradnje inaugurisana odredbama člana 19. i 20. Konvencije ujedinjenih naroda protiv transnacionalnog organizovanog kriminala. Države potpisnice u skladu sa navedenim odredbama za potrebe efikasne borbe protiv organizovanog kriminala mogu zaključiti bilateralne ili multilateralne sporazume ili aranžmane prema kojima se u odnosi na stvari koje su predmet istraga,krivičnih gonjenja ili sudskih postupaka u jednoj ili više država zainteresovani nadležni organi mogu da obrazuju zajedničke istražne organe i po principima domaćeg pravnog sistema korištenje posebnih istražnih radnji.

4.15.3. Sprovođenje privremenih mjera zamrzavanja odnosno privremenog oduzimanja prihoda stečenih kriminalom

Sprovođenje *privremenih mjera zamrzavanja odnosno privremenog oduzimanja prihoda stečenih kriminalom* je slijedeći model međunarodne saradnje koji se realizuje na zahtjev druge države koja je pokrenula krivični postupak ili postupak oduzimanja. Ove mjere se poduzimaju u cilju onemogućavanja trgovine, prenosa, raspolaganja vlasništvom nad imovinom koja bi kasnije mogla biti predmet zahtjeva za oduzimanje.

U okviru Evropske unije donijeta je *Okvirna odluka Vijeća o izvršenju naloga za zamrzavanje imovine ili dokaza* kojom se utvrđuju pravila prema kojima država članica priznaje i na svojoj teritoriji izvršava nalog za zamrzavanje koji je izdao sudski organ druge države u okviru krivičnog postupka. Tako, da se odredbama člana 4. ovog dokumenta predviđa da nalog za zamrzavanje sudski organ može direktno uputiti nadležnom sudskom organu, koji će priznati nalog za zamrzavanje i preduzeti mjere potrebne za njegovo izvršenje, bez odlaganja. Saradnja u smislu ove Odluke podrazumijeva postojanje povjerenja da su odluke koje se uzajamno priznaju i izvršavaju donijete u skladu sa principima zakonitosti, supsidijarnosti i svrsishodnosti.

4.15.4. Realizacija pomoći u oduzimanju, vraćanju ili razmijeni prihoda stečenih kriminalom

Realizacija pomoći u oduzimanju, vraćanju ili razmijeni prihoda stečenih kriminalom je sljedeći model međunarodne saradnje koji se realizuje na osnovu naloga suda države koja je zahtjev podnijela ili se takav zahtjev prosljeđuje nadležnim tijelima u zavisnosti od unutrašnje pravne procedure.

Zatim, nadležna državna tijela razmatraju takav zahtjev i ukoliko se odobri izvršavaju ga poštujući postupak oduzimanja određen unutrašnjim pravnim sistemom. U slučajevima međunarodne pravne pomoći u vraćanju i razmjeni prihoda stečenih kriminalom međunarodni pravni akti upućuju u određenim slučajevima da pitanja raspolaganja oduzetom imovinom ostavljaju domaćem zakonodavstvu države kojoj je zahtjev upućen ili zamoljena strana ima obavezu da izvrši povraćaj oduzete imovine strani moliocu u slučajevima pronevjere javnih sredstava ili pranja takvih sredstava ako je osnovano utvrđeno prethodno vlasništvo, ali su moguće i situacije u kojima se daje prioritet zahtjevima država za povraćaj oduzete imovine ukoliko je to u skladu sa domaćim zakonodavstvom u cilju obeštećenja žrtava krivičnog djela ili omogući povrat imovine zakonitim vlasnicima.

U cilju efikasnije realizacije navedenih modela međunarodne saradnje u oduzimanju prihoda stečenih kriminalom države bi trebalo da inkorporiraju navedene modela saradnje u unutrašnja zakonodavna rešenja. Nažalost Bosna i Hercegovina i pored brojnih inicijativa još uvijek nije na državnom nivou usvojila Zakon o oduzimanju imovine proistekle iz krivičnih djela. Međutim, pozitivan primjer ovakvog pristupa je i inkorporiranje ovih modaliteta saradnje u Zakon o oduzimanju imovine stečene izvršenjem krivičnih djela RS.

Međunarodna saradnja u smislu odredba ovog zakona obuhvata pružanje pomoći u pronalaženju imovine proistekle iz krivičnog djela, zabranu raspolaganja i privremeno ili trajno oduzimanje imovine proistekle iz krivičnog djela. Nadležnost domaćeg tužilaštva, odnosno suda u postupku međunarodne saradnje određuje se shodno primjeni odgovarajućih zakonskih odredba o međunarodnoj pravnoj pomoći i u krivičnim stvarima. Sadržajem odredbi ovog zakona se uređuje način I postupak pružanja međunarodne pravne pomoći u

krivičnim stvarima, ako međunarodnim ugovorima nije drugačije određeno ili ako međunarodni ugovori ne postoje. Zamolnice domaćih pravosudnih organa za međunarodnu pravnu pomoć u pravilu se dostavljaju se stranim pravosudnim organima posredstvom Ministarstva pravde Bosne i Hercegovine. Na isti način dostavljaju se domaćim pravosudnim organima zamolnice stranih pravosudnih organa za međunarodnu pravnu pomoć. Svi eventualni izuzeci od navedenog pravila u dostavljanju moraju biti predviđeni međunarodnim ugovorima osim u slučaju kada ne postoji zaključen međunarodni ugovor kada Ministarstvo pravde Bosne i Hercegovine dostavlja i prima zamolnice za međunarodnu pravnu pomoć posredstvom Ministarstva vanjskih poslova Bosne i Hercegovine.

Sadržajem odredaba člana 24. ovog zakona data je mogućnost formiranja zajedničkih istražnih timova ukoliko to opravdavaju okolnosti konkretnog slučaja. Zajednički istražni timovi radi vođenja krivične istrage na teritoriji jedne ili više država se formiraju sporazumom nadležnog tužilaštva Bosne I Hercegovine s nadležnim organima strane države.

Razvijanje navedenih modela međunarodne saradnje u oduzimanju prihoda stečenih kriminalom je neizostavan dio strategije suprotstavljanja organizovanom kriminalu, jer savremeni organizovani kriminal je globalni fenomen koji se brzo razvija i čiji dometi i kobne posljedice predstavljaju prijetnju sigurnosti međunarodne zajednice u cjelini.

4.16. Međunarodne organizacije putem kojih se podstiče implementacija mehanizama za oduzimanje prihoda stečenih kriminalom

U cilju što efikasnije međunarodne saradnje u oduzimanju prihoda stečenih organizovanim kriminalom poseban značaj imaju međunarodne organizacije pomoću kojih se na strateškom i operativnom nivou podstiče implementacija efikasnih mehanizama oduzimanja prihoda stečenih kriminalom. U nastavku sadržaja teksta dajemo prikaz organizacije, funkcija i ciljeva vodećih međunarodnih organizacija koje djeluju u globalnim i regionalnim okvirima i programa (projekata) koje realizuju međunarodne organizacije kao dijela koordiniranog međunarodnog odgovora problemima suprotstavljanja organizovanom kriminalu i oduzimanja prihoda stečenih kriminalom.

Internacionalna policijska zajednica svjesna potrebe svesna potrebe suprotstavljanja organizovanom kriminalu i oduzimanja prihoda stečenih kriminalom, donela je mnogobrojna međunarodna akta kojima reguliše ovu oblast.

4.16.1. INTERPOL

Ovim naporima pridružio se i *INERPOL*[219] koji je svojim rezolucijama (Rezolucije AGN/52/RES/8, iz 1983. godine; AGN/57/ RES/8, iz 1988. godine; AGN/66/RES/17, iz 1997. godine) pozvao države članice da težište svojih istraga fokusiraju na identifikaciju, praćenje i oduzimanje protivpravno stečenih prihoda kriminalnih organizacija. Ove rezolucije također pozivaju članice da poboljšaju razmjenu informacija na tom polju i upućuju Vlade država članica da donesu zakone koji će omogućiti pristup finansijskim evidencijama i konfiskaciju prihoda stečenih kriminalom. Kao dio napora internacionalne policijske zajednice za suprotstavljanje organizovanom kriminalu nastao je i specijalizovani ogranak unutar policijskog odjeljenja Generalnog sekretarijata Interpola pod nazivom *FOPAC*.

[219] www.interpol.int,09.02.2012.,14,23.,

FOPAC je francuska skraćenica za *Fonds Provenant d`Activites Criminelles*, koji je formirala Generalna skupština Interpola u Kanu 1983. godine. Generalni sekretarijat Interpola i FOPAC kao njegov specijalizovani ogranak usko sarađuju sa drugim internacionalnim organizacijama sa ciljem razvoja svesti o potrebi korištenja finansijskih istražnih metoda u borbi protiv organizovanog kriminala i drugih oblika kriminala. Također, ova saradnja je usmjerena na objedinjavanje napora u suprotstavljanju organizovanom kriminalu u globalnim okvirima i razvoju saradnje i koordinacije u implementaciji internacionalnih programa koji teže oduzimanju prihoda stečenih kriminalom.

4.16.2. GRECO

GRECO (*Groups of States against Corruption*)[220] je komitet Savjeta Evrope osnovan s ciljem unapređenja kapaciteta članica za suprotstavljanje korupciji. Proces unapređenja kapaciteta za suprotstavljanje korupciji koncipiran je kroz fleksibilan i efikasan sistem evaluacije implementacije mjera za suprotstavljanje korupciji među kojima oduzimanje prihoda stečenih kriminalom zauzima značajno mjesto. Evaluaciju sprovode ekspertske grupe i na osnovu rezultata evaluacije predlažu se konkretne mjere (zakonske, organizacione, edukativne i sl.) za poboljšanje sistema za suprotstavljanje korupciji.

GRECO je posebno odgovoran za praćenje da li se države članice pridržavaju usvojenih principa za borbu protiv korupcije i implementacije mjera predviđenih međunarodno pravnim instrumentima usvojenim s ciljem ostvarivanja *Programa aktivnosti protiv korupcije* (Programme of Action against Corruption - PAC) koji realizuje ovo međunarodno tijelo.
Dosadašnje aktivnosti rezultirale su usvajanjem tri takva instrumenta: *Krivičnopravna konvencija o korupciji* iz 1999. godine (ETC br. 173), *Građanskopravna konvencija o korupciji* usvojena 1999. godine (ETC br.174) i *Preporuka (R 10) o pravilima ponašanja za javne službenike* usvojena 2000. godine. Učešće u radu ovog međunarodnog tijela naročito je značajno za zemlje koje se nalaze u procesu tranzicije u koje spada i naša zemlja, jer korupcija predstavlja ozbiljnu prijetnju demokratskim procesima, vladavini prava i ostvarivanju ljudskih prava. Efikasna borba protiv korupcije zahtijeva multidisciplinaran pristup ovom problemu i visok nivo međunarodne saradnje u oduzimanju prihoda stečenih kriminalom, koji se može ostvariti učešćem u radu ovakvih međunarodnih tijela.

4.16.3. Radna grupa za finansijske akcije (FATF)

Radna grupa za finansijske akcije (Financial Action Task Force – FATF [221] osnovana je na Samitu G-7 u Parizu 1989. godine, kao koordinirani internacionalni odgovor pranju novca u međunarodnim okvirima. Kao rezultat rada Grupe za finansijske akcije aprila 1990. godine definisano je *Četrdeset preporuka*, koje čine okvir za implementaciju mjera za suprotstavljanje pranju novca i oduzimanju prihoda stečenih kriminalom na nacionalnom I međunarodnom planu. *Četrdeset preporuka* sačinjene su tako da predstavljaju jedan fleksibilan okvir, koji omogućuje državama koje žele da ga primjene prilagođavanje ekonomskim, društvenim i političkim prilikama u zemlji. Treba istaći da *Četrdeset preporuka* ne predstavljaju međunarodnu konvenciju, već set mjera u suprotstavljanju pranju novca i oduzimanju prihoda stečenih kriminalom, koje svaka država može da primjeni ako postoji adekvatna politička volja. *Četrdeset preporuka* donesene su 1990. godine, a 1996. godine pretrpjele su određene izmjene u odnosu na nove trendove pranja novca. Naime, *Grupa za*

[220] www.coe.int/t/dghl/.../greco,09.02.2012.,14,40.
[221] www.fatf-gafi.org,09.02.2012.,14,33.

finansijske akcije je usvojila 2002. godine i osam Posebnih preporuka o finansiranju terorizma čime se pridružila globalnim naporima u borbi protiv finansiranja terorizma. Neke od najvažnijih obaveza definisanih u *Četrdeset preporuka* su: inkriminacija pranja novca kao teškog krivičnog djela (Preporuka 4), definisanje zakonskih okvira za privremeno oduzimanje i oduzimanje imovine pribavljene krivičnim djelima (Preporuka 7); definisanje obaveza finansijskim institucijama da vrše identifikaciju klijenata, uključujući i privilegovane klijente, kao i da vode evidenciju o transakcijama i čuvaju te podatke određen vremenski period (Preporuke 10,11 i 12); definisanje obaveza finansijskim institucijama da prijavljuju sumnjive transakcije nadležnim organima (Preporuka 15), sprovođenje mjera interne kontrole u finansijskim institucijama (Preporuka 19); uspostavljanje adekvatnog sistema eksterne kontrole i supervizije finansijskih institucija (Preporuke 26, 27, 28, 29) i definisanje pravnih okvira za međunarodnu saradnju i koordinaciju na svim nivoima u suprotstavljanju pranju novca (Preporuke od 32 do 40). *Grupa za finansijske akcije* tijesno sarađuje sa drugim regionalnim organizacijama, čiji se osnovni ciljevi odnose na suprotstavljanje pranju novca i oduzimanju prihoda stečenih kriminalom kao što su: *AGP* (Asia Pacific Group of Money Laundering), *PC-R-EV* (Committee of Concile of Europe), *OGBS* (Offshore Group of Banking Supervisors) i druge.

Kao dio sistema za suprotstavljanje pranju novca i traganju za prihodima stečenim organizovanim kriminalom stvoren je određen broj specijalizovanih vladinih agencija koje se bave ovom problematikom. Ovi entiteti koje su stvorile različite vlade nazivaju se zajedničkim imenom *jedinice za finansijske istrage*.Te jedinice omogućavaju veoma dobru komunikaciju i razmjenu informacija i druge oblike međunarodne saradnje na različitim nivoima u istragama i u isto vrijeme štite povjerljivost podataka. Većina jedinica za finansijske istrage počela je da radi devedesetih godina XX vijeka, i bile su rezultat potreba pojedinih država da se efikasno suprotstave organizovanom kriminalu i pranju novca.

4.16.4. EGMONT GRUPA

Od 1995. godine, određen broj jedinica za finansijske istrage počeo je da radi zajedno u neformalnoj organizaciji nazvanoj ***Egmont grupa***[222]. Osnovni cilj ove grupe bio je formiranje foruma jedinica za finansijske istrage, koji će poboljšati saradnju i komunikaciju između različitih država. Modaliteti te saradnje odnose se na: širenje sistema razmjene finansijsko-obavještajnih informacija, poboljšanje nivoa stručnosti osoblja organizacija i omogućavanje bolje saradnje između jedinica za finansijske istrage primjenom novih tehnoloških dostignuća.

4.16.5. MONEYVAL

Izabrani komitet eksperata za ocjenjivanje mjera protiv pranja novca Saveta Evrope - ***Moneyval*** (*Select Committee of Experts on the Evaluation of Anti-Money Laundering Measurements*)[223] osnovan je 1997. godine s ciljem uspostavljanja efikasnih sistema suprotstavljanja pranju novca i finansiranju terorizma u zemljama članicama. Aktivnosti ovog međunarodnog tijela usmjerene su na ocjenjivanje da li se njegove članice pridržavaju odgovarajućih standarda vezanih za borbu protiv pranja novca, oduzimanja prihoda stečenih kriminalom i finansiranja terorizma. *MONEYVAL* ima 27 članova i 2 privremena člana i kao

[222] www.egmontgroup.org,09.02.2012.,14,29.
[223] www.coe.int.moneyval,09.02.2012.,14,32.

regionalno tijelo na prostoru Evropske unije za borbu protiv pranja novca aktivno participira u radu *Grupe za finansijske akcije*, *Svjetske banke* i *MMF* u njihovim naporima u borbi protiv ove negativne pojave u globalnim okvirima. Naša zemlja je aktivni član ovog međunarodnog tjela, što je pozitivan primjer aktivnosti i participacije naše zemlje u radu međunarodnih organizacija koja se bave problemima suprotstavljanja organizovanom kriminalu i pranju novca.

4.16.6. CARDS

Cards[224] je regionalni projekat Evropske unije i Vijeća Evrope usmjeren na jačanje policijskih kapaciteta za borbu protiv teških krivičnih djela u zemljama jugoistočne Evrope. Projekat je počeo sa realizacijom 2004. godine i obuhvata slijedeće zemlje: Albaniju, Bosnu i Hercegovinu, Hrvatsku, Srbiju, Crnu Goru i Makedoniju. U okviru CARDS regionalnog projekat realizuje se podprojektu CARPO (Razvoj pouzdanih i funkcionalnih policijskih sistema i jačanje borbe protiv glavnih kriminalnih aktivnosti i jačanje policijske saradnje) koji ima dva modula. Koordinator prvog modula, Instrumenti za borbu protiv privrednog i organizovanog kriminaliteta"je Vijeće Evrope, a drugog modula „Obuka po svim pitanjima koja se odnose na trgovinu ljudima, krijumčarenje i ilegalne migracije'' je Međunarodna organizacija za migracije. Osnovni ciljevi ovih projekta su jačanje kapaciteta za borbu protiv kriminala razvijanjem i implementacijom regionalnih strategija za suzbijanje kriminala zasnovanih na standardima koji važe u Evropskoj uniji. Projekat obuhvata niz aktivnosti zemalja obuhvaćenih projektom (seminari, obuke, studijske posjete) koje su usmjerene na: razvoj regionalnih strategija za suprotstavljanje ekonomskom i organizovanom kriminalu; jačanje kapaciteta za sprovođenje finansijskih istraga usmjerenih na oduzimanje nezakonito stečenih prihoda; korištenje specijalnih istražnih tehnika i obavještajnog rada zasnovanog na poštovanju ljudskih prava i standarda koji važe u Evropskoj uniji; stvaranje efikasnih programa za zaštitu svjedoka u slučajevima organizovanog kriminala; jačanje kapaciteta za međunarodnu saradnju u suprotstavljanju kriminalu i razvijanje programa obuke za suprotstavljanje trgovinu ljudima, krijumčarenju i ilegalnim migracijama. Navedene aktivnosti se konkretizuju na nacionalnom nivou kroz razvijanje planova implementacije mjera za svaku oblast pojedinačno, definisanje programa za edukaciju i obuku, s ciljem podizanja nivoa stručnosti u implementaciji mjera određenih projektom i definisanje kriterijuma za praćenje progresa u implementaciji navedenih mjera. Međunarodne organizacije u oblasti suprotstavljanja organizovanom kriminalu imaju izuzetan značaj u promociji i sprovođenju međunarodnih standarda u oduzimanju prihoda stečenih kriminalom. Naime, ove organizacije podstiču članove da implementiraju standarde za suprotstavljanje organizovanom kriminalu i oduzimanje prihoda stečenih kriminalom, sprovode procjene sistema za suprotstavljanje organizovanom kriminalu, ukazuju na postojeće slabosti ovih sistema i omogućuju razmjenu podataka značajnih za istrage.

4.17 Institucije koje generišu posjeduju i čuvaju dokumentaciju, evidenciju , poslovne knjige, finansijske izvještaje i drugu dokumentaciju o prihodim, rashodima/troškovima, imovini i sredstvima i obavezama pravnih i fizičkih lica

Od brzog i efikasnog pristupa podacima o imovini, obavezama, prihodima i troškovima osumnjičenih koji se nalaze u javnim i privatnim bazama, registrima, dokumentciji, evidenciji, poslovnim knjigama i finansijskim izvještajima , zavisi i krajnji uspjeh finansijske istrage kao i postupci osiguranja odnosno privremenog oduzimanja imovine.Stoga

[224] www.coe.int./t/dghl/cooperation/.../peojects/CARPO/carpo_eng.asp,09.02.2012.,14,14.

u nastavku kroz minijaturni vodič identificiramo institucije koje generišu posjeduju ičuvaju dokumentaciju, evidenciju , poslovne knjige, finansijske izvještaje idrugu dokumentaciju o prihodim, rashodima/troškovima, imovini i sredstvima i obavezama pravnih i fizičkih lica

4.17.1. Centralna banka Bosne i Hercegovine

Osnovni ciljevi, poslovi, zadaci i nadležnosti Centralne banke su utvrđeni Zakonom o centralnoj banci Bosne i Hercegovine.[225] Centralna banka definira i kontrolira provođenje monetarne politike Bosne i Hercegovine i upravlja službenim deviznim rezervama ostvarenim izdavanjem domaće valute.

Centralna banka pomaže i održava odgovarajuće platne i obračunske sisteme i koordinira djelatnosti agencija za bankarstvo bh. entiteta, koje su nadležne za izdavanje dozvola za rad i superviziju banaka. Pored navedenog, Centralna banka u skladu sa sadržajem odredaba Odluke o Centralnom registru kredita poslovnih subjekata i fizičkih lica u Bosni i Hercegovini[226] i Odlukom o jedinstvenom registru transakcijskih računa[227] vodi: (1) Centralnom registru kredita poslovnih subjekata i fizičkih lica u Bosni i Hercegovini (2) Centralni registar transakcijskih računa. Pored navedenog, Centralna banka u skladu sa Zakon o platnim transakcijama u Federaciji Bosne i Hercegovine[228] , Zakon o platnim transakcijama u Republici Srpskoj[229] i Zakonom o platnim transakcijama BD BiH[230] vodi registar: Swift kodove banaka.

4.17.2. Državna agencija za istrage i zaštitu, Finansijsko obavještajni odjel,

Zakonom o Državnoj agenciji za istrage i zaštitu[231] je osnovana upravna organizacija u okviru Ministarstva sigurnosti BiH s operativno samostalnošću osnovana radi obavljanja policijskih poslova. U okviru Državne agencije za istrage i zaštitu djeluje unutrašnja organizaciona jedinica fInansijsko obavještajno odjeljenje koje prima, prikuplja, evidentira, analizira, istražuje i prosljeđuje tužilaštvu informacije, podatke i dokumentaciju primljene u skladu sa zakonom i drugim propisima o sprečavanju pranja novca i finansiranja terorističkih aktivnosti**.**

U okviru Finansijsko obavještajnog odjela se vodi baza podataka o svim sumnjivim, gotovinskim transakcijama iznad utvrđenog limita i vezanim transakcijama pravnih I fizičkih lica koje su u propisanoj proceduri prijavili obveznici iz zakona o sprečavanju pranja novca I finansiranja terorizma odnosno njihovi supervizori/regulatori kao I druge Finansijsko obavještajne jedinice.

Također, Državna agencija za istrage i zaštitu u skladu sa odredbama člana 34. stav 1. tačka 1. do 12. i stav 2. Zakona o policijskim službenicima BiH,[232] vodi evidencije koje se mogu i trebaju koristiti po potrebi.

[225] Vidi "Službeni glasnik BiH",broj:1/97,29/02,08/03,13/03,14/03,9/05 i 76/06,
[226] Vidi „Službeni glasnik BiH",broj 12/09,
[227] Vidi "Službeni Glasnik BiH",broj 27/04,15/06,31/06 I 28/08.
[228] Vidi "Službene novine Federacije Bosne i Hercegovine",broj 32/00
[229] Vidi "Službeni glasnik RS", broj 12/01
[230] Vidi „Službeni glasnik BD BiH",broj 5/01
[231] Vidi „Službeni glasdnik BiH",broj",broj 27/04,63/04,35/05 i 49/09)
[232] Vidi „Službeni glasnik BiH",broj 27/04,63/04,5/06,33/06,58/06,63/08 i 35/09

4.17.3. Uprava za indirektno oporezivanje Bosne I Hercegovine

Uprava za indirektno oporezivanje Bosne i Hercegovine je samostalna upravna organizacija koja svoj rad temelji na odredbama zakona koji regulišu sistem indirektnog oporezivanja[233] nadležnost i organizaciju Uprave,[234] postupak indirektnog oporezivanja,[235] postupak prinudne naplate,[236] carinsku politiku,[237] carinske prekršaje,[238] carinskoj tarifi,[239] porez na dodatnu vrijednost,[240] akcize[241] i uplata na jedinstven račun i raspodjelu prihoda.

Na temelju zakona i pripadajućih provedbenih akata (pravilnici, uputstva, odluke, instrukcije, objašnjenja, obavijesti koji regulišu navedena pitanja u okviru Uprave za indirektno oporezivanje se nalazi dokumentacija i evidencija za svaki od provedenih postupaka iz nadležnosti uprave za indirektno oporezivanje.

Pred toga, Uprava za indirektno oporezivanje u skladu sa Odredbama Pravilnika o registraciji i upisu u Jedinstven registar obveznika indirektnih poreza[242] vodi Jedinstveni registar obveznika indirektnih poreza.

4.17.4. Agenciju za identifikacijske isprave, evidenciju i razmjenu podataka BiH.

Agenciju za identifikacijske isprave, evidenciju i razmjenu podataka BiH (IDDEEA) je osnovana Zakonom o Agenciji za identifikacijske isprave, evidenciju i razmjenu podataka BiH [243] u junu 2008. godine. IDDEEA je nadležna za donošenje standarda iz oblasti identifikacionih dokumenata, administraciju i održavanje servera na kojima se nalaze podaci iz centralnih evidencija, hostovanje aplikacija putem kojih nadležni organi vode upravne postupke oko izdavanja ličnih dokumenata, održavanje mreže za prenos podataka između institucija sa svih nivoa vlasti i personalizaciju (štampanje) ličnih dokumenata.

Lične dokumente u skladu sa zakonskim propisima izdaju nadležna ministarstva unutrašnjih poslova, u Republici Srpskoj MUP Republike Srpske, u Federaciji kantonalni MUP-ovi, a u Brčkom Javni registar Brčko distrikta. Zahtjevi za izdavanje dokumenata podnose se u organizacionim jedinicama MUP-ova u mjestu prebivališta.

4.17.5. Porezna/Poreske uprave Federacije Bosne I Hercegovine i Republike Srpske

Porezna uprava Federacije BiH je nadležna za provođenje i izvršavanje aktivnosti iz oblasti svih vrsta federalnih, kantonalnih, gradskih i općinskih poreza, doprinosa, taksi, posebnih naknada, članarina turističkih zajednica, članarina obrtničkih komora i novčanih kazni za porezne prekršaje.[244]

---

[233] Vidi Zakon o sistemu indirektnog oprezivanja („Službeni glasnik BiH“,broj:44/03)
[234] Vidi Zakon o Upravi za indirektno oprezivanje(„Službeni glasnik bIH“,broj 89/05,
[235] Vidi Zakon o postupku indirektnog oprezivanja u BiH(„Službeni glasnik BiH“,broj 44/03,52/04,34/07,49/09)
[236] Vidi Zakon o postupku prinudne naplate indirektnih poreza(„Službeni glasnik BiH“,broj 89/05)
[237] Vidi Zakon o carinskoj politici(„Službeni glasnik BiH“,broj 57/04,51/06,93/08,54/10,76711)
[238] Vidi Zakon o carinskim prekršajima(„Službeni glasnik BiH“,broj 88/05)
[239] Vidi Zakon o carinskoj tarifi BiH(„Službeni glasnik BiH“,broj 31/02,32/04,48/05
[240] Vidi Zakon o porezu na dodatu vrijednost(„Službeni glasnik BiH“,broj 09/05,35/05 i 100/98)
[241] Vidi Zakon o akcizama u Bosni i Hercegovini(„Službeni glasnik BiH“,broj 49/09)
[242] Vidi „Službeni glasnik BiH“,broj 28/07 i 54/10)
[243] Vidi “Službeni glasnik BiH“,broj 56/08,
[244] Vidi Zakon o doprinosima („Službene novine F BIH“,broj 35/98,16/01,37/01,1/02,17/06,14/08);Zakon o porezu na dobit („Službene novine F BiH“,broj 97/07,14/08,39/09),

Osnovna djelatnost i funkcionisanje Porezne uprave Federacije BiH regulisana su Zakonom o Poreznoj upravi F BiH[245]. Zakonom o Poreznoj upravi Federacije BiH reguliše se osnov za primjenu svih poreznih zakona,[246] Zakona o Jedinstvenom sistemu registracije, kontrole i naplate doprinosa i Zakona o doprinosima u Federaciji Bosne i Hercegovine i odnosnih podzakonskih akata, te definišu određena prekršajna djela iz oblasti poreza i sankcija za ta djela.

Poreska uprava Republike Srpske je osnovana zakonom[247]kojim je uređen jedinstven postupak u primjeni materijalnih poreskih zakona ,a Poreskoj upravi je data nadležnost za sprovođenje svih materijalnih poreskih zakona[248].

4.17.6. Komisija za hartije od vrijednosnih RS, Komisija za vrijednosne papire F BIH i Zakon o tržištu hartija od vrijednosti BD BiH

Postoje tri nedržavne Komisije za vrijednosne papire u BiH, na nivou Federacije je to Komisija za vrijednosne papire F BiH,[249] na nivou entiteta Republike Srpske je to Komisija za hartije od vrijednosnih RS[250] i za Brčko Distrikt je to Komisija za papire od vrijednosti brčko Distrikta Bosne i Hercegovine.[251] Kao što je navedeno ranije, takva komisija ne postoji na državnom nivou da koordinira i usklađuje njihove zadatke. Pošto su zakoni o tržištu vrijednosnim papirima uglavnom usklađeni i komentari koji slijede jednako se primjenjuju na sve tri Komisije. Komisija za vrijednosne papire je stalno nezavisno pravno tijelo osnovano zakonom koje reguliše i kontroliše izdavanje i trgovinu vrijednosnim papirima. Komisija je odgovorna, *inter alia,* za:

- donošenje regulativa za implementaciju zakona kada je za to ovlaštena u skladu sa zakonom;
- nadziranje i zaštita tržišta vrijednosnih papira;
- izdavanje ili povlačenje dozvola, licence i odobrenja pravnim i fizičkim licima da posluju u skladu sa zakonom;
- nadzor nad institucijama / licima kojima izdaje licence;
- stopira izdavanje i trgovinu nekim vrijednosnim papirima;
- vodi evidencije i registre u skladu sa zakonom.

4.17.7. Sarajevska i Banjalučka Berze

Postoje dvije berze u BiH – u Sarajevu i Banja Luci. Berza je uspostavljena u skladu sa zakonima o tržištu vrijednosnih papira/hartija na kojima preko ovlaštenih brokerskih

[245] Vidi („Službene novine Federacije BiH" broj: 33/02, 28/04, 57/09 i 40/10)
[246] Vidi Zakon o porezu na dohodak („ Službene novine F BiH “,broj 10/08,9/10 i 44/11),
[247] Vidi Zakon o poreskoj upravi Republike srpske („Službeni glasnik RS “,broj 112/07,22/08,34/09
[248] Vidi Zakon o doprinosima („Službeni glasnik RS“, broj 51/01, 96/03, 128/06, 120/08, 1/11), Zakon o porezu na imovinu („Službeni glasnik RS“,broj:51/01, 53/07); Zakon o posebnim republičkim taksama („Službeni glasnik RS“, broj: 8/94,29/00, 18/01, 22/01, 60-I dio/03,41/05,51/06; Zakon o boravišnoj taksi („ Službeni glasnik RS “,broj 78/11 i 118/05); Zakon o igrama na sreću („Službeni glasnik RS“,broj 110/08,53/10,62/10 i 67/10); Zakon o porezu na dobit („Službeni glasnik RS“, broj 91/06); Zakon o porezu na dohodak („Službeni glasnik RS“,broj 91/06,128/06,120/08,71710 i 1/11); Zakon o porezu na nepokretnosti („Službeni glasnik RS“, broj 110/08 i 118/09);
[249] Vidi Zakon o tržištu hartija od vrijednosti („Službene novine F BiH2, broj 85/08)
[250] Vidi Zakon o tržištu hartija od vrijednosti („Službeni glasnik RS“, broj:92/06 i 34/09)
[251] Vidi Zakon o papirima od vrijednosti („Službeni glasnik BD BiH), broj: 15/03, 27/04, 42/04, 28/07)

posrednika obavljaju transakcije vrijednosnim papirima i koji ne trebaju biti akcionari. Cilj berzi je da obezbjeđuju organizovano tržište za transakcije vrijednosnim papirima.

4.17.8. Registar vrijednosnih papira u Federaciji BiH

Registar vrijednosnih papira u Federaciji BiH je osnovan Zakonom o registru vrijednosnih papira.[252] Registar vrijednosnih papira obavlja poslove registriranja, čuvanja i održavanja podataka o vrijednosnim papirima i poslove prijenosa, u skladu sa zakonom kojim se ureduje emisija i promet vrijednosnih papira. Registar vrijednosnih papira Federacije Bosne I Hercegovine ima organizovan Registar za emitente vrijednosnih papira i Registar za vlasnike vrijednosnih papira.

Registar za emitente vrijednosnih papira obavlja slijedeće poslove: (1)registraciju, čuvanje, vođenje i održavanje podataka o vrijednosnim papirima; (2) izradu lista dioničara i lista vlasnika vrijednosnih papira sa stanjem na dan po zahtjevu emitenta; (3) izradu drugih izvještaja po zahtjevu emitenta; (4) usluge u slučaju statusnih promjena i u slučaju promjene vrijednosnih papira zbog konverzije, denominacije vrijednosnih papira, spajanja i podjele dionica emitenta; (5) usluge u izvršavanju prava iz vrijednosnih papira (dostavljanje emitentima podataka o vlasnicima vrijednosnih papira, podataka o dioničarima, koji imaju pravo: glasa na skupštini, na obračun i isplatu dividende i druga prava) i drugo, saglasno posebnom ugovoru.

Registar za vlasnike vrijednosnih papira obavlja slijedeće poslove: (1) vođenje stanja vrijednosnih papira na računima vlasnika vrijednosnih papira; (2) izdavanje certifikata – izvoda i potvrda o stanju na računu vrijednosnih papira; (3) izradu drugih izvještaja po zahtjevu emitenta; (4) usluge u vezi vođenja prava trećih osoba na vrijednosnom papiru na posebnim računima, založnog prava, prava ograničenja raspolaganja, plodouživanja i druga prava; (5) uslugu u vezi preuzimanja dioničkog društva i provođenja tender ponude na osnovu posebnog ugovora između vlasnika vrijednosnih papira i Registra. Registracija podataka o vrijednosnim papirima i vlasnicima vrijednosnih papira, koje uprava društva dostavlja Registru, vrši se na računima emitenata i vlasnika vrijednosnog papira (investitora). Nakon otvaranja računa vlasnika vrijednosnih papira i nakon svake promjene stanja vrijednosnih papira na računu, Registar izdaje vlasniku vrijednosnog papira certifikat – izvod o stanju na računu vrijednosnih papira koji pokazuje stanje na računu vrijednosnih papira na kraju mjeseca u kojem je došlo do promjene stanja na računu, uz napomenu da certifikat - izvod o stanju na računu ne predstavlja vrijednosni papir, već potvrdu da je osoba na čiji se račun certifikat – izvod o stanju na računu odnosi, upisana kod Registra kao vlasnik vrijednosnih papira navedenih u certifikatu – izvodu. Svi podaci koji se nalaze na računu vlasnika vrijednosnog papira predstavljaju povjerljivu informaciju, a pravo uvida u račun ima samo vlasnik računa - investitor i ovlašteno lice u Registru.

4.17.9. Centralni registar Hartija od vrijednosti RS

Centralni registar hartija od vrijednosti AD Banja Luka funkcioniše u skladu sa odredbama Zakona o tržištu hartija od vrijednosti[253] u cilju da emitentima, vlasnicima hartija od vrijednosti i ovlaštenim učesnicima tržišta kapitala pruži brzu i efikasnu uslugu uz poštovanje principa sigurnosti.

[252] ("Službene novine F BiH", broj 39/98, 36/99 i 33/04).
[253] Vidi „Službeni glasnik Republike Srpske“, broj: 92/06 i 34/09)

Registar je pravno lice sa javnim ovlaštenjima za poslove[254] koje vodi bazu podataka u kojoj se upisuju, vode i čuvaju podaci o hartijama od vrijednosti, vlasnicima, pravima i ograničenjima prava na hartijama od vrijednosti, u skladu sa zakonom, propisima Komisije za hartije od vrijednosti i opštim aktima Registra.

Poslovi Registra su: (a) registracija i čuvanje podataka o hartijama od vrijednosti i njihovim vlasnicima i svim transakcijama u pogledu prenosa vlasništva ili promjene statusa hartija od vrijednosti; (b) registracija i čuvanje podataka o sticanju vlasništva i drugih prava iz hartija od vrijednosti; (c) upis i brisanje prava trećih lica na hartijama od vrijednosti, kao i upis i brisanje zabrane prava raspolaganja na osnovu ugovora, sudskih odluka i odluka nadležnih organa (d) otvaranje i vođenje računa emitenata, vođenje knjige akcionara, otvaranje i vođenje računa vlasnika hartija od vrijednosti, kao i izdavanje izvještaja, izvoda i potvrda o stanju i promjenama na tim računima; (e) otvaranje i vođenje računa berzanskom posredniku i drugim članovima Registra; (f) obračun, poravnanje i prenos hartija od vrijednosti na osnovu poslova sa hartijama od vrijednosti zaključenim na berzi i drugom uređenom javnom tržištu; (g) prenos hartija od vrijednosti na osnovu ugovora, sudskih odluka i odluka drugih nadležnih organa.

Registar može obavljati poslove depozitara investicionih fondova i druge poslove za koje dobije saglasnost Komisije. Centralni registar vodi evidenciju: a) berzanskih posrednika, (b) kastodi banaka, (c) akcionara, (d) emitenata.

4.17.10. Agencije za informatičke i posredničke usluge F BiH(Sarajevo i Mostar)

Dom naroda Parlamenta Federacije Bosne i Hercegovine, Zaključkom broj: 01-858/99[255], obavezao je Vladu F BiH i Upravni odbor Zavoda za platni promet da u procesu transformacije Zavoda, između ostalog, formira poslovnu banku ili drugu servisnu instituciju od preostalog dijela aktive i uposlenika Zavoda.

Vlada F BiH je Zaključkom broj: 268/00 od 05.10.2000. godine dala saglasnost na prijedlog Odluke o osnivanju servisnih institucija u Sarajevu i Mostaru. Na osnovu navedenih obaveza iz zaključaka Parlamenta i Vlade F BiH, te utvrđenog programa, Upravni odbor Zavoda za platni promet F BiH donio je Odluku o osnivanju Agencije za finansijske, informatičke i posredničke usluge d. d. Sarajevo i Agencije za pružanje financijskih, informatičkih i posredničkih usluga d. d. Mostar. Cilj osnivanja agencija je preuzimanje dijela zaposlenika Zavoda, kao i preuzimanje poslova Zavoda koji se ne mogu prenijeti na banke i druge institucije u procesu transformacije Zavoda i njegovog ukidanja, te razvoj novih poslova predviđenih programom. Agencije su počele sa radom u 2001. godini. Djelatnost agencija utvrđena je aktom o osnivanju i statutima agencija, a potvrđene su i Zakonom o prestanku važenja Zakona o unutrašnjem platnom prometu[256] , kao i posebnim odlukama Vlade F BiH[257]donesenim na osnovu navedenog zakona. AFIP obavlja slijedeće poslove: 1) vođenje blokiranih računa, (2) vođenje, čuvanje i raspolaganje arhivom ZPP-a, (3) prodaje taksenih maraka i mjeničnih obrazaca, (4) prijema i obrade polugodišnjih i godišnjih obračuna pravnih lica, i (5) ostali poslovi koje vlada Federacije BiH i Parlament Federacije BiH ocijene da im trebaju pripasti, saglasno njihovim mogućnostima i osposobljenosti a na osnovu ukazane

[254] Vidi „Zakona o tržištu hartija od vrijednosti“,član 189. stav 1.
[255] Vidi “Službene novine F BiH”, br. 40/99,
[256] Vidi“Služene novine F BiH”, br. 56/04
[257] Vidi“Službene novine F BiH”, br. 74/04

potrebe. Zakonom o računovodstvu i reviziji eksplicitno ne navodi AFIP već navodi ovlaštenu instituciju koja može, ali i ne mora biti AFIP.

4.17.11. Agencija za posredničke, informatičke i finansijske usluge Banja Luka

U skladu sa sadržajem odredaba Zakona o računovodstvu I reviziji RS I Zakona o jedinstvenom registru finansijskih izvještaja Republike srpske[258] uspostavljen je jedinstveni registar finansijskih izvještaja. Registar je centralni izvor informacija o imovinskom, prinosnom i finansijskom položaju lica i poduzetnika, obveznika predaje finansijskih izvještaja u registar. Registar uspostavlja i vodi Agencija za posredničke, informatičke i finansijske usluge. Agencija prikuplja, evidentira i obrađuje finansijske izvještaje, arhivira podatke, upravlja bazom podataka, te osigurava zaštitu baze podataka i dokumenata koji su arhivirani. Agencija odgovara za vjerodostojnost računskog unosa podataka.

Agencija uspostavlja posebnu evidenciju obveznika preuzimanjem podataka upisanih u sudski registar, podataka iz registra Poreske uprave Republike Srpske, Registra jedinice razvrstavanja Republičkog zavoda za statistiku i registra nadležnog organa jedinice lokalne samouprave. Evidencija obveznika ažurira se upisom i izmjenama upisa u navedene registre. Navedeni subjekti su dužni da Registru dostavljaju podatke o promjenama koje su nastale do isteka poslovne godine za koju podnose finansijski izvještaj, a koje se upisuju u registar za koje su ti subjekti nadležni. Podaci iz Registra su javni I dostupni bez dokazivanja pravnog interesa.

4.17.12. Javna i privatna preduzeća/društva za distribuciju električne energije, ptt usluga, RTV pretplate, usluge mobilne telefonije, zemnog gasa, vode i kanalizacije te usluge odvoza smeća i održavanje zajedničkih dijelova zgrada

U knjigovodstvu navedenih javnim preduzećima se nalazi dokumentacija (ugovori, fakture, opomene, uplate, tužbe i sl.) za svakog legalnog korisnika usluga koje navedena preduzeća/društva izvrše kao i način i dinamika naplate tih usluga od strane kupaca. Ova dokumenta koja je evidentirana u poslovnim knjigama tih preduzeća. Podaci javnih preduzeća sadržanih u navedenoj dokumentaciji i poslovnim knjigama su vjerodostojni podaci o troškovima osumnjičenih koji su predmet finansijske istrage,a prihodi i obaveze pojedinaca koji su zaposleni u ovoj vrsti preduzeća, odnosno društava.

4.17.13. Fond za penzijsko invalidsko osiguranje Republike srpske Federalni zavod za penzijsko/mirovinsko invalidsko osiguranje

Radi ostvarivanja prava iz penzijsko invalidskog osiguranja kao i utvrđivanja potreba i interesa u oblasti ovog osiguranja Zakonom o penzijskom i invalidskom osiguranju je osnovan Fond za penzijsko invalidsko osiguranje Republike Srpske, a u Brčko Distriktu Bosne I Hercegovine Federalni zavod za penzijsko/mirovinsko invalidsko osiguranje je javna ustanova čija su nadležnosti, organizacija, prava i obaveze utvrđene posebnim zakonom.[259] Zakonima koji reguliše navedena pitanja nisu obuhvaćena pitanja sticanja, ostvarivanje i prestanak prava iz penzijskog i invalidskog osiguranja, ko se smatra osiguranikom, penzijski staž, osiguravanje sredstava za penzijsko i invalidsko osiguranje i druga pitanja u vezi s penzijskim i invalidskim osiguranjem već su ta pitanja uređena

[258] Vidi „Službeni glasnik Republike Srpske“,broj 74/10,
[259] Vidi Zakon o organizaciji penzijskog i invalidskog osiguranja F BiH (“Sl. novine F BiH”, br. 32/01 i 18/05);

posebnim zakonima.[260] Rema sadržaju odredbi posebnog zakona obaveznim penzijskim i invalidskim osiguranjem osiguranicima se osiguravaju prava za slučaj invalidnosti, smrti i starosti. Na dobrovoljno penzijsko i invalidsko osiguranje mogu se osigurati lica koja nisu obavezno osigurana. Pored navedenog vođenje evidencije o osiguranicima i korisnicima prava iz PIO/MIO je propisano odredbama Zakona o matičnoj evidenciji o osiguranicima i korisnicima prava iz PIO,[261] u Republici srpskoj je posebnim zakonom[262] je osnovan Centralni registar obaveznog socijalnog osiguranja. Kako je Federalni zavod za penzijsko/mirovinsko invalidsko osiguranje pravno lice kao I Fond za penzijsko invalidsko osiguranje Republike Srpske na njega se primjenjuju odredbe Zakona o reviziji I računovodstvu u smislu knjigovodstvenih isprava, evidencije i registara, poslovnih knjiga, finansijskih izvještaja, revizorskih izvještaja, popisa i čuvanja istih.

4.17.14. Fond zdravstvenog osiguranja Brčko Distrikta Bosne i Hercegovine

Odredbama člana 5. Zakona o zdravstvenom osiguranju Brčko Distrikta Bosne i Hercegovine je utvrđeno da se radi realizacije prava iz zdravstvenog osiguranja Distrikta odlukom skupštine Distrikta formira posebna ustanova Fond zdravstvenog osiguranja Brčko Distrikta Bosne I Hercegovine. Također odredbama istog zakona su propisani oblici osiguranja (obavezno, prošireno, dobrovoljno i posebno), obveznici plaćanja doprinosa i finansiranje zdravstvenog osiguranja, korisnici, način i uslovi korištenja zdravstvenog osiguranja i zaštita prava iz zdravstvenog osiguranja korisnika.

4.17.15. Zavod zdravstvenog osiguranja i reosiguranja Federacije Bosne i Hercegovine i Zavodi zdravstvenog osiguranja u Kantonima

Zdravstveno osiguranje, kao dio socijalnog osiguranja građana, čini jedinstveni sistem u okviru koga građani ulaganjem sredstava, na načelima uzajamnosti i solidarnosti, obavezno u okviru kantona osiguravaju ostvarivanje prava na zdravstvenu zaštitu i druge oblike osiguranja na način koji je utvrđen ovim zakonom, drugim zakonima i propisima donesenim na osnovu zakona. Pod uvjetima utvrđenim ovim zakonom i drugim zakonima i propisima donesenim na osnovu zakona, građani Federacije imaju pravo na zdravstveno osiguranje, koje obuhvata: obavezno zdravstveno osiguranje, prošireno zdravstveno osiguranje dobrovoljno zdravstveno osiguranje.

Radi obavljanja poslova i ostvarivanja prava iz obaveznog zdravstvenog osiguranja koja su od interesa za sve kantone, kao i provođenja određenih prava po osnovu konvencija, drugih međunarodnih ugovora ili zakona i obavljanja poslova obaveznog zdravstvenog reosiguranja osniva se Zavod zdravstvenog osiguranja i reosiguranja Federacije Bosne i Hercegovine (u daljem tekstu: Federalni zavod osiguranja i reosiguranja). Federalni zavod osiguranja i reosiguranja i kantonalni zavod osiguranja obavezni su, u okviru jedinstvenog informacionog sistema, organizirati praćenje ostvarivanja i korištenja prava iz obaveznog zdravstvenog osiguranja i reosiguranja, praćenje uplata i potrošnje, po obveznicima doprinosa, kao i drugih sredstava i lično za svakog osiguranika.

---

[260] Vidi Zakon o penzijskom i invalidskom osiguranju F BiH ("Sl. novine F BiH", br. 29/98 (49/00), 32/01, 73/05, 59/06 i 4/09); Zakon o penzijskom i invalidskom osiguranju ("Sl. glasnik RS", broj 34/03, 62/04, 84/04, 85/05, 101/05, 63/06, 5/09, 107/09);

[261] Vidi „Sl. novine F BiH", br. 42/04;

[262] Vidi Zakon o Centralnom registru obaveznog socijalnog osiguranja ("Sl. glasnik RS", br. 30/10).

Odredba stava 1. ovog člana shodno se primjenjuje i na zavode dobrovoljnog zdravstvenog osiguranja. Kantonalni zavodi osiguranja i Federalni zavod osiguranja i reosiguranja su pravna lica s pravima i obavezama te odgovornošću utvrđenom ovim Zakonom i statutima kantonalnih zavoda osiguranja i Federalnog zavoda osiguranja i reosiguranja. Kantonalni zavodi osiguranja se mogu međusobno udruživati radi ostvarivanja potreba iz obaveznog zdravstvenog osiguranja.

Posebnim zakonom[263] u Federaciji Bosne I Hercegovine uređena su načela, način organiziranja i provođenja zdravstvene zaštite. Zdravstvena zaštita građana, u smislu ovog Zakona, je skup mjera, aktivnosti i postupaka na unapređenju prava na život, očuvanju i poboljšanju zdravlja ljudi, koje poduzima Federacija Bosne i Hercegovine, kantoni, općine, zdravstvene ustanove, zdravstveni radnici, preduzeća, druga pravna lica i građani.

4.17.16. Fond zdravstvenog osiguranja Republike Srpske

Zakonom o zdravstvenom osiguranju[264] Republike srpske uređen je sistem obaveznog I proširenog zdravstvenog osiguranja, prava iz osiguranja, način ostvarivanja prava i načela privatnog zdravstvenog osiguranja. Ostvarivanje prva iz obaveznog zdravstvenog osiguranja obezbjeđuje Fond zdravstvenog osiguranja kao samostalna organizacija kojom upravljaju osiguranici u skladu sa zakonom i drugim propisima kojima se regulišu određena pitanja iz organizacije i finansiranja zdravstvenog osiguranja.

Posebnim zakonom[265] je uređen sistem zdravstvene zaštite, organizacije zdravstvenih službi, društvene brige za zdravlje stanovništva, prava i obaveza pacijenata, zdravstvena zaštita stranaca i sl.

4.17.17. Agencija za rad i zapošljavanje BiH, Zavod za zapošljavanje F BiH, Javna ustanova Zavod za zapošljavanje RS, Zavod za zapošljavanje Brčko Distrikta BiH

Agencija za rad i zapošljavanje Bosne i Hercegovine je osnovana kao samostalna upravna organizacija u okviru institucija Bosne i Hercegovine, a nadležnosti su joj regulisane članom 6. Zakona o Agenciji za rad i zapošljavanje Bosne i Hercegovine[266]. Iz brojnih nadležnosti Agencije za potrebe ovog modela izdvojili smo slijedeće: (1) u koordinaciji sa Ministarstvom civilnih poslova Bosne i Hercegovine izvršava preuzete međunarodne obaveze iz oblasti zapošljavanja, a sarađujući sa nadležnim entitetskim zavodima za zapošljavanje i Zavodom za zapošljavanje Brčko Distrikta BiH (2) inicira zaključivanje međunarodnih ugovora u oblasti zapošljavanja i učestvuje u vođenju pregovora za zaključivanje međunarodnih ugovora u oblasti socijalnog osiguranja za dio nezaposlenosti i prati njihovo provođenje u saradnji sa zavodima za zapošljavanje entiteta i Brčko Distrikta BiH (3) prikuplja inostrane i domaće zahtjeve i informacije o ponudi i potražnji domaće i strane radne snage i u saradnji sa entitetskim zavodima za zapošljavanje i Zavodom za zapošljavanje Brčko Distrikta BiH realizuje iste u granicama svojih nadležnosti i mogućnosti tržišta rada u Bosni i Hercegovine.

[263] Zakon o zdravstvenoj zaštiti(„Službene novine F BIH“,broj 46/10.,
[264] „Službeni glasnik RS“, broj 55/07
[265] Zakon o zdravstvenoj zaštiti, „Službeni glasnik RS“ broj:106/09.
[266] Vidi „Službeni glasnik BiH“, broj: 21/03 i 43/09,

Pored Agencije u entitetima i Brčko distriktu su u skladu sa zakonima[267] osnovani Zavodi za zapošaljavanje čije obaveze i odgovornosti su posredovanje u zapošljavanju , javno obavještavanje o mogućnostima zapošljavanja, savjetovanje u vezi sa profesionalnom orjentacijom, stručno osposobljavanje i priprema za zapošljavanje, isplate novčanih naknada nezaposlenim licima i omogučavanje da ista u periodu trajanja materijalno pravnog obezbjeđenja ostvaruju i prava na zdravstveno i penzijsko i invalidsko osiguranje, vođenje evidencija u oblasti rada i zapošljavanja, odobravanje zapošljavanja stranih državljana i osoba bez državljanstva u skladu sa zakonima[268],o bavljanje organizacionih, stručni, administrativnih i drugih poslova u vezi sa ostvarivanjem prava nezaposlenih lica i sl..U toku finansijske istrage veoma je važno u fazi identifikacije prihoda i radno-pravnog i socijalnog statusa osunjičenog pogotovo u slučaju kada nezaposlena osoba uvečava imovinu i/ili troši znatno iznad svojih mogućnosti

4.17.18. Općinski organi/Uredi za katastar/Javni registar

Katastar ili javni registar je registar podataka o promjenama na zemljištu i nekretninama. Uz svoje druga zaduženja, katastar je podrška sistemu registracije prava vlasništva i drugih stvarnih prava vezanih za nekretnine odnosno podrška Zemljišno knjižnim uredima u Općinskim sudovima (tzv. gruntovnicama). Uredi za katastar izdaju posjedovne listove koji sadrže podatke o posjedniku,ali nisu dokaz o vlasništvu. Podaci o vlasništvu vidljivi su samo iz zemljišnih knjiga odnosno vlasničkog lista.

4.17.19. Sudovi nadležni za upis pravnih lica u registar

Registracija poslovnih subjekata u Bosni i Hercegovini, entitetima i BD BIH je regulisana zakonima[269] koji su uglavnom usaglašeni. Za registracije poslovnih subjekata odnosno samostalnih poduzetnika u skladu sa zakonima[270] su nadležni općinski i osnovni sudovi u entitetima i BD BiH. Prema zakona u nadležnim sudovima se vodi Registar koji je baza podataka koja sadrži podatke i isprave o subjektima, a sastoji se od Glavne knjige Registra i Zbirke isprava Registra. Glavna knjiga Registra je javni dio Registra koji sadrži podatke o subjektima upisa propisane ovim zakonom, a vodi se u elektronskom i štampanom obliku. Glavnu knjigu Registra u štampanom obliku vodi sud nadležan prema sjedištu poslovnog subjekta. Zbirka isprava Registra je dio Registra koji sadrži isprave na osnovu kojih je izvršen upis podataka o subjektima upisa u Glavnu knjigu Registra, kao i druge dokaze dostavljene i sastavljene u postupku upisa u Registar, kao i odluke donesene u postupku upisa u registar.

---

[267] Vidi Zakon o posredovanju u zapošljavanju i pravima za vrijeme nezaposlenosti („Službeni glasnik RS“,broj 30/10), Zakon o posredovanju u zapošljavanju i socijalnoj sigurnosti nezaposlenih osoba („ Službene novine F BiH“,broj 41/01,22/05) i Zakon o zapošljavanju i pravim za vrijeme nezaposlenosti („Službeni glasnik BD BiH“,broj 33/04,19/07,25/08)

[268] Vidi Zakon o zapošljavanju stranaca„Službene novine Federacije BiH“,broj 8/99),Zakon o zapošljavanju stranaca u Brčko Distriktu B i H (Službeni glasnik BD BiH”,broj 15/09,19/09 I 20/10) i Zakon o zapošljavanju stranih državljana i lica bez državljanstva(„Službeni glasnik“,broj 94/04)

[269] Okvirni Zakon o registraciji poslovnih subjekata u Bosni i Hercegovini („Sl. glasnik BiH“, broj 42/04), Zakon o registraciji poslovnih subjekata u F BIH („Sl. novine F BiH“, broj 27/05 i 68/05) i Zakon o registraciji poslovnih subjekata („Sl. glasnik BD BiH“, br. 15/05).

[270] Zakon o sudovima Federacije Bosne i Hercegovine (“Sl. novine F BIH”, br. 38/05 i 22/06), Zakon o sudovima RS (”Sl. glasnik RS”, broj 111/04, 109/05, 37/06 i 119/08) i Zakon o sudovima Brčko Distrikta BIH (“Službeni glasnik BD BIH”, broj 19/07, 20/07, 39/09, 31/11).

4.17.20. Općinski/osnovni sudovi-Zemljišne knjige

U skladu sa sadržajem odredaba Zakona o sudovima F BiH[271] općinski sudovi obavljaju zemljišno knjižne poslove, a u Republici Srpskoj u skladu sa odredbama Zakona o sudovima RS[272] sudovi obavljaju zemljišno knjižne poslove. Zakonom o zemljišnim knjigama F BIH[273] i Zakonom o zemljišnim knjigama RS[274] sadržajem identičnih odredaba uređuje vođenje održavanje i uspostavu zemljišnih knjiga, kao i upis nekretnina i prava na nekretninama u zemljišne knjige Republici Srpskoj. Zemljišna knjiga, u smislu ovog zakona, je javna knjiga i javni registar stvarnih prava na nekretninama i drugih prava, koja su zakonom predviđena za upis, kao i ostalih zakonom predviđenih činjenica od značaja za pravni promet (član 2.). Zemljišna knjiga se sastoji od glavne zemljišne knjige, zbirke isprava i pomoćnih registara. Glavna zemljišna knjiga se sastoji od zemljišnoknjižnih uložaka. Glavna knjiga se vodi za jednu katastarsku općinu (član 15.). Upisi se vrše u zemljišnoknjižni uložak. U zemljišnoknjižni uložak se upisuje jedno zemljišnoknjižno tijelo. Zemljišnoknjižno tijelo se sastoji od jedne ili više katastarskih parcela, koje se nalaze u istoj katastarskoj općini i na kojima postoje isti pravni odnosi. Zemljišnoknjižni uložak se sastoji iz natpisa (naslova) i tri odjeljka (A, B i C) (član 16.). Pored zemljišne knjige vode se također slijedeći pomoćni registri: (1). registar vlasnika, (2). registar parcela, (3). dnevnik (član 22.). U registar vlasnika se upisuje prezime, ime, poštanska adresa, rođeno ime i datum rođenja vlasnika kao i katastarska općina i broj zemljišnoknjižnog uloška u koji su upisane nepokretnosti koje pripadaju vlasniku. Za pravno lice upisuje se u smislu stava 1. ovog člana njen naziv i registrovano sjedište (član 23.). U registar parcela unosi se parcela nakon upisa u odjeljak A sa uputom na zemljišnoknjižni uložak ili uloške u kojima je ona upisana. Registar parcela se vodi za svaku katastarsku općinu za koju se vodi i glavna knjiga. Registar parcela se može voditi mašinskim putem (član 24.). U dnevnik se registruju zahtjevi za upis i dodjeljuju se registarske oznake. Kod svakog upisa se obavezno naznačava registarska oznaka upisa. To važi za upise u sve odjeljke. Završetak obrade zahtjeva donošenjem rješenja o odobrenju ili odbijanju zahtijevanog upisa potrebno je ubilježiti u dnevnik sa naznakom datuma donošenja rješenja (član 25.).

4.17.21. BH Direkcija civilne avijacija

Direkcija za civilno zrakoplovstvo Bosne i Hercegovine (BHDCA) kao organ nadležan i odgovoran za obavljanje funkcije regulatora i nadzor u oblasti civilnog zrakoplovstva i kontroli letenja, osnovana je 1997. godine sa ciljem da odgovori obavezama Bosne i Hercegovine kao države članice Međunarodne organizacije civilnog zrakoplovstva *(International Civil Aviation Organization - ICAO)* i potpisnice Čikaške konvencije.

Direkcija za civilno zrakoplovstvo Bosne i Hercegovine (BH DCA) vodi Registar aerodrome. Oblik i sadržaj Registra aerodrome, kao i način njegovog vođenja utvrđen je posebnim propisom koji donosi BH DCA. Prava i odgovornost za izgradnju aerodrome imaju entitetske institucije u BiH. Entitetske institucije mogu prenijeti svoje pravo i odgovornost za izgradnju i upravljanje aerodromom na bilo koju fizičku i pravnu osobu. Direkcija za civilno zrakoplovstvo također vodi registar civilnih zrakoplova. Registar je javna knjiga. Oblik i sadržaj Registra, kao i način vođenja registra,uređen je posebnim propisom koji donosi BH DC.Pri vođenju finansijske istrage jedna od adresa za utvrđivanje imovine osumnjčenog je i

[271] Vidi „Službene novine F BIH", broj 38/05 I 22/06)
[272] Vidi „Službeni glasnik RS", broj 111/04,109/05, 37/06 i 119/08)
[273] Vidi "Sl. novine F BIH", broj 19/03 i 54/04.
[274] Vidi "Sl. glasnik RS", broj 67/03)

registar i dokumentacija o vlasništvu nad aerodromima i zrakoplovima svih vrsta u Bosni i Hercegovini.

4.17.22. Kapetanije za unutrašnju i Kapetanije za pomorsku plovidbu

Podatke o brodovima, jahtama, čamcima, splavovima i drugim plutajućim objektima i njihovim vlasnicima se mogu dobiti u nadležnim kapetanijama i njihovim organizacionim jedinicama. Kapetanije i njihove područne organizacione jedinice u Republici Srpskoj vrše upis brodova, čamaca i plutajućih objekata u upisnik u skladu sa zakonom.[275] Također, Kapetanije za unutrašnju plovidbu-promet i kapetanije za pomorsku plovidbu-promet u Federaciji Bosne i Hercegovine u skladu sa odredbama zakona[276] i vode registre brodova, čamaca i plutajućih objekata. Kapetanija Distrikta u skladu sa odredbama zakona[277] vodi upisnik brodova i upisnik čamaca i plutajućih objekata.U toku finansijske istrage nerijtko će se radi utvrđivanja imovine osumnjičenog zatražiti podaci vlasništvu nad brodovima,jahtama i sl plovilima.

4.17.23. Banke

Osnivanje, poslovanje, upravljanje, supervizija i prestanak pravnih lica koja obavljaju poslove primanja novčanih depozita i davanje kredita kao i drugih poslova (banke) uređuje se zakonima.[278] U skladu sa odredbama zakona banke mogu obavljati poslove primanja svih vrsta depozita i drugih novčanih sredstava; davanje i uzimanje kredita i finansijski lizing; davanje svih oblika novčanog jemstva; učešće, kupovina i prodaja instrumenata tržišta novca i kapitala za svoj i tuđi račun; usluge platnog prometa i prenosa novca; kupovina i prodaja strane valute; izdavanje i upravljanje sredstvima plaćanja (uključujući kreditne kartice, putne i bankarske čekove); pohranjivanje i upravljanje vrijednosnim papirima i drugim vrijednostima; usluge finansijskog menadžmenta; kupovina i prodaja vrijednosnih papira i druge poslove. S obzirom na vrstu poslova u bankama se mogu dobiti podaci i dokumentacija o stanje i prometu sredstava na računima pravnih i fizičkih osoba, odobrenim kreditima i njihovoj otplati, izdatim karticama i stanjima na istim, izdatim bankarskim i putnim čekovima, podaci o datim garancijama, otvorenim akreditivima, upisanim hipotekama, o kupovini i prodaji strane valute, podaci o zaključenim ugovorima o sefu i o otvaranju sefa od strane vlasnika i/ili drugog ovlaštenog lica; pohranjenim vrijednosnim papirima i sl.U okviru finansijske istrage u pravilu se odnos spram banke , njenih i proizvoda klijenata uspostavlja u skladu sa odredbama člana 72[279].Zakona o krivičnom postupku BiH odnosno sličnim odredbama iz nedržavnih zakona o krivičnom postupku.

4.17.24. Mikrokreditne organizacije

Mikrokreditne organizacije su nedepozitne finansijske organizacije koje obavljaju djelatnost mikrokreditiranja s ciljem poboljšanja materijalnog položaja korisnika mikrokredita, povećanja uposlenosti, pružanja podrške razvoju poduzetništva i stjecanja dobiti. Osnivanje,

[275] Vidi Zakon o unutrašnjoj plovidbi, „Službeni glasnik RS, broj 58/01 i 113/05.
[276] Vidi Zakon o unutrašnjoj i pomorskoj plovidbi, „Službene novine Federacije BiH“, br. 73/05.
[277] Vidi Zakon o unutrašnjoj plovidbi u Brčko Distriktu Bosne i Hercegovine, „Službeni glasnik BD BIH“, br. 28/08 i 19/10).
[278] Zakon o bankama, „Sl. novine F BiH“, br. 39/98, 32/00, 48/01, 27/02, 41/02, 58/02, 13/03, 19/03 i 28/03), Zakon o bankama RS, („Sl. glasnik RS“, br. 44/03, 74/04) i Zakon o bankama Brčko Distrikta („Sl. glasnik BD BiH“, br. 5/03 i 19/07)
[279] Zakon o krivičnom postupku Bosne i Hercegovine (“Službeni glasnik BiH”,broj 3/03, 32/03, 36/03, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09).,

registrovanje, djelatnost, oblik organizovanja, poslovanja, način upravljanja, prestanak rada i nadzor poslovanja mikrokreditnih organizacija je uređen zakonima.[280] Mikrokreditne organizacije posjeduju dokumentaciju, evidencije-registre i poslovne knjige iz koji se mogu koristiti podaci o zaključenim ugovorima o mikrokreditima, njihovoj realizaciji i otplati za pravna i fizička lica. Regulatorni i nadzorni organ za mikrokreditne organizacije su entitetske Agencije za bankarstvo.

4.17.25. Lizing društva

Lizing društva su pravna lica sa sjedištem u Federaciji Bosne i Hercegovine i Republici Srpskoj koja su upisana u sudski registar na osnovu dozvole za obavljanje poslova lizinga izdate od strane nadležne Agencije za bankarstvo. Poslovi lizinga, uslovi osnivanja, poslovanje i prestanak rada davaoca lizinga, prava i obaveze subjekata lizinga, prestanak ugovora o lizingu, registracija svojinskih prava nad predmetom lizinga, izvještavanje, revizija i nadzor nad poslovanjem davaoca lizinga regulisani su zakonima[281] obzirom da je leasing posao pravni posao u kojem davalac leasinga prenosi pravo posjedovanja i korištenja predmeta leasinga na korisnika leasinga na određeni vremenski rok, a za uzvrat korisnik leasinga se obavezuje da mu za to plaća ugovorenu leaseing naknadu, leasing društva posjeduju dokumentaciju, evidencije-registre i poslovne knjige iz kojih se mogu koristiti podaci o zaključenim ugovorima o lizingu i njihovoj vrsti uslovima i otplati; podaci o akontacijskoj naknadi, podaci o leazing naknadi, podaci o registrovanim zalozima i sl. Knjigovodstvene isprave, poslovne knjige, finansijske izvještaje, popise obaveza, kapitala i imovine, revizorske izvještaje i dr. čuva u skladu sa odredbama Zakona o reviziji i računovodstvu.

4.17.26. Agencije za bankarstvo F BiH i RS

Agencije za bankarstvo F BiH i RS su odgovorne za regulisanje i nadzor nad bankama, štedne i kreditne (mikro kreditne) organizacije, finansijske lizing organizacije i aktivnosti transfera novca. Obje agencije rade prema svojim zakonima o agenciji za bankarstvo na entitetskom nivou. Obje agencije za bankarstvo su nezavisne, neprofitne institucije. Ne postoji agencija za bankarstvo u Brčko distriktu ali nadzor nad filijalama banaka koje posluju u Distriktu spada pod entitetske agencije odgovorne za relevantnu centralu banke. Usklađeni glavni zadaci agencija za bankarstvo koje određuju njihovi zakoni su: (1) da izdaju i povlače dozvole bankama i mikrokreditnim organizacijama, (2) da regulišu i nadziru bankarske i mikrokreditne organizacije, (3) upravljaju ili nadziru procedure za obnovu ili likvidaciju banaka uključujući i stečajne procedure, (4) da obavljaju aktivnosti podrške antiterorističkim mjerama uključujući i mjere u vezi sa rezolucijama Savjeta sigurnosti UN-a, (5) da poduzimaju odgovarajuće aktivnosti na sprečavanju finansiranja aktivnosti koje ugrožavaju mirovni sporazum, (6) da traže otvaranje računa u Centralnoj banci za transfer sredstava na blokirane račune, (7) da sarađuju u razmjeni informacija sa Centralnom bankom.

[280] Zakon o mikrokreditnim organizacijama ("Sl. glasnik RS", br. 64/06), Zakon o mikrokreditnim organizacijama („Sl. novine F BiH, br. 59/06).
[281] Zakon o leazingu („Službeni glasnik RS", br. 70/07) i Zakon o leasingu („Službene novine F BiH", br. 85/05 i 39/09)

4.17.27. Investiciono-razvojna banka Republike Srpske

Investiciono-razvojna banka Republike Srpske je osnovana posebnim zakonom.[282] Banka je registrovana kao akcionarsko društvo, u kojem 100% vlasništvo ima Republika Srpska. Strateški ciljevi Investiciono-razvojne banke RS su podsticanje investicija i stimulisanje razvoja u Republici Srpskoj. Pored toga,uloga ove banke je profesionalno i efikasno upravljanje imovinom Republike Srpske, koja je formalno pravno registrovana na šest fondova. Investiciono-razvojna banka RS nema karakter poslovne banke,odnosno prema Zakonu, nema pravo da prikuplja depozite niti da daje garancije, te na taj način ne potpada pod jurisdikciju Agencije za bankarstvo RS. Investiciono-razvojna banka Republike Srpske ne vrši plasman sredstava namijenjenih razvojnim projektima direktno, već posredstvom poslovnih banaka i mikrokreditnih društava.

4.17.28. Razvojna banka Federacije BiH

Razvojna banka Federacije BiH također je osnovana posebnim zakonom[283] i čija je zadaća provođenje ekonomske politike Vlade Federacije Bosne i Hercegovine radi privrednog razvoja i zapošljavanja,kroz stimulativno kreditiranje koje podrazumijeva razvojne stimulativne kamatne stope,koje su u naravi niže od tržišnih kamatnih stopa. Izvori sredstava za poslovanje banke,u skladu sa odredbama Zakona o razvojnoj banci, čine sredstva budžeta Federacije Bosne i Hercegovine, sredstva ostvarena iz procesa privatizacije i sredstava kreditora međunarodnih finansijskih institucija i fondova, kojim se zadužuje Federacija BiH ili za koje je garant. Banka u ime Federacije BiH upravlja i domaćim i stranim sredstvima koja su namijenjena za finansiranje projekata u F BiH. Razvojna banka prima depozite u domaćoj i stranoj valuti, ali ne posluje sa primarnim ciljem ostvarivanja dobiti. Ne primjenjuje u cijelosti odredbe Zakon o bankama i to one koje se odnose na odobrenje Agencije za rad, pružanje bankovnih i ostalih finansijskih usluga, osnivanje filijala i pravnih osoba, nadzor Agencije, osiguranje uloga, privremenu upravu, likvidaciju, stečaj te kaznene odredbe. Na razvojnu banku se ne primjenjuju propisi o izdvajanju i održavanju obaveznih rezervi kod Centralne banke BiH i Zakon o osiguranju depozita.

4.17.29. Agencija za osiguranje depozita BiH

Agencija za osiguranje depozita Bosne i Hercegovine je samostalna, neprofitna, pravna osoba sa punim ovlaštenjem u skladu sa zakonom države.[284] Osnovi zadaci Agencije za osiguranje depozita Bosne i Hercegovine su: osiguranje prikladnih depozita ("prikladni depozit" je ukupan iznos svih sredstava koji rezultiraju iz depozita, štednih računa ili certifikata banke koje je deponent deponovao u banci članici) fizičkih osoba u bankama članicama u skladu sa Zakonom o osiguranju depozita u bankama Bosne i Hercegovine; izdavanje certifikata o članstvu bankama koje zadovoljavaju kriterije za učešće u programu osiguranja depozita,oduzimanje putem suspenzije ili okončanja certifikata o članstvu; investiranje sredstava koja čine Fond za osiguranje depozita u skladu sa ograničenjima Politike investiranja agencije u skladu sa Zakonom o osiguranju depozita u bankama Bosne i Hercegovine; isplata osiguranja depozita u slučaju prestanka rada banke članice u skladu sa Zakonom o osiguranju depozita u bankama BiH; donošenje podzakonskih akata kojima se regulira osiguranje depozita i poslovanje Agencije u skladu sa Zakonom o osiguranju

[282] Zakon o Investiciono-razvojnoj banci Republike Srpske(„Službeni glasnik RS“,broj 56/06)
[283] Zakon o Razvojnoj banci Federacije BiH, „Sl. novine F BiH“, br. 37/08.
[284] Zakonom o osiguranju depozita u bankama Bosne i Hercegovine ("Službeni glasnik BiH", br. 20/02, 18/05, 100/08 i 75/09).

depozita u bankama Bosne i Hercegovine. Banke članice plaćaju premiju osiguranja, gdje se kao osnovica premije osiguranja koriste prosječni prikladni depoziti na kraju svakog mjeseca uvećani za obračunatu kamatu. Uplata premije vrši se tromjesečno. Tromjesečja počinju prvog dana januara, aprila, jula i oktobra. Visina stope premije iznosi 0,3%. Upravni odbor Agencije najmanje jedanput godišnje utvrđuje visinu stope premije osiguranja za sve banke članice, na prijedlog direktora Agencije. Najveći iznos osiguranog depozita, zajedno sa obračunatom kamatom, koji isplaćuje Agencija po fizičkom licu po banci članici, iznosi prikladni depozit umanjen za zakonski ili ugovorni dug fizičkog lica prema banci članici u visini utvrđenoj odlukom Upravnog odbora Agencije a koji sada iznosi KM 35.000,00 ili koji je manji.

4.17.30. Društva za osiguranje

Djelatnost osiguranja u F BiH i RS mogu obavljati društva za osiguranje koja su obrazovana kao dionička društva ili društva za uzajamno osiguranje u skladu sa zakonima.[285] Društva za osiguranje mogu obavljati samo djelatnost osiguranja. Djelatnost osiguranja podrazumijeva zaključivanje ugovora o neživotnom i životnom osiguranju, a poslovi osiguranja zaključivanje ugovora o osiguranju i reosiguranju i obradu zahtijeva za naknadu koji proizišđu iz tih ugovora. U dokumentaciji, evidenciji (bilansnoj i vanbilansnoj), poslovnim knjigama, finansijskim izvještajima se iskazuju podaci o policama osiguranja,premijama osiguranja, isplaćenim naknadama štete, kapitalu izloženom riziku u pogledu životnog osiguranja, bruto fakturisanih premija, garantni fond, posrednicima (zastupnicima i brokerima) osiguranja, portfelj osiguranja i sl.

Pored navedenih podataka u društvima za osiguranje se vode i čuvaju poslovne knjige,finansijski izvještaji, revizorski izvještaji i druga dokumentacija i evidencije koja može biti izvor relevantnih podataka o imovini,obavezama,troškovima i prihodima pojedinaca koji su predmet finansijske istrage.

4.17.31. Agencija za osiguranje u BIH , Agencija za nadzor osiguravajućih društva u F BIH i RS

Državna agencija za osiguranje je osnovana Zakonom o Agenciji za osiguranje BiH.[286] Državna agencija za osiguranje je nezavisna institucija koja podnosi izvještaje Savjetu ministara. Glavna uloga Državne agencije za osiguranje je usklađivanje entitetskih zakona o osiguranju i ostalih zakonskih dokumenata; da djeluje kao arbitar u parnicama između entitetskih agencija za osiguranje I da koordinira njihov rad.

Osiguravajuće poslovanje je regulisano i pod nadzorom je Agencija za nadzor osiguranja na federalnom nivou i nivou Republike Srpske. Obje agencije su osnovane entitetskim zakonima o osiguravajućim društvima i imaju nadležnost nad osiguravajućim kompanijama i kompanijama za reosiguranje kao i za posrednike pri osiguranju. Funkcije Agencije za nadzor osiguranja Federacije Bosne i Hercegovine i Agencija za nadzor osiguranja Republike Srpske utvrđene su međusobno usklađenim zakonima. Agencije se uspostavljene zakonima kao nezavisne neprofitnu instituciju u formi pravnog subjekta koji je za svoje operacije odgovoran Vladi odnosnog entiteta. Regulatorni i nadzorni ciljevi Agencija, *inter alia*, uključuju odgovornosti:

[285] Zakon o društvima za osiguranje u privatnom osiguranju, „Sl. novine F BiH“, broj 24/05 i Zakonom o društvima za osiguranje, „Sl. glasnik RS“, broj 17/05, 01/06 i 64/06.
[286] Zakon o Agenciji za osiguranje u Bosni i Hercegovini, „Sl. glasnik BiH“, broj 12/04.

- ✓ nadgledanja primjenu zakona i podzakonskih akata u osiguravajućim i ostalim regulativama;
- ✓ regulisanja aktivnosti reosiguravajućih/osiguravajućih društava i posrednika pri osiguranju;
- ✓ promovisanja povjerenja tržišta osiguravajućih aktivnosti;
- ✓ sprječavanje finansijskog kriminala zabranom osiguravajućih aktivnosti koje nisu u skladu sa zakonom;
- ✓ informisanje i savjetovanje o raznim vrstama životnog i neživotnog osiguranja;
- ✓ savjetovanje i zaštiti klijenta.

4.17.32. Notari

Služba notara je javna služba koju obavljaju notari, koji su samostalni i nezavisni nosioci te službe i uspostavljena je preko tri nedržavna zakona[287] koja su u velikoj mjeri usaglašena. Zadatak notara je da vrši obradu, ovjeravanje i potvrđivanje javnih isprava, te vrši druge poslove u skladu sa ovim zakonom. Notarske isprave su sve isprave notara, koje on sačini na osnovu ovog zakona u okviru svoje nadležnosti. Notarske isprave su: notarski obrađene isprave, notarske ovjere i notarske potvrde. Notarske isprave vrijede kao javne isprave i važe na teritoriji cijele Republike Srpske, kod svih organa vlasti, pravnih lica i drugih institucija nezavisno od toga od kojeg su notara na teritoriji Bosne i Hercegovine izdate. Notarski obrađene isprave, koje je notar sačinio u granicama svojih službenih ovlaštenja u propisanoj formi, imaju punu dokaznu snagu javne isprave o izjavama datim pred notarom. Notarske ovjere i potvrde imaju dokaznu snagu javne isprave o činjenicama o kojima se u njima svjedoči. Pravni poslovi koji za svoju pravnu valjanost zahtijevaju notarsku obradu isprava odnose se na: (a) pravne poslove o regulisanju imovinskih odnosa između bračnih drugova, kao i između lica koja žive u vanbračnoj životnoj zajednici, (b) raspolaganja imovinom maloljetnih i poslovno nesposobnih lica, (c) pravne poslove kojima se obećava neka činidba kao poklon s tim što se nedostatak notarske forme u ovom slučaju nadomješta izvršenjem obećane činidbe, (d) pravne poslove, čiji je predmet prenos ili sticanje vlasništva ili drugih stvarnih prava na nekretninama; (e) osnivačka akta privrednih društava. Prema sadržaju odredaba člana 4. st. 1. t. i. važećeg Zakon o sprečavanju pranja novca i finansiranja terorizma[288] notari su obveznici u smislu Zakona.

4.17.33. Poslovni subjekti (preduzeća ili privredna društva)

Na državnom nivou ne postoji zakon o poslovnim subjektima (preduzećima ili privrednim društvima). Osnivanje, poslovanje, upravljanje I zatvaranje poslovnih subjekata regulišu entitetski zakoni i zakon Brčko Distrikta BiH. U Federaciji BiH je Zakon o privrednim društvima[289] uređuje osnivanje, poslovanje, upravljanje I prestanak privrednih društava u Federaciji Bosne i Hercegovine. Društvo je pravno lice koje samostalno obavlja djelatnost proizvodnje i prodaje proizvoda i vršenja usluga na tržištu radi sticanja dobiti (član 2. stav 1.). Privredno društvo u Federaciji BiH može biti organizovano u jedan od slijedećih oblika (1) društvo sa neograničenom odgovornošću, (2) komanditno društvo, (3) dioničko društvo, (4) društvo sa ograničenom odgovornošću.

---

[287] Zakon o notarima („Sl.užbene novine F BiH“, broj 45/02), Zakon o notarima (Službeni glasnik RS“, broj 86/04,2/05,74/05,76/05,91/06,37/07,50/10,43/11) i Zakon o notarima Brčko Distrikta („Službeni glasnik Brčko Distrikta Bosne i Hercegovine“, broj 9/03 i 17/06).

[288] Zakon o sprečavanju pranja novca i finansiranja terorističkih aktivnosti, „ Službeni glasnik BiH, broj

[289] „Službene novine F BiH“, broj: 23/99, 45/00, 2/02, 6/02, 29/03, 68/05, 91/07, 84/08.

Zakon o privrednim društvima RS[290] navodi da je privredno društvo pravno lice koje osnivaju pravna i/ili fizička lica radi obavljanja djelatnosti u cilju sticanja dobiti. Pravne forme privrednih društva u smislu zakona su ortačko društvo, komanditno društvo, društvo sa ograničenom odgovornošću i akcionarsko društvo (otvoreno i zatvoreno).

Odredbama Zakona o preduzećima Brčko Distrikta BiH[291] je utvrđeno da preduzeće označava pravno lice koje samostalno na tržištu obavlja djelatnost radi sticanja dobiti. Preduzeće u skladu sa zakonom može biti organizovano u jedan od slijedećih oblika: društvo sa ograničenom odgovornošću, komanditno društvo, dioničko društvo i društvo sa ograničenom odgovornošću.

U okviru svakog od oblika organizovanja privrednih društva odnosno preduzeća se u skladu sa zakonima vodi, nalazi I čuva dokumentacija i evidencija, poslovne knjige, finansijski i revizorski izvještaji koja se odnosi na registraciju,upravljanje, zastupanje,vlasničku strukturi,poslovanje i sl. Slijedom navedenog, privredna društva su vrlo često pouzdan izvor relevantnih podataka te materijalnih i ličnih dokaza o prihodima, troškovima, imovini, obavezama pojedinca.

4.17.34. Udruženja i fondacija

Udruženje je u smislu važećih državnih i nedržavnih zakona, svaki oblik dobrovoljnog povezivanja više fizičkih ili pravnih lica radi unapređenja ili ostvarivanja nekog zajedničkog ili opšteg interesa ili cilja, u skladu sa Ustavom i zakonom, a čija osnovna svrha nije sticanje dobiti. Fondacija je pravno lice koje nema svoje članstvo, koja se osniva radi upravljanja određenom imovinom u javnom ili zajedničkom interesu. Udruženja i fondacije ostvaruju carinske, poreske i druge olakšice za svoj rad u skladu sa zakonom.

Osnivanje i poslovanje neprofitnih organizacija je regulisano na državnom, entitetskom i nivou Distrikta raznim zakonima o udruživanjima i fondacijama.[292] Zakoni su uglavnom usklađeni. Udruženje se može osnovati od strane najmanje tri domaće ili strane fizičke osobe, dok fondaciju mogu osnovati jedna ili više. Udruženja mogu osnovati svoje saveze ili ostale oblike udruživanja gdje su njihovi interesi povezani na višem nivou (udruženja na visokom nivou). Registracija udruženja i fondacija je dobrovoljna, ali one mogu steći status pravne osobe od datuma njihovog upisivanja u registar. Ne postoji jedinstven Registar udruženja I fondacija. Na svakom nivou, državnom, entitetskom i nivou BD, zakon imenuje odgovorna tijela za registraciju i/ili vođenje registra udruženja i fondacija: Ministarstvo pravde BiH, Ministarstvo pravde F BiH, Ministarstvo uprave i lokalne samouprave RS, okružni sudovi (RS) i Osnovni sud BD.

Udruženja i fondacije se u skladu sa zakonima dužna voditi i čuvati dokumentacija i evidencija , poslovne knjige, finansijski i revizorski izvještaji koja se odnosi na osnivanju, registraciju, upravljanje, poslovanje i sl. Slijedom navedenog, udruženja i fondacije su vrlo često pouzdan izvor relevantnih podataka te materijalnih i ličnih dokaza o prihodima i obavezama pojedinca.

[290] („Službeni glasnik RS“,broj:127/08,58/09 i 100/11)
[291] (“Službeni glasnik BD BiH”,broj 11/01,10/02,14,02,1/03,08/034/04,19/07,34/07,49/11)
[292] Zakon o udruženjima i fondacijama Bosne i Hercegovine („Službeni glasnik BiH“, br. 32/01, 42/03); Zakon o udruženjima i fondacijama Federacije BiH, („Službene novine F BiH“, br. 45/02); Zakon o udruženjima i fondacijama RS („Sl. glasnik RS“, br. 52/01 i 42/05); i Zakon o udruženjima i fondacijama („Sl. glasnik BD BiH“, br.12/02 i 19/07).

4.17.35. Ministarstvo unutrašnjih poslova Republike Srpske, Kantonalna ministarstva unutrašnjih poslova i Javni registar Brčko Distrikta.

Lične dokumente u skladu sa zakonskim propisima[293] izdaju nadležna ministarstva unutrašnjih poslova,u Republici Srpskoj Ministarstvo unutrašnjih poslova Republike Srpske[294], u Federaciji Bosne I Hercegovine kantonalna Ministarstva unutrašnjih poslova[295],a u Brčkom Distriktu Bosne I Hercegovine Javni registar Brčko Distrikta.

Nadležni organi za izdavanje pasoša za državljane BiH koji imaju prebivalište van teritorije Bosne I Hercegovine,kao I izdavanje diplomatskih pasoša je mInistarstvo vanjskih poslova BiH,a za izdavanje službenih pasoša Bosne I Hercegovine je Ministarstvo civilnih poslova BiH.

Nadležni organ za izdavanje ličnih karata I vozačkih dozvola za strane državljane su kantonalna ministarstva unutrašnjih poslova u Federaciji Bosne I Hercegovine,MUP Republike Srpske u Republici srpskoj i Javni registar Brčko Distrikt za Brčko Distrikt Bosne I Hercegovine.

Također,nadležni organ za izdavanje putnih isprava za lica bez državljanstva i putnog lista za strance je Služba za poslove sa strancima, za putne isprave za izbjeglice je Ministarstvo sigurnosti Bosne i Hercegovine, a za izdavanja identifikacionih dokumenata, licima kojima je priznata međunarodna zaštita je bilo Ministarstvo za ljudska prava i izbjeglice.

Naponema edukatorima

Kroz praktične primjere prezentirati materijalne dokaze koji se nalaze u navedenim institucija, razjasniti postupak prikupljanja istih koji je u direknoj zavisnosti od toga da li se radi o privatnosti ili ne odnosno narušavaju li se postuopkom ludska prava građana ili ne.

Pored navedenog, objasniti i značenje pojedinih dokumenata koji se generišu u navedenim institucijama kao i njihovo značenje u vezi sa drugim dokumentima u hioptetikim slučajevima.(npr.nalog 1450, SWIFT doznaka,ugovor o lombardnom kreditu, ugovor o finansijskom leszingu i sl)

4.18. Sistem računovodsve i knijigovodstva a u BIH

Donošenjem novih zakona o računovodstvu i reviziji entiteta u BiH[296] bilo je neophodno na putu ka harmonizaciji računovodstvenog i revizijskog sistema BiH radi usaglašavanja domaćeg zakonodavstva sa pravnim stečevinama Evropske unije, kao i uslijed razvoja tržišta

[293] Zakon o JMB („Sl. glasnik BiH“, broj 32/01, 63/08), Zakon o prebivalištu i boravištu državljana BiH („Službeni glasnik BiH“,broj 32/01, 56/08), Zakon o ličnoj karti državljana Bosne i Hercegovine („Službeni glasnik BiH“ broj: 32/01, 16/02, 32/07, 53/07, 56/08), Zakon o putnim ispravama Bosne i Hercegovine („Sl. glasnik BiH“, broj: 4/07, 1/99, 9/99, 27/00, 32/00, 19/01, 47/04, 15/08, 39/08)

[294] Zakon o unutrašnjim poslovima („Sl. glasnik RS“, broj 48/03)

[295] MUP Unsko-sanskog kantona, MUP Posavskog kantona, MUP Tuzlanskog kantona, MUP Zeničko-dobojskog kantona, MUP Bosansko-podrinjskog kantona, MUP Srednjobosanskog kantona, MUP Hercegovačko-neretvanskog kantona, MUP Zapadno-hercegovačkog kantona, MUP Kantona Sarajevo, MUP kantona 10.

[296] Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine(„Službene novine F BiH“,broj 89/09) i Zakon o računovodstvu i reviziji Republike Srpske(„Službeni glasnik RS“,broj:36/09 i 52/11

kapitala, značajnih izmjena u oblasti profesionalne regulative, donošenja novih ili izmjena postojećih zakona iz oblasti bankarstva, tržišta vrijednosnih papira, investicionih fondova, osiguranja i dr

Zakonom o računovodstvu i reviziji Bosne i Hercegovine[297] uspostavljen je jedinstveni okvir kojim je utvrđena obaveza primjene međunarodnih standarda računovodstva i revizije, uključujući i kodeks profesionalne etike za profesionalne računovođe i revizore na cijeloj teritoriji Bosne I Hercegovine.Također, su utvrđeni jednoobrazni zahtjevi za provođenje obuke i sticanje kvalifikacija, testiranja, certifikacije i licenciranja profesionalnih računovođa i revizora, koji su obavezni na cijeloj teritoriji BiH, uzajamno priznavanje kvalifikacija profesionalnih računovođa i revizora i nesmetano obavljanje revizije na cijeloj teritoriji BiH, obaveza usaglašavanja provedbenih i drugih propisa Federacije Bosne i Hercegovine, Republike Srpske i Brčko Distrikta BIH sa odredbama ovog zakona. Pored navedenog uređeno je i osnivanje nezavisne Komisije za računovodstvo i reviziju BiH, koja nadgleda primjenu standarda i vrši druge poslove u skladu sa ovlaštenjima iz državnog Zakona, za cijelu teritoriju BiH.

Doneseni entitetski zakoni o računovodstvu i reviziji Federacije Bosne i Hercegovine i Republike Srpske također propisuju obavezu primjene Međunarodnih standarda finansijskog izvještavanja (IFRS) i Međunarodnih revizijskih standarda (ISA), a njihove odredbe su u značajnoj mjeri usklađene i sa zahtjevima sadržanim u relevantnim direktivama EU te predstavljaju osnov za provedbu reforme korporativnog finansijskog izvještavanja i za jačanje i unapređenje računovodstvene profesije na putu uključivanja Bosne i Hercegovine u evropske integracione procese.

Dakle, oba entiteta su usvojili zakone o računovodstvu i reviziji. Donošenjem ovih zakona je napravljen značajan iskorak na ”evropskom putu”, međutim još uvijek je potrebno daljnje usklađivanje kako bi se u potpunosti ispunili međunarodni standardi računovodstva i revizije.
U novim entitetskim zakonima sadržane su odredbe kojim se precizno uređuje pitanje od značaja za uspostavljanje sistema knjigovodstva i računovodstva, kao što su: preciziranje kriterijuma za razvrstavanje pravnih lica (što je i osnov za primjenu standarda finansijskog izvještavanja te godišnjih izvještaja o poslovanju); jasno definisanje pravila koja se odnose na obaveze popisa imovine i obaveza i druge aktivnosti koje se provode s ciljem usaglašavanja knjigovodstvenog sa stvarnim stanjem; utvrđivanje pitanja koja se odnose na obavezu izrade konsolidovanih izvještaja,u skladu sa pravilima sadržanim u relevantnim MRS/MSFI; utvrđivanje obaveze i obveznika izrade periodičnih finansijskih izvještaja; definisanje obaveze i načina vođenja osnovnih i pomoćnih poslovnih knjiga; utvrđivanje pitanja od značaja za uspostavljanje sistema javnog nadzora nad računovodstvenom i revizorskom profesijom.

Entitetski zakoni o računovodstvu i reviziji su u značajnoj mjeri usaglašeni. Međutim, postoje i određene diskrepanse kako između zakona entiteta, tako i u odnosu na državni zakon. Uporedna analiza odredaba Zakona o računovodstvu i reviziji RS i Zakona o računovodstvu i reviziji u F BIH upravo ima za cilj da pokaže u kojoj mjeri su odredbe entitetskih zakona, nzapravo, međusobno usaglašene, a u čemu su prisutna odstupanja, što može biti polazna osnova za eventualno donošenje jedinstvenog zakonskog okvira kojim će biti uređen računovodstveni i revizijski sistem u našoj zemlji, a koji će u potpunosti odgovarati zahtjevima Evropske unije.

[297] Vidi „Službeni glasnik Bosne i Hercegovine“,broj:42/04

4.18.1. Obveznici primjene zakona

Odredbe entitetskih zakona o računovodstvu i reviziji se primjenjuju na sva privredna društva, uključujući društva za osiguranje, mikrokreditna društva, leasing društva, investicione fondove, društva za upravljanje investicionim fondovima, brokersko-dilerska društva, berze, banke te druge finansijske organizacije, zadruge, profitna i neprofitna pravna lica čije je sjedište registrovano u Federaciji [298], odnosno Republike Srpske[299]. Također, identično je propisano da se odredbe ovih zakona odnose na sva pravna lica i druge oblike organizovanja koje je pravno lice sa sjedištem u Federaciji, odnosno RS osnovalo u inostranstvu, ako propisima tih država nije utvrđena obaveza vođenja poslovnih knjiga I sastavljanja finansijskih izvještaja.

Odredbe ovih zakona odnose se i na poslovne jedinice i pogone pravnih lica sa sjedištem izvan RS[300], ali samo ako se te poslovne jedinice smatraju obveznicima poreza na dobit u Federaciji (prema propisu o porezu na dobit), odnosno ako se preko tih organizacionih jedinica ostvaruje prihod u RS [301].

Također, utvrđeno je da se odredbe entitetskih zakona odnose i na još neke kategorije korisnika, tj. na korisnike prihoda budžeta Federacije, budžeta kantona, budžeta općina i gradova i vanbudžetskih fondova[302] odnosno na korisnike prihoda budžeta Republike, budžeta općina i gradova i budžetskih fondova[303]. Kako je već napomenuto, ovdje je izuzetak napravljen samo kod primjene međunarodnih računovodstvenih standarda, u smislu da se do objavljivanja MR SJS primjenjuju važeći propisi institucija BIH, entiteta i Brčko Distrikta o računovodstvu i finansijskom izvještavanju, dok se ostale opće odredbe Zakona odnose i na ta pravna lica.

Po pitanju obveznika primjene, bitna razlika između entitetskih zakona jeste u tome što je Zakonom o računovodstvu i reviziji Republike Srpske[304], za razliku od Zakona o računovodstvu i reviziji u Federaciji Bosne i Hercegovine, dozvoljena mogućnost da poduzetnici sami izaberu da vode dvojno knjigovodstvo, odnosno da se odluče da li će svoje poslovne knjige voditi po propisima o porezu na dohodak ili po propisima o računovodstvu (u kom slučaju moraju primjenjivati odredbe Zakona o računovodstvu i reviziji RS). S timu vezi, u Republici Srpskoj je donesen Pravilnik o sistemu dvojnog knjigovodstva kod poduzetnika[305]. Na žalost, ovakva mogućnost vođenja računovodstva za poduzetnike nije data poduzetnicima u odredbama Zakonu o računovodstvu i reviziji u Federaciji BiH. Naravno ovo pitanje je višestruko značajno u kontekstu usaglašavanja propisa unutar BIH i u kontekstu potrebe usaglašavanja sa i standardima Evropske unije.

---

298 Vidi „Zakon o računovodsvu i reviziji u Federaciji Bosne i Hercegovine“,član 3(1. i 2.),
299 Vidi „Zakon o računovodsvu i reviziji Repunlike srpske“,član 3(1.i 2.).
300 Vidi„Zakon o računovodsvu i reviziji ,član 3(3).
301 Vidi „Zakon o računovodsvu i reviziji u Federaciji Bosne i Hercegovine“,član 3(3).
301 Vidi „Zakon o računovodsvu i reviziji Repunlike srpske“,član 3(3).
302 Vidi “Zakon o računovodsvu i reviziji u Federaciji Bosne i Hercegovine“,član 3(4).
303 Vidi „Zakon o računovodsvu i reviziji Repunlike srpske“,član 3 (4).
304 Vidi „Zakon o računovodsvu i reviziji Repunlike srpske“,član 3 (1).
305 Vidi “Službeni glasnik RS”,broj 94/09.

4.18.2. Razvrstavanje pravnih lica

Isti i na jednak način su definisani kriteriji za razvrstavanje pravnih,koji su propisani odredbama člana 5. Zakona o računovodstvu i reviziji RS, odnosno članu 4. Zakona o računovodstvu i reviziji F BIH. Sadržjem navedenih odredaba entitetskih zakona utvrđeni su pokazatelji prema kojima se na dan sastavljanja finansijskih izvještaja pravna lica razvrstavaju na mala, srednja i velika,a to su:

- visina prihoda,
- vrijednost imovine,
- prosječan broj zaposlenih u toku poslovne godine,

	Prosječan broj zaposlenih u toku poslovne godine	Prosječna vrijednost poslovne imovine	Ukupan godišnji prihod
Mala pravna lica	Manje od 50	Manje od 1 milion KM	Manji od 2 miliona KM
Srednja pravna lica	50 do 250	od 1 do 4 miliona KM	od 2 do 8 miliona KM
Velika pravna lica	Više od 250	Veća od 4 miliona KM	Veći od 8 miliona KM

Pravna lica se svrstavaju u određene kategorije ukoliko ispunjavaju najmanje dva od navedena tri uslova. Pri tome, u srednja pravna lica razvrstavaju se i ona čije vrijednosti su veće od gornjeg iznosa samo jednog od kriterija propisanih za srednja pravna lica (odnosno koja zadovoljavaju jedan od kriterija propisanih za velika pravna lica).
Pored toga, velika pravna lica se po principu javne odgovornosti uvijek svrstavaju: banke, mikrokreditne organizacije, mikrokreditne zadruge, društva za osiguranje, leasing društva, društva za upravljanje investicionim fondovima, društva za upravljanje obaveznim, odnosno dobrovoljnim penzijskim fondovima, brokersko-dilerska društva i druge finansijske organizacije.

Na dan sastavljanja finansijskih izvještaja pravna lica su dužna samostalno izvršiti razvrstavanje u skladu sa navedenim kriterijima i tako dobivene podatke koristiti za narednu poslovnu godinu. Novoosnovana pravna lica razvrstavaju se na osnovu podataka iz finansijskih izvještaja za tekuću poslovnu godinu,srazmjerno broju mjeseci poslovanja,a dobiveni podaci koriste se za tekuću i narednu poslovnu godinu.

Obavještenje o razvrstavanju pravnog lica u mala srednja ili velika, pravno lice je, uz godišnje finansijske izvještaje, dužno dostaviti instituciji ovlaštenoj za prijem i obradu finansijskih izvještaja. U Republici Srpskoj je to APIF[306], a ovlaštena institucija o kojoj govori Zakon F BIH[307] podrazumijeva Finansijsko-informatičku agenciju (FIA) Federacije BiH, koja se treba formirati ”spajanjem” postojećih agencija AFIP-a d. d. Sarajevo i FIP-a d. d. Mostar koja će preuzeti poslove jedinstvenog prikupljanja, analize i vođenja registra finansijskih izvještaja svih pravnih lica na teritoriji F BiH, u skladu sa Prijedlogom Federalnog Zakona o finansijsko-informatičkoj agenciji,koji se već duže vrijeme nalazi u parlamentarnoj proceduri.

Razvrstavanje na mala, srednja i velika pravna lica je značajna novina koju donose entitetski zakoni, koja predstavlja sa praksom EU i susjednih zemalja. Ova podjela je višestruko značajna ,a posebno sa aspekta:

[306] Vidi „Zakon o računovodstvu i reviziji Republike Srpske“,član 22.
[307] Vidi “Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine“,član 44.

- obima primjene računovodstvenih Standarda,;
- obim i sadržaj obrazaca finansijskih izvještaja;
- revizije finansijskih izvještaja.

Također, navedenim je ispoštovan jedan od najvažnijih zahtijeva Evropske komisije, koja zahtijeva usaglašavanje računovodstvenih propisa Bosne i Hercegovine sa relevantnim direktivama EU. Naravno, potpuno usaglašavanje u kvantitativnom smislu nije moguće s obzirom na to da je po kriterijima Evropske unije najveći broj bosanskohercegovačkih preduzeća male ekonomske snage.

4.18.3. Sistem računovodstva i knjigovodstva

Odredbe kojim je propisana obaveza pravnog lica da donese opći interni akt organizacije računovodstva[308] (član 11. stav 1. Zakona o računovodstvu i reviziji u F BiH i član 6. Zakona o računovodstvu i reviziji RS[309]) su identične. Ovim općim internim aktom pravna lica trebaju da urede,odnosno utvrde organizaciju računovodstva na način koji omogućava sveobuhvatno evidentiranje, kao i sprečavanje i otkrivanje pogrešno evidentiranih poslovnih promjena; interne računovodstvene kontrolne postupke; računovodstvene politike; lica koja su odgovorna za zakonitost i ispravnost nastanka poslovne promjene i sastavljanje i kontrolu knjigovodstvenih isprava o poslovnoj promjeni; kretanje knjigovodstvenih isprava i rokove za njihovo dostavljanje na dalju obradu; postupke pripreme sastavljanja i prezentacije finansijskih izvještaja; postupke prikupljanja, obrade i prezentacije podataka u vezi sa pripremom i sastavljanjem godišnjih izvještaja o poslovanju, te finansijskih podataka za statističke, porezne i druge potrebe i druga pitanja od značaja za uspostavljanje efikasnog sistema knjigovodstva i računovodstva u pravnom licu.

Obaveza donošenja akta o organizaciji računovodstvenog informacijskog sistema,koja je propisana u članu 13. Zakona o računovodstvu i reviziji u F BiH, u Zakonu o računovodstvu i reviziji RS nije posebno utvrđena, a i ovo pitanje je već tretirano u okviru obaveze donošenja općeg internog akta o organizaciji računovodstva. U Zakonu F BiH su sadržane dosta detaljne odredbe o sadržaju ovog akta uključujući način primjene, formiranja, kretanja, odlaganja I čuvanja dokumentacije, kao i postupke, metode i tehnike za vođenje poslovnih knjiga, knjiženje), oblik samih knjiga, sastavni dijelovi poslovnih knjiga itd. (što je sve već okvirno navedeno u članu 11. Zakona o računovodstvu i reviziji u F BiH).

Odredba člana 6. stav 3. Zakona o računovodstvu i reviziji RS kojom je propisana obaveza da pravno lice mora osigurati računovodstveni softver koji omogućava funkcionisanje sistema internih računovodstvenih kontrola i onemogućava brisanje proknjiženih poslovnih događaja (u slučaju da pravno lice vrši obradu podataka na računaru) nije posebno naglašena u Zakonu o računovodstvu i reviziji u F BiH, već se o ovom pitanju (u dijelu koji govori o vođenju poslovnih knjiga na računaru,član 31. Zakona o računovodstvu i reviziji u F BiH) kaže da se u tom slučaju, uporedo sa memorisanim podacima,moraju osigurati i memorisanje aplikativnog softvera, kako bi podaci bili dostupni kontroli.

[308] Vidi „Zakon o računovodstvu i reviziji u Fedearacije Bosne i Hercegovine“,član 11.stav 1
[309] Vidi „Zakon o računovodstvu i reviziji Republike Srpske“, član 6.

4.18.3.1. Knjigovodstvene isprave

Knjigovodstvena isprava je u entitetskim zakonima definisana na istovjetan način, izuzev što se u Zakonu o računovodstvu i reviziji u F BiH kaže da je to pisani dokaz (a ne dokument kako stoji u Zakonu o računovodstvu i reviziji RS) o nastaloj poslovnoj promjeni[310]. Također, fotokopija knjigovodstvene isprave nije posebno razdvojena u Zakonu o računovodstvu i reviziji u F BiH od isprave u vidu elektronskog zapisa, kao što je to u Zakonu o računovodstvu i reviziji RS[311].

Podjela na knjigovodstvene isprave interne i eksterne prirode,kao i primjeri jednih i drugih posebno su navedeni samo u Zakonu o računovodstvu i reviziji u F BIH[312], u što se Zakon o računovodstvu i reviziji RS nije upuštao.

Pitanju kontrole knjigovodstvene isprave i ispravki u knjigovodstvenim ispravama više pažnje je posvećeno u Zakonu o računovodstvu i reviziji u F BiH[313] (član 17.,18. i 19.) u odnosu na Zakon o računovodstvu i reviziji RS.

Rok za dostavljanje knjigovodstvenih isprava računovodstvu od 3 (tri) dana od dana kada je poslovna promjena nastala, odnosno kada je knjigovodstvena isprava primljena, jednak je oba enitetska zakona[314].

Rok za knjiženje knjigovodstvene isprave u poslovnim knjigama je, također, definisan na isti način zakona u oba entitetska tj. u roku 8 (osam) dana od dana prijema knjigovodstvene isprave[315].

Napomena edukatorima

Iako će učesnici edukacije biti tužioci i pripadnici agencija za sprovođenje zakona, smatramo uputnim da im edukatori kroz praktične primjere predstave neke od knjigovodsvenih isprava sa osvrtom na njihov nastanak, elemente , hodogram, kontrola, knjigovodstveni tretman i čuvanje.

Edukatori također treba da osiguraju da učesnici kroz praktičnim primjerima usvoje osnovne tehnike identifikacije za finansijsku istragu nephodnih kjigovodstvenih isprava i mjesta na kojima su generisana ,evidentirana i čuvaju se.

4.18.3.2. Poslovne knjige

Odredbe entitetskih zakona su i po pitanjima definicije poslovnih knjiga dosta slične,a u nekim svojim dijelovima i potpuno identične.

---

[310] Vidi „ Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine“,član 14(1) i Zakon o reviziji i računovodstvu Repunlike Srpske“,član 7 (1).

[311] Vidi „ Zakon o reviziji i računovodstvu Repunlike Srpske“,član 7(3.i 4.).

[312] Vidi „ Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine“,član 16(2.,3.i 4)

[313] Vidi „ Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine“,član 17.,18. i 19.

[314] Vidi „ Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine“,član 16.(6.). i Zakona o računovodstvu i reviziji Republike Srpske“,član 8.tačka 5

[315] Vidi „ Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine“,član 19.(2) i Zakona o računovodstvu i reviziji Republike Srpske“, član 16. stav 6. Zakona RS).

Poslovne knjige su definisane kao jednoobrazne evidencije o stanju i promjenama na imovini, obavezama, kapitalu, prihodima i rashodima pravnih lica. Čine ih: dnevnik, glavna knjiga i pomoćne knjige. Propisano je da se poslovne knjige[316] u Zakonu o računovodstvu i reviziji u F BiH, odnosno dnevnik i glavna knjiga[317] prema Zakonu o računovodstvu i reviziji RS) vode po sistemu dvojnog knjigovodstva. U Zakonu F BiH je dodatno propisano da se poslovne knjige mogu voditi na slobodnim listovima, povezane ili prenijete na neki od elektronskih medija,tako da se, po potrebi, mogu odštampati ili prikazati na računaru[318]. Kod elektronskog vođenja poslovnih knjiga, u Zakonu RS, u kojem, inače, nije posebno naveden oblik u kojem se mogu voditi poslovne knjige, se kaže samo da je u slučaju kada se poslovne knjige vode u elektronskom obliku pravno lice, odnosno organizacioni dio pravnog lica ili poduzetnik (u smislu kontrole) ovlaštenim kontrolnim organima moraju osigurati pristup centralnoj bazi podataka, radi nesmetane kontrole poslovnih knjiga[319].

Definisano je da je dnevnik poslovna knjiga u koju se poslovni događaji nastali u toku obračunskog perioda unose hronološki, prema redoslijedu njihovog nastanka (u Zakonu o računovodstvu i reviziji F BiH se dodaje da se dnevnik može uspostaviti kao jedinstvena poslovna knjiga ili više knjiga koje su namijenjene za evidentiranje promjena na pojedinim skupinama bilansnih i vanbilansnih pozicija)[320].

Glavna knjiga se definiše na sličan naču in, pa se tako u Zakonu o računovodstvu i reviziji RS kaže da je to sistemska evidencija u kojoj se prikazuju stanja i promjene na imovini, obavezama, vlastitom kapitalu, prihodima i rashodima. U toku obračunskog perioda i koja predstavlja osnov za izradu finansijskih izvještaja[321].

Pomoćne knjige se definišu kao analitičke evidencije koje se vode za nematerijalna ulaganja, nekretnine, postrojenja i opremu, plasmane, finansijske plasmane, zalihe, gotovinu i gotovinske ekvivalente, obaveze, kapital i druge bilansne pozicije[322] (potpuno identično u Zakonu o računovodstvu i reviziji u F BiH I Zakonu o računovodstvu i reviziji RS). Razlika je u tome što su odredbe Zakona o računovodstvu i reviziji u F ederaciji Bosne i Hercegovine nešto detaljnije pa se tako u sadržaju odredabačlanu 22. poimenično navode druge pomoćne knjige koje dopunjavaju podatke u nekoj poziciji u glavnoj knjizi ili osiguravaju bilo koje druge podatke: knjiga (dnevnik) blagajne, knjiga ulaznih faktura (KIF),knjiga deviznih sredstava, knjiga izdatih čekova, knjiga dospijeća mjenica, knjiga dionica, knjiga udjela I dr.), dok je u odredbama članu 10. Zakona o računovodstvu i reviziji RS sadržana samo opća odredba da se broj i sadržaj pomoćnih knjiga, način njihovog vođenja i povezivanja sa glavnom knjigom i slično, pravno lice ili poduzetnik uređuje svojim opštim aktom u skladu sa zakonom.

[316] Vidi"Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine",član 20(2),
[317] Vidi"Zakon o računovodstvu i reviziji Republike Srpske",član 10(3.
[318] Vidi „Zakon o računovodstvu i reviziji u Federacije Bosne i Hercegovine",član 20(3).
[319] Vidi"Zakon o računovodstvu i reviziji Republike Srpske",član 13(8).
[320] Vidi"Zakon o računovodstvu Republike Srpske",član 10(3) i Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine",član 20(5).
[321] Vidi"Zakon o računovodstvu Republike Srpske",član 10(5) i Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine",član 21(4).
[322] Vidi"Zakon o računovodstvu Republike Srpske",član 10(6) i Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine",član 22(1. i 2.).

Odredbe federalno Zakona o sastavu glavne knjige (bilansna i vanbilansna evidencija) i uslova za evidentiranje poslovnih promjena u blansnoj evidenciji (da se poslovni događaj stvarno dogodio i da kao takav pripada prošlosti poslovanja, da se njegov učinak može novčano izraziti,da promjena nastala poslovnim događajem utiče na poziciju sredstava, obaveza, kapitala, troškova, rashoda, prihoda i rezultata poslovanja i da se nastanak poslovnog događaja može dokazati vjerodostojnom knjigovodstvenom ispravom)[323] nisu predmet sadržaja odredaba Zakon o računovodstvu i reviziji RS. Također, naglašava se da u slučaju promjene metoda elektronske obrade podataka,glavna knjiga mora biti tako organizovana da se može izvršiti kontrola knjiženja[324].

4.18.3.2.1. Vođenje poslovnih knjiga

Sadržaj odredbe članova Zakona o računovodstvu i reviziji u F BiH i Zakona o računovodstvu i reviziji RS koje regulišu način vođenja poslovnih knjiga su uglavnom usaglašene, a odnose se na uslove koje mora ispunjavati lice koje vodi poslovne knjige, koje se utvrđuju aktom pravnog lica (i poduzetnika prema Zakonu o računovodstvu i reviziji RS)[325].

Djelomična razlika je međutim, u odredbama koje se odnose na situaciju kada se vođenje poslovnih knjiga povjerava licu ili poduzetniku registrovanom za pružanje računovodstvenih usluga, gdje se kao uslov u Zakonu o računovodstvu i reviziji F BIH navodi samo da to pravno lice ili poduzetnik ima zaposlena lica kojima povjerava vođenje poslovnih knjiga i sastavljanje finansijskih izvještaja, bez uslova da ta lica budu kvalificirana i da ispunjavaju i druge uslove utvrđene ovim zakonom i općim aktom pravnog lica, što se postavlja kao uslov u Zakonu o računovodstvu i reviziji RS[326].

Inače,mogućnost i modaliteti uslužnog vođenja poslovnih knjiga pravnih lica u narednom periodu su jedno od pitanja oko kojeg već postoje brojni praktični problemi i dileme, čije se rješavanje očekuje uskoro, pogotovo stoga što je obaveza ispunjavanja navedenog uslova "zapošljavanja" (još makar jednog lica), prelaznim odredbama Zakona o računovodstvu i reviziji u F BiH, prolongirana do početka 2011. godine.

Naponena edukatorima

Na praktičnom primjeru objasniti značenje,otvaranje,vođenje i zaključivanje poslovnih knjiga koje vode pravna lica i poduzetnici i njihov značaj za sastavljanje finansijskih izvještaja, obračunavanje i plačanje fiskalnih obaveza i sl.

4.18.3.3. Kontni okvir

[323] Vidi „Zakon o računovodstvu i reviziji u federaciji Bosne i Hercegovine",član 21.stav 6

[324] Vidi „Zakon o računovodstvu i reviziji u federaciji Bosne i Hercegovine",član 21.stav 8.

[325] Vidi"Zakon o računovodstvu Republike Srpske",član 12(1) i Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine",član 24(1).

[326] Vidi"Zakon o računovodstvu Republike Srpske",član 12(2) i Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine",član 24(2).

Odredbe Zakona o računovodstvu i reviziji u F BiH I Zakona o računovodstvu i reviziji RS o knjiženju poslovnih promjena po osnovu kontnog plana su potpuno iste.. Također, formalna nadležnost za donošenje kontnog okvira (plana) je i prema jednom i drugom zakonu, data Ministarstvu ,a ne kako se očekivalo Savezu, kao profesionalnom tijelu).

4.18.3.4. Popis imovine i obaveza

Popis imovine i obaveza je detaljnije regulisan u Zakonu o računovodstvu i reviziji u F BiH u odnosu na Zakon o računovodstvu i reviziji RS. Obaveze popisa za pravna lica i dijelove tih pravnih lica koja obavljaju poslove u inostranstvu (ako stranim propisima za pravna lica i njihove dijelove nije propisana obaveza posebnog vođenja knjigovodstva), obaveza podnošenja i revizije godišnjih finansijskih izvještaja, kao i obaveza popisa za pravno lice kod kojeg se nalaze tuđa sredstva, postupak provođenja popisa u skladu sa internim aktom i Odlukom o popisu, u smislu određivanja komisije, način i rokove popisa i dr. su pitanja koja u RS nisu posebno definisana na način kao što je to utvrđeno u Zakonu F BiH[327].

U Zakonu o računovodstvu i reviziji RS sadržane su samo odredbe koje se tiču rokova popisa, pa se tako propisuje obaveza popisa imovine i obaveza za pravna lica ili poduzetnike na početku poslovanja kao i najmanje jednom godišnje, sa stanjem na dan kada se završava poslovna godina ili neki drugi obračunski period određen u skladu sa ovim zakonom,izvrše popis imovine i obaveza s ciljem da utvrde njihovo stvarno stanje, te da stanje u poslovnim knjigama usklade sa stvarnim stanjem utvrđenim popisom, ali se daje i mogućnost da pravno lice i poduzetnik svojim općim aktom odrede i druge rokove za popis.

Zakonom o računovodstvu i reviziji u F BiH nije predviđena mogućnost da se odredbe i neki drugi rokovi za popis, a mogućnost dužih perioda za popis predviđena je samo za popis materijala u knjižnicama, kao što su: knjige, fotografije, filmovi, arhivska građa i slično, s tim da ti periodi ne mogu biti duži od pet godina[328] (član 25. stav 8. Zakona o računovodstvu i reviziji u F BIH).Zakonom o računovodstvu i reviziji u F BIH i Zakonom o računovodstvu i reviziji RS je propisana obaveza popisa u slučajevima promjene cijene,statusnih promjena, otvaranja stečajnog, odnosno likvidacionog postupka, kao i kod primopredaje dužnosti računopolagača (s tim da u Zakonu F BiH u članu 25. stav 6. stoji samo primopredaje dužnosti, bez naglašavanja na koga, što se jasno kaže u članu 15. stav 5. Zakona RS).

Detalji oko načina popisa u smislu određivanja lica koja mogu biti u popisnoj komisiji, odnosno da u popisnoj komisiji ne mogu biti lica koja su materijalno ili finansijski zadužena za sredstva koja popisuju i njihovi neposredni rukovodioci; da podatke iz knjigovodstva ne unose lica iz knjigovodstva, već popisna komisija; da sastavljanje izvještaja i utvrđivanje viškova i manjkova vrši popisna komisija i najkasnije 15 dana od dana isteka poslovne godine vrši njegovo dostavljanje nadležnom tijelu na razmatranje, pitanja su koja prema članu 26. Zakona o računovodstvu i reviziji F BiH pravno lice treba da uredi svojim općim internim aktom i Odlukom o popisu, dok u Zakonu o računovodstvu i reviziji RS ovi detalji oko načina popisa nisu posebno regulisani.

[327] Vidi"Zakon o računovodstvu Republike Srpske",član 15 i Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine",član 25. i 26.
[328] Vidi „Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine",član 25(8).

Napomena edukatora

S obzoirom na značenje popisa za finansijsku istragu primjerom godišnjeg popisa objasniti njegov uticaj na bilansne pozicije pravnih lica.

4.18.3.5. Obračun amortizacije

U odredbama Zakona o rašunovodstvu i reviziji RS, za razliku od Zakona o računovodstvu i reviziji u F BiH, uopće nisu sadržane odredbe koje govore o načinu obračuna amortizacije[329](a radi se materiji koja je već uređena u MRS/MSFI).

4.18.3.6. Usaglašavanje potraživanja i obaveza

Obaveza usaglašavanja međusobnih potraživanja i obaveza (konfirmacija salda) prije sastavljanja godišnjih izvještaja, kao i način dokazivanja odgovarajućom knjigovodstvenom ispravom, propisani su na sličan način u oba entitetska zakona, ali i u tom dijelu ima izvjesnih razlika.

Prema Zakonu o rašunovodstvu i reviziji u F BiH, obaveza primaoca konfirmacije je da pošiljaocu/dužniku, povjeriocu ili njegovom revizoru) odgovori na konfirmaciju u roku od osam dana (uz propisani novčanu kaznu od 5.000 do 15.000 KM ukoliko na konfirmaciju ne odgovori u utvrđenom roku)[330], dok se u Zakonu o računovodstvu i reviziji RS ne navodi takav poseban rok. Također, u Zakonu o računovodstvu i reviziji u F BIH ne pravi se jasna razlika između IOS-a i revizorskih konformacija, s obzirom na propisanu obavezu usaglašavanja svih potraživanja i obaveza po stanju na dan 31.12[331]. U Zakonu o računovodstvu i reviziji RS je propisano da pravno lice ima obavezu da odgovori na zahtjev ovlaštenog revizora za potvrdu stanja potraživanja i obaveza, iz čega proizlazi da su revizori dužni da provode proceduru konfirmacije i svi oni kojima revizor uputi zahtjev za konfirmaciju su dužni da na njega odgovore[332].

Obaveza povjerioca da prije sastavljanja finansijskih izvještaja dužniku dostavi spisak neplaćenih računa, propisana u Zakonu o računovodstvu i reviziji u F BiH, nije izričito sadržana u Zakonu RS[333].U oba zakona je propisana je obaveza da se u bilješkama (napomenama), uz finansijske izvještaje, navedu i obrazlože sva neusaglašena stanja potraživanja i obaveza, s tim da u Zakonu RS nije predviđena obaveza planiranja aktivnosti o tom pitanju i način njihovog rješavanja, kao što je propisano u Zakonu F BiH[334].

4.18.3.7. Zaključivanje poslovnih knjiga i utvrđivanje finansijskog rezultata

Na potpuno isti način je propisano da se poslovne knjige zaključuju poslije knjiženja svih poslovnih promjena i obračuna na dan završetka poslovne godine najkasnije do roka za dostavljanje finansijskih izvještaja, kao i u slučajevima statusnih promjena, prestanka poslovanja i u drugim slučajevima u kojima je neophodno zaključiti poslovne knjige[335].

[329] Vidi „Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine“,član 27.
[330] Vidi „Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine“,član 28(4).
[331] Vidi „Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine“,član 28(5).
[332] Vidi“Zakon o računovodstvu i reviziji Republike Srpske“,16(2).
[333] vidi„Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine“,član 28(2).
[334] vidi„Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine“,član 28(6)i “Zakona o računovodstvu i reviziji Republike Srpske“,16(3).
[335] Vidi“Zakon o računovodstvu i reviziji u Federaciji Bosne i hercegovine,član 29(1) i „Zakon o računovodstvu i reviziji Republike srpske,član 11(6).

U Zakonu računovodstvu i reviziji F BIH , u slučaju kada se poslovne knjige vode kao elektronski zapis, glavna knjiga se mora nakon zaključivanja na kraju poslovne godine zaštititi na način da nije moguća izmjena pojedinih ili svih njenih dijelova ili listova,da ju je moguće u svakom trenutku odštampati na papir i da se mora potpisati elektronskim potpisom u skladu sa Zakonom o elektronskom potpisu ili se mora odštampati na papir i uvezati na način da nije moguća izmjena pojedinih ili svih njenih dijelova ili listova i mora je potpisati i ovjeriti lice ovlašteno za zastupanje pravnog lica i na kraju odložiti[336].

Također, Zakon o računovodstvu i reviziji F BiH se upušta i u pitanje raspoređivanja dobiti i pokriće gubitka, što pravno lice treba da vrši u skladu sa odredbama Zakona o privrednim društvima i odredbama Zakona o računovodstvu i reviziji F BIH, internog općeg akta i odluke nadležnog organa[337]. U Zakonu RS nisu posebno navedene slične odredbe jer su smatrali da se radi se o materiji koja je već uređena drugim propisima (kao što je zakon o privrednim društvima) i internim aktima samog pravnog lica.

4.18.3.8. Način i rokovi čuvanja knjigovodstvene dokumentacije

Način čuvanja knjigovodstvenih isprava je na identičan način propisan u oba entitetska zakona, s tim da u Zakonu o računovodstvu i reviziji RS nema odredbi o "odlaganju u fascikle i registratore", arhiviranju knjigovodstvenih isprava i slične odredbi koje sadržava Zakon računovodstvu i reviziji u F BiH.

U oba zakona je propisano da se knjigovodstvene isprave čuvaju u izvornom materijalnom I elektronskom obliku,u obliku elektronskog zapisa ili na mikrofilmu, te da se čuvaju u poslovnim prostorijama pravnog lica, odnosno organizacionog dijela pravnog lica ili lica kome je povjereno vođenje poslovnih knjiga.

Kada je riječ o rokovima čuvanja, trajno se čuvaju:

- Platne liste ili analitičke evidencije o plaćama u vezi sa plaćanjem doprinosa (isto u oba entitetska zakona),
- Kupoprodajni ugovori po kojima je izvršeno sticanje nekretnina (prema Zakonu F BiH), odnosno "isprave kojima se dokazuju vlasništvo I vlasnički odnosi na nekretninama" (član 9. stav 2. Zakona o računovodstvu i reviziji RS),
- Hartije od vrijednosti (navedeno samo u Zakonu RS),
-

Prema odrebama člana 31(6) Zakonu o računovodstvu i reviziji u F BiH, trajno se čuvaju još i:

- Godišnji računovodstveni obračun,
- Finansijski izvještaji,
- Konsolidirani finansijski izvještaji,
- Izvještaji o izvršenoj reviziji i svi interni akti od uticaja na finansijsko poslovanje.

Prema odredbama člana 13 (2) Zakonu o računovodstvu i reviziji RS, finansijski izvještaji i izvještaji o reviziji se, također, čuvaju trajno, u originalnom obliku.

[336] Vidi"Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine,član 29(3).
[337] Vidi"Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine,član 30(2).

Knjigovodstvene isprave na osnovu kojih su podaci uneseni u dnevnik I glavnu knjigu čuvaju se najmanje jedanaest godina, odnosno knjigovodstvene isprave na osnovu kojih su podaci uneseni u pomoćne knjige čuvaju se najmanje sedam godina[338]. Prema Zakonu o računovodstvu i reviziji RS, rok čuvanja knjigovodstvenih isprava na osnovu kojih su podaci uneseni u poslovne knjige je najmanje pet godina ili duže, ako su posebnim propisima određeni duži rokovi za čuvanje pojedinih vrsta isprava[339].

Glavna knjiga i dnevnik čuvaju se najmanje jedanaest godina (Zakon o računovodstvu i reviziji F BiH)[340], odnosno najmanje deset godina (Zakon o računovodstvu i reviziji RS)[341]. Pomoćne knjige se, prema odredbama Zakonu računovodstvu i reviziji F BiH, čuvaju najmanje sedam godina[342],dok je rok za čuvanje pomočnih knjiga prema odredbama zakona o računovodstvu i reviziji RS najmanje pet godina[343]. Periodični obračuni, kao i isprave platnog prometa putem ovlaštenih finansijskih institucija čuvaju se najmanje pet godina[344]. Godišnji izvještaj o poslovanju čuva se u originalnom obliku jedanaest godina nakon isteka poslovne godine[345]. Pomoćni obračuni, prodajni ni kontrolni blokovi i sl. čuvaju se dvije godine[346] . Revizorska društva čuvaju šest godina dokumentaciju na osnovu koje je obavljena revizija[347], odnosno (dokumentaciju na osnovu koje je obavljena revizija društva za reviziju imaju obavezu da čuvaju najmanje pet godina[348].

Na temelju navedenih odredbi i njihove komparacije može zaključiti da su rokvi za čuvanje knjigovodstvenih isprava , poslovnih knjiga i dokumentacije propisani odredbama Zakonu računovodstvu i reviziji RS kraći u odnosu na rokove čuvanja dokumentacije, knjigovodstvenih isprava i poslovnih knjiga iz Zakon o računovodstvu i reviziji u F BIH.

4.18.3.9. Finansijsko izvještavanje

O ovom pitanju odredbečlanova 35., 36., 37. i 38. Zakona o računovodstvu i reviziji u F BiH su suštinski identični sa članovima 17. i 18. Zakona o računovodstvu i reviziji RS. Razlika je samo u formulaciji, gdje se u članu 35. Zakona F BiH kaže da ”pravna lica finansijske izvještaje sastavljaju i prezentiraju za poslovnu godinu i to za period od 1. januara do 31. decembra tekuće godine sa usporedivim podacima za prethodnu godinu”,umjesto”za poslovnu godinu završenu 31.decembra tekuće godine sa uporednim podacima za prethodnu godinu” kako se navodi u odredbama članu 17. Zakona o računovodstvu i reviziji RS što je po profesionalnom sudu ispravnije, jer samo neki elementi finansijskih izvještaja predstavljaju izvještaj ”za period”, dok ostali izvještaji pokazuju stanje “na dan”.

[338] Vidi“Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine,član 32(1.i 2.).
[339] Vidi „Zakon o računovodstvu i reviziji Republike Srpske“,član 9(3).
[340] Vidi“Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine,član 32(1).
[341] Vidi „Zakon o računovodstvu i reviziji Republike Srpske“,član 13(3).
[342] Vidi“Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine,član 32(1).
[343] Vidi Zakon o računovodstvu i reviziji Republike Srpske“,član 13(4).

[344] Vidi“Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine,član 32(2).

[345] Vidi Zakon o računovodstvu i reviziji Republike Srpske“,član 13(4) i “Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine,član 32(3).

.
[346] Vidi“Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine,član 32(4).

[347] Vidi“Zakon o računovodstvu i reviziji u Federaciji Bosne i Hercegovine,član 32(5).
[348] Vidi Zakon o računovodstvu i reviziji Republike Srpske“,član 13(5).

Predviđeno je i da zavisno pravno lice čije matično pravno lice sa sjedištem u inostranstvu ima poslovnu godinu različitu od kalendarske, uz saglasnost ministra, može sastavljati i prezentirati finansijske izvještaje za period koji je različit od prethodno navedenog perioda. Također, pravno lice kod kojeg nastane statusna promjena, finansijski izvještaj sastavlja na dan statusne promjene, a poslovni događaji nastali između dana bilansa i dana upisa u sudski registar obuhvataju se u finansijskom izvještajima prethodnog pravnog lica ili novog pravnog lica, što se utvrđuje odlukom o statusnoj promjeni.

Finansijski izvještaji sastavljaju se u slučaju otvaranja, odnosno zaključenja stečaja, odnosno postupka likvidacije pravnog lica.

Godišnje finansijske izvještaje čine: bilans stanja-izvještaj o finansijskom položaju na kraju perioda, bilans uspjeha-izvještaj o ukupnom rezultatu za period, izvještaj (bilans) o gotovinskim tokovima-Izvještaj o tokovima gotovine, Izvještaj o promjenama na kapitalu i bilješke (napomene) uz finansijske izvještaje.

Izuzetno, mala pravna lica (a u RS i poduzetnici koji vode dvojno knjigovodstvo) su obavezna sastavljati samo bilans stanja i bilans uspjeha.[349]

Također, identično je utvrđeno da se korisnicima finansijskih izvještaja, uz godišnji finansijski izvještaj, prezentira i poseban izvještaj sačinjen prema zahtjevu Federalnog (odnosno Republičkog) zavoda za statistiku.

Za finansijske izvještaje utvrđen je odgovornost lica koje je ovlašteno za zastupanje pravnog lica,upisano u sudski registar.

Međutim po pitanju obaveze ovjere finansijskih izvještaja postoji razlika u članu 37. Zakona o računovodstvu i reviziji u F BiH u odnosu na odgovarajuće odredbe člana 17. Zakona o računovodstvu i reviziji RS. Naime u članu 17. stav 10. Zakonu RS se kaže da ”finansijske izvještaje pravnog lica potpisuju lice ovlašteno za zastupanje pravnog lica upisano u sudski registar i stručno osposobljeno lice iz člana 12. ovog zakona (lice sa odgovarajućom licencom) koje je, u skladu sa odredbama ovog zakona i općim aktom pravnog lica, ovlašteno da sastavlja izvještaje”. U članu 37. stav 2. Zakona F BiH stoji da ”finansijski izvještaji pravnog lica pa i oni štampani na računaru, moraju biti ovjereni potpisom i pečatom certificiranog računovođe koji sadrži naziv “certificirani računovođa”, njegovo ime i prezime, kao i broj važeće licence, izuzev za certificirane računovođe iz člana 5. stava 6. ovog zakona. Istovremeno, finansijski izvještaji moraju biti potpisani od strane lica ovlaštenog za zastupanje pravnog lica, upisanog u sudski registar, koje podnosi izvještaje, ovjerene pečatom pravnog lica-podnosioca. Slijedi logičan zaključak, da samo certificirani računovođa (a ne i, eventualno certificirani računovodstveni tehničar), prema Zakonu o računovodstvu i reviziji u F BiH, može ovjeriti finansijske izvještaje pravnog lica.

Odredbma člana 18. Zakona o računovodstvu i reviziji RS i člana 38. Zakona o računovodstvu i reviziji F BiH u kojima se propisuje obaveza sastavljanja i prezentovanja polugodišnjih izvještaja se ne razlikuju. Naime, propisano je da su pravna lica koja su razvrstana u velika i srednja dužna sastavljati i prezentirati polugodišnje finansijske izvještaje, tj. finansijske izvještaje pripremljene za obračunski period od 1. januara do 30.

[349] Vidi Zakon o računovodstvu i reviziji Republike Srpske“,član 17(7).

juna, ali i ona pravna lica čijim se vrijednosnim papirima trguje na tržištu kapitala ili su u postupku pripreme za izlazak na ta tržišta obavezna su sastavljati i prezentirati polugodišnje finansijske izvještaje, ako je takva obaveza predviđena propisima kojima se uređuje poslovanje vrijednosnim papirima. Sadržajem odredaba člana 39(1). Zakona o računovodstvu i reviziji u F BiH, identično kao i u članu 21. stav 1. Zakona o računovodstvu i reviziji RS, kaže se da ministar propisuje sadržaj i formu finansijskih izvještaja koji se pripremaju i prezentuju u skladu sa ovim Zakonom (s tim da se u stavu 2. člana 21. Zakona o računovodasvu i reviziji RS naglašava da poduzetnici koji su se, u skladu sa ovim zakonom, opredijelili da vode dvojno knjigovodstvo, svoje finansijske izvještaje pripremaju na odgovarajućim obrascima finansijskih pripisanim za pravna lica). U stavu 2. člana 39. Zakona o računovodstvu i reviziji F BIH je naglašeno da ”pravna lica koja knjigovodstvo vode na sredstvima za automatsku obradu podataka, finansijski izvještaj mogu predati i na propisanoj formi obrasca štampanom na računaru s tim da, uz takve obrasce, istovjetne podatke podnesu i na elektronskom mediju”(što nije posebno istaknuto u Zakonu o računovodstvu i reviziji RS).

4.18.3.10. Godišnji izvještaj o poslovanju

Odredbe entitetskih zakona o godišnjem izvještaju o poslovanju su identične, s tim da je u Zakon o računovodstvu i reviziji F BiH (uslijed razdvajanja ovih odredaba u dva člana, u odnosu na samo jedan član u Zakonu o računovodstvu RS) proizašla tehnička nepodudarnost, jer u članu 41. stav 2. Zakona F BiH, umjesto ”izuzetno od odredaba iz stava 1. ovog člana” treba da stoji „*izuzetno od odredaba iz stava 1. člana 40.“*

Inače,odredbama oba entitetska zakona je propisana obaveza za srednja i velika pravna lica da (uz ostale godišnje finansijske izvještaje) pripreme i tzv. godišnji izvještaj o poslovanju u kome će dati objektivan prikaz poslovanja pravnog lica i njegov položaj, uključujući i opis glavnih rizika i neizvjesnosti sa kojima se suočava i mjera poduzetih na zaštiti životne sredine, te je i njegov sadržaj na potpuno identičan način utvrđen u odredbama entitetskih zakona.

Mala pravna lica su izuzeta od obaveze,s tim da je Zakonu o računovodstvu i reviziji F BiH navedeno da su i ona dužna da informacije o otkupu vlastitih dionica navedu u zabilješkama uz finansijske izvještaje.

4.18.3.11. Konsolidirani finansijski izvještaj

Obavezu izrade konsolidiranih finansijskih izvještaja, prema Zakonu o računovodstvu i reviziji u F BiH, imaju statusni oblici povezivanja u skladu sa Zakonom o privrednim društvima. Prema Zakonu računovodstvu i reviziji RS, konsolidovanim finansijskim izvještajem smatraju se finansijski izvještaji pripremljeni na nivou grupe međusobno povezanih pravnih lica koja čine jednu ekonomsku cjelinu, u skladu sa stavom 2. člana 19. Zakona o računovodstvu i reviziji RS.

Dakle, u F BIH je obaveza sačinjavanja i predaje konsolidovanih izvještaja propisana za statusne oblike povezivanja, pri čemu se Zakon o račiunovodtvu i reviziji F BIH poziva na odredbe Zakona o privrednim društvima koje govore o statusnim oblicima povezanosti pravnih lica.

Prema Zakonu o računovodstvu i reviziji RS, ova obaveza se vezuje uz određene kriterije za definisanje ekonomske cjeline, pri čemu ekonomsku cjelinu u izvještajnom smislu mogu da čine: pravno lice koje ostvaruje kontrolu nad jednim ili više pravnih lica i kontrolisana pravna lica (matično i zavisna pravna lica), zatim pravna lica koja učestvuju u zajedničkoj kontroli nad jednim ili više pravnih lica, i pravno lice koje ostvaruje značajan uticaj nad jednim ili više pravnih lica (pridružena pravna lica). Također, prema Zakonu RS, konsolidovane finansijske izvještaje pripremaju i prezentuju pravna lica koja, direktno ili indirektno ostvaruju kontrolu nad jednim ili više povezanih pravnih lica, koja sa drugim pravnim licima učestvuju u zajedničkoj kontroli nad drugim pravnim licima ili koja nad drugim (pridruženim) pravnim licima ostvaruju značajan uticaj.

Pri tome, u odredbama Zakona o računovodstvu i reviziji BiH nije učinjen izuzetak od obaveze pripreme i prezentacije konsolidovanih finansijskih izvještaja na nivou grupe ukoliko su zadovoljeni određeni uslovi, kao što je to propisano u članu 19. stav 4. Zakona o računovodstvu i reviziji RS. Naime, u slučaju da grupa povezanih pravnih lica zadovoljava kriterije u pogledu ukupne vrijednosti imovine ili ukupnog prihoda (ne računajući efekte internih transakcija između tih povezanih lica), po kojima se svrstava u kategoriju malih pravnih lica, Zakonom o raćčunovodstvu i reviziji RS je propisano da u tom slučaju nema obaveze pripreme i prezentacije konsolidovanih finansijskih izvještaja na nivou grupe.

U odredbama oba zakona je naglašeno da se pri izradi konsolidovanih finansijskih izvještaja koriste pravila i procedure sadržane u relevantnim računovodstvenim standardima.

Napomena edukatoru

Svaki od navedenih izvještaja kratko predstaviti i objasniti njegovo značenje informacija koje se nalaze u sadržaju istih.

4.18.3.12. Predaja polugodišnjih i godišnjih finansijskih izvještaja

Odredbe entitetskih zakona u kojima se razrađuje pitanje predaje finansijskih izvještaja su u osnovi, dosta podudarne. Naime, propisana je obaveza predaje finansijskih izvještaja Ovlaštenoj instituciji ,odnosno APIF-u , i to polugodišnjeg najkasnije do posljednjeg dana februara tekuće godine za prethodnu godinu.

Razlike su slijedeće:

- rok za predaju konsolidovanih finansijskih izvještaja je mart (prema Zakonu o računovodstvu i reviziji RS) dok je prema Zakonu o računovodstvo i reviziju F BIH rok april tekuće godine za prethodnu godinu;
- odredbama Zakona o računovodstvu F BiH i RS, posebno propisani rokovi za predaju finansijskih izvještaja o statusnim promjenama, pa se kaže da godišnje finansijske izvještaje pravno lice treba dostaviti u roku od 60 dana od dana nastanka statusne promjene, pokretanje postupka likvidacije ili otvaranje stečaja, a za ostale poslovne godine u roku od 120 dana od dana isteka poslovne godine;
- Obaveza predaje odluke o utvrđivanju finansijskih izvještaja, odluke o prijedlogu raspodjele dobiti ili pokriću gubitka (ili izjave o neaktivnosti), koje se sa odredbama člana 44. Zakona o računovodstvu i reviziji u F BiH, predaju uz finansijske izvještaje, nije predviđena u Zakonu o računovodstvu i reviziji RS;

- U članu 44. Zakona o računovodstvu i reviziji F BiH je propisan obaveza predaje revizorskog izvještaja sa priloženim finansijskim izvještajima koji su bili predmet revidiranja do kraja tekuće godine za prethodnu godinu, dok u Zakonu nije propisana obaveza.

4.18.3.13. Nadzor

Ovlaštenje za nadzor nad aktivnostima pravnih lica (u RS i poduzetnika), zbog provjere da li se te aktivnosti koje su od značaja za organizaciju i funkcionisanje sistema knjigovodstva i računovodstva (kao i pripremu i prezentaciju finansijskih izvještaja, prema zakonu RS) obavljaju u skladu sa odredbama ovog i drugih relevantnih zakona i propisa donesenih na osnovu tih zakona,u zakonu F BiH I Zakonu RS je različito uspostavljeno. Naime, prema Zakonu F BiH,nadzor vrši Porezna uprava Federacije Bosne i Hercegovine,dok je Zakonom RS ovlaštenje za nadzor (uključujući i "nadzor i nad radom pravnih lica i poduzetnika registrovanih za pružanje računovodstvenih usluga") dato Ministarstvu finansija Republike Srpske.

Nadzor,pri tome, podrazumijeva praćenje, prikupljanje knjigovodstvenih isprava, poslovnih knjiga, (godišnjih) finansijskih izvještaja, te drugih poreznih i statističkih izvještaja, odnosno svih informacija koje su potrebne za provjeru aktivnosti od značaja za organizaciju i funkcionisanje sistema knjigovodstva i računovodstva, u smislu proceduralnih aktivnosti (bez nadzora nad primjenom MRS/MSFI).

U odredbama i jednog i drugog zakona rečeno je da nadzor obavljaju i druge institucije ukoliko su posebnim propisima ovlaštene za obavljanje nadzora nad aktivnostima pojedinih pravnih lica na koja se primjenjuju odredbe ovog zakona,pri čemu se kao takve u Zakonu RS i izričito pominju Agencija za bankarstvo RS, Agencija za osiguranje RS i Komisija za hartije od vrijednosti RS, svaka u okviru svojih nadležnosti.

Za potrebe nadzora, između ostalog, Ministarstvo finansija RS imenuje i Savjet za računovodstvo i reviziju, koji ima značajnu ulogu u smislu praćenja procesa primjene računovodstvenih i revizijskih standarda, davanja inicijative za odgovarajuća i blagovremena rješenja radi što efikasnije primjene računovodstvenih i revizijskih standarda u Republici, izvještavanje ministra o stanju u vezi sa primjenom računovodstvenih i revizijskih standarda i drugim sličnim aktivnostima,uz saradnju sa Komisijom za računovodstvo i reviziju BiH, domaćim i stranim obrazovnim ustanovama, (kako je definisano članovima 25., 26. i 27. Zakona RS). Članove ovog Savjeta imenuje ministar, a čine ga, pored zaposlenih iz Ministarstva, univerzitetskih profesora i drugih lica koja svojim teoretskim i praktičnim iskustvom u predmetnoj oblasti mogu da doprinesu efikasnijem radu Savjeta, i članovi profesionalnog tijela (Savez računovođa i revizora RS), pri čemu se predstavnici Poreske uprave, koja prema Zakonu F BIH ima primarnu ulogu po pitanju nadzora, uopće i ne spominju.

Ovako definisan mehanizam kontrole i nadzora nad revizijskom i računovodstvenom profesijom ima svrhu da poveća kvalitet finansijskih i revizijskih izvještaja, kao i povećanje discipline u oblasti računovodstva i revizije.

4.18.3.14. Revizija finansijskih izvještaja

4.18.3.14.1. Obveznici revizije

Odredbe entitetskih zakona po pitanju obveznika revizije su usaglašene, odnosno obavezi revizije podliježu: finansijski izvještaji pravnih lica razvrstani na velika i srednja, konsolidovani finansijski izvještaji, finansijski izvještaji pravnih lica čijim se vrijednosnim papirima trguje ili se vrši priprema za njihovo emitovanje na organizovanom tržištu vrijednosnih papira, kao i finansijski izvještaji onih pravnih lica za koje je ova obaveza uređena posebnim propisima kojima je regulisano njihovo poslovanje (npr. banke, osiguranja, fondovi i dr.). Mala pravna lica ne podliježu ovoj obavezi, ali mogu da se odluče da se revizija njihovih finansijskih izvještaja vrši u skladu sa odredbama zakona.

U Zakonu F BiH je propisano da organ pravnog lica utvrđen odgovarajućim pravnim aktom donosi odluku o izboru društva za reviziju (član 52. stav 1.) U Zakonu RS sadržana je sličnoga odredba u članu 29. stav 7., pa se uopšteno kaže da ”nadležni organ u pravnom licu odlučuje o izboru privrednog društva za reviziju u skladu sa zakonom”.

U oba zakona je propisano da reviziju finansijskih izvještaja jednog pravnog lica isto privredno društvo za reviziju može da obavlja najduže pet godina uzastopno,odnosno još dvije godine nakon isteka roka,ukoliko društvo za reviziju obezbijedi da reviziju izvrši drugi revizor.

Također, na istovjetan način je utvrđena obaveza da privredna društva za reviziju najkasnije do 15. januara tekuće godine ministarstvu dostave fotokopije ugovora o reviziji zaključenih u toku prethodne godine (pri tome, treba primijetiti i to da, prema Zakonu RS, nadzor nad revizijom i jeste na ministarstvu, dok to nije slučaj prema Zakonu F BiH).

Pravo na naknadu za obavljenu reviziju utvrđeno je u oba entitetska zakona,s tim da se u Zakonu F BiH kaže da se iznos naknade utvrđuje ugovorom,ali da ona ne može biti niža od tarife revizorskih usluga koje utvrđuje i donosi Komora uz saglasnost Ministarstva,dok se u Zakonu RS kaže da se iznos naknade za reviziju utvrđuje ugopvorom o reviziji.međutim,Savjet za računovodstvo i reviziju RS,koji je formiran u skladu sa zahtijevima zakona RS,prihvatio je inicijativu za definisanje kriterija za utvrđivanje cijene revizorskih usluga, kao i inicijativu za ştvaranje preduslova za primjenu Međunarodnih standarda finansijskog izvještavanja za mala i srednja preduzeća.(Inače,konačna verzija MSFI za mala i srednja preduzeća objavljena je od IFAC-a sredinom prošle godine i njihova primjena bi bila mnogo racionalnija od primjene osnovnih MSFI. Planom rada Ministarstva finansija RS za 2010. godinu predviđeno je i donošenje Pravilnika o primjeni MSFI za mala i srednja preduzeća).

Zakonom F BiH je naglašeno da se zaključivanjem ugovora o reviziji između pravnog lica kod kojeg se obavlja revizija i društva za reviziju, a kojim se utvrđuju međusobna prava i obaveze ugovornih strana, vrši u pisanom obliku i da se ne može otkazati iz neopravdanih razloga,te da”razlika u mišljenju u vezi oblasti računovodstva i revizije između predstavnika pravnog lica kod kojeg se obavlja revizija i društva za reviziju, nije opravdan razlog za otkazivanje ugovora o reviziji” (ovakva odredba o nemogućnosti otkaza ugovora o reviziji uslijed neopravdanih razloga nije sadržana u Zakonu RS).

Po pitanju načina postupanja društva za reviziju koje u toku obavljanja revizije ostane bez minimalno jednog zaposlenog ovlaštenog revizora na neodređeno vrijeme sa punim radnim vremenom, na potpuno jednak način je uređeno u članu 40. Zakona RS i člana 52. stav 8. i 9. Zakona F BIH: obaveza prekida s radom i obavještavanje Ministarstva i pravnog lica-klijenta u roku od osam dana, te nemogućnost zaključivanja novog ugovora o reviziji do promjene okolnosti i ispunjavanja propisanih uslova.

4.19. Poslovne knjige i evidencije za obavljanje samostalne djelatnosti

Poreznim obveznicima koji obavljaju samostalnu djelatnost iz člana 12. stav 2. tačka 1., 2. i 3. Zakona o porezu na dohodak, dohodak se utvrđuje na osnovu poslovnih knjiga i drugih evidencija propisanih člana 19. Zakona. Poslovne knjige su: (1) knjiga prihoda i rashoda (obrazac KPR-1041), (2) knjiga prometa (obrazac KP-1042), (3) popisna lista dugotrajne imovine (obrazac PLDI-1043), (4) evidencija o potraživanju i obavezama (obrazac EPO-1044). Poslovne knjige se moraju voditi uredno, tačno i ažurno. Poslovne knjige se vode odvojeno za svaki porezni period. Po isteku godine porezni obveznik je dužan poslovne knjige zaključiti i potpisati. Ako porezni obveznik obavlja više samostalnih djelatnosti, poslovne knjige i evidencije dužan je voditi za svaku djelatnost odvojeno. Poslovne knjige i evidencije, uključujući i prateće kompjuterske evidencije i dokumentaciju na osnovu koje se vrši knjiženje, moraju se čuvati pet godina od dana predaje porezne prijave sačinjene na osnovu tih poslovnih knjiga. Za svaku prodaju,odnosno obavljenu uslugu, porezni obveznik je dužan izdati račun koji mora sadržavati slijedeće podatke: (a) podatke o izdavaocu računa, (b) podatke o izdvojenom/izdvojenim poslovnim prostorima, ako je promet obavljen putem tih prostora, (3) datum izdavanja računa, (4) naziv robe i usluge, (5) jediničnu cijenu i ukupan iznos računa. Račun se izdaje u najmanje dva primjerka s tim da se jedan primjerak daje kupcu, a drugi služi za knjiženje u poslovnim knjigama.

Za obveznike poreza na dohodak, koji obavljaju samostalnu djelatnost iz člana 14.stav 1tačka a), b) i c) Zakona o porezu na dohodak BD BiH utvrđena su gotovo identično rješenje kao u Federaciji Bosne i Hercegovine.[350]

Zakonom o računovodstvu i reviziji Republike Srpske[351], za razliku od Zakona o računovodstvu i reviziji u Federaciji Bosne i Hercegovine, dozvoljena mogućnost da poduzetnici sami izaberu da vode dvojno knjigovodstvo, odnosno da se odluče da li će svoje poslovne knjige voditi po propisima o porezu na dohodak ili po propisima o računovodstvu (u kom slučaju moraju primjenjivati odredbe Zakona o računovodstvu i reviziji RS). S timu vezi, u Republici Srpskoj je donesen Pravilnik o sistemu dvojnog knjigovodstva kod poduzetnika[352].Ovakva mogućnost vođenja računovodstva za poduzetnike nije data poduzetnicima u odredbama Zakonu o računovodstvu i reviziji u Federaciji BiH.

Napomena edukatoru

Predstaviti sve vrste poslovnih knjiga koje su dužni voditi poduzetnici i sadržaj informacija koje se nalaze u njima te objasniti razlike u zakonskim tretmanima .

[350] Vidi"Zakon o porezu na dohodak („ Službeni glasnik Bd BiH",broj 60/10),vidi član 20 (Poslovne knjige i evidencije)
[351] Vidi „Zakon o računovodsvu i reviziji Republike Srpske",član 3 (1).
[352] Vidi "Službeni glasnik Republike Srpske",broj 94/09.

5. LITERATURA

5.1. Osnovna literatura

- George A.Manning, Ph.D.C.F.E.,E.A."FINANCIAL INVESTIGATION and FORENSIC ACCOUNTING" Taylor&Francis Group, Boca Rata-London-Singapore, 2005.;
- James R.Richards „Transnational Criminal Organizations,Cybercrime,and Money Laundering" CRC PRESS, Boca Ration-London-New York-Wasington.D.C.;
- Doug Hopton „Money Laundering- Concise Guide for All Business",Gower Publishing Company,USA,2006.;
- Robinson,Jeffrey"Laundrymen",Simon&Schuster Children s Publishing,1998.godine,
- Mr.Goran Bošković „PRANJE NOVCA",BeoSing,Beograd,2005.godine;
- Dr.Dragan Jovašević,Mr.Marina Gajić-Glamočlija"KRIVIČNO DELO PRANJA NOVCA" BeoSING,Beograd,2008.godine

5.2. Naučni radovi

- Dr.Sonja Cindori,viša asistentica,Pravni fakultet Svaučilište u Zagrebu"PROCJENA RIZIKA POREZNIH SAVJETNIKA U SUSTAVU SPRJEČAVANJA PRANJA NOVCA"Zbornik Pravnog fakultreta u Rijeci,broj 2(809-827)2010.;

- Mr.sci. Žana Pedić, Ministarstvo finansija, Zagreb,Nefinansijski sektopr i samostalne profesije u kontekstu sprječavanja pranja novca,UDK 343 359, Pregledni znastveni rad, Zbornik Pravnog fakulteta Rijeka broj 1.,2010.;

5.3. Objavljeni članci

- Christine Victoria Thomason,How has the establishment of the Internet changed the ways in wihich offenders launder their dirty money, Internet Jurnal of Criminology, 2009.,

- Australian Goverment, Australian Institute of Criminology " Cyber thrat lanscape faced by financial and insurance industri" , 21.02.2011, www.aic.gov.au/crime_types/cybercrime.aspx

- Sonja Cindori, Sustav sprječavanja pranja novca, Finansijska teorja i praksa, 2007.

- Sanja Katušić-Jergović, sutkinja Županijskog suda u Velikoj Gorici, Pranje novca (Pojam, karakteristike, pravna regulativa i praktični problemi),UDK 343.341, 343.359, Stručni članak,2007.godine(www.pravo.unizg.hr);

- CARNet HRVATSKA AKADENSKA I ISTRAŽIVAČKA MREŽA, Elektronički novac NCERT-PUBDOC-2010-09-311, Nacionalni CERT+ (www.cert.hr) u suradnji s LS&S (www.LSS.hr).,

- CARNet HRVATSKA AKADEMSKA ZAJEDNICA i ISTRAŽIVAČKA MREŽA,Bankarski zločudni programi-2010-10-290, NCERT+(www.cert.hr) u suradnji sa LS&S (www.LSS.hr).

- Mr. Dragan Đurđević,dokotorant na Fakultetu civilne odbrane u Beogradu,Pranje novca i zlopotreba informacionih tehnologija, Ziteh, Beograd, 2010.(www.singipedia.com);

- Mirjana Drakulić i Ratomir Drakulić,Fakultet organizacionih nauka u Beogradu,Cyber kriminal,(www.fu.-student.com/...../index.php?,08.02.2012.,0,11.);

- Michaela Poremska Masaryk: Unioversity in Brno:Money Laundering as a Cybercrime of White-Colors,2009.godina, email:poremska@seznam.cz;

- Christine Howlett,2000 CHURCHILL FELLOW SHIP "Investigation&Contol of Money Laundering via Alternative Remittance &Unedrground Benking Systems,April 2001.Churchill Trust;

- Gup , B., E., (2006) Money Laundering, Financing Terrorism And Suspicious Activities, Nova Science Publishers, i u Gustitus, L., Bean, E., Roach, R., (2001), Economic Perspectives, An Electronic Journal of the U.S. Department of State, Vol. 6, No. 2.

5.4. Presude Suda BiH

- Presuda suda Bosne i Hercegovine broj:S1 2K 003427 09 k(X-K-05/64-2) od 13.12.2010.godine;
- Presuda suda Bosne i Hercegovine broj:X-KŽ-07/436 od 16.12.2010.godine;
- Presudu Suda Bosne i Hercegovine broj:X-K-07/436 od 10.05.2010.godine;
- Presudu Suda Bosne i Hercegovine broj :X-K/05710 od 24.03.2006.godine;
- Presuda Suda Bosne i Hercegovine broj: X-KŽ-05/10 od 15.05.2006.godine;
- Presuda Suda Bosne i Hercegovine broj:X-KŽ-06/177 od 09.03.2010.godine,
- Presuda Suda Bosne i Hercegovine broj:X-K-05/164 od 29.04.2008.godine;
- Presuda Suda Bosne i Hercegovine broj:X-KŽ-05/164 od 30.03.2009.godine;
- Presuda Suda Bosne i Hercegovine broj:KPŽ-04/09 od 17.11.2009.godine;
- Presuda Suda Bosne i Hercegovine broj:KPV-07/04 od 23.12.2008.godine;
- Presuda Suda Bosne i Hercegovine broj:S1 2 K 003427 09 Kž(veza X-KŽ-05/64-2) od 04.04.2011.godine;
- Presuda Suda Bosne i Hercegovine broj :KPŽ-16/09 od 2602.2010.godine;
- Presuda Suda Bosne i Hercegovine broj:KPV-01/08 od 24.06.2008.godine;
- Presuda Suda Bosne i Hercegovine broj:KPV-01/06 od 25.03.2009.godine,
- Presuda Suda Bosne i Hercegovine broj:KPV-03/04 od 08.12.2006.godine;
- Presuda Suda Bosne i Hercegovine broj:KPŽ-13/10 od 15.10.2010.godine;
- Presuda Suda Bosne i Hercegovine broj:X-K-06/177 od 24.09.2009.godine;

5.5. Priručnici

- Republika Crna Gora i European Commission-CADRS POLICE"JAČANJE KAPACITETA ZA EFIKASNO PROVOĐENJE FINANSIJSKE ISTRAGE USMJERENE NA ODUZIMANJE IMOVINE STEČENE KRIVIČNIM DJELOM-PRIRUČNIK ZA OBUKU IZ OBLASTI FINANSIJSKIH ISTRAGA, POSEBNI DIO, Podgorica, 2006.godine;

- Robert Golobinek i saradnici, CARDS Regionalni program 2002/2003, Projekt:Razvoj pouzdanih i funkcionalnih policijskih sistema i jačanja borbe protiv glavnih kriminalnih aktivnosti i jačanje policijske saradnje(CARPO) "Finansijske istrage i oduzimanje imovine stečene krivičnim delima"- Priručnik za pripadnike policije i pravosuđa;

- THE WORLD BANK/THE INTERNATIONAL MONETARY FOUND"Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism-Second Edition and Supplement on Special Recommendation IX(Paul Allan Schot) 2006.godina.

- ORGANIZATION FOR ECONOMIC CO-OPERTION AND DEVALPMENT"Money Laundering Awareness Handbook for Tax Examineres and Tax Auditores,2009.

- Leko, V., (1998), Rječnik bankarstva, Masmedia, 1998.godina,Zagreb.

- Dokument za edukaciju sudija i tužilaca Vijeća Europe koji je sačinila Radne grupe u okviru Projekta o kibernetičkom kriminalu i Lisabonske mreže,Strazbur,2008.

5.6. web stranice

- http://www.aci.net/kalliste/homepage.html;

- http://www.seebiz.net/finansije/bankarstvo-i-osiguranje/cbbih;

- http://www.info-market.ba/bs/scena/12670;

- http://ahzco.ffri.hr/seminar/2005/ebankarstvo/smart kartice.htm

- http://www.cybnershengen.com ,

- http://www.cybnershengen.com ,

- http://www.cisco.com

- http://pandalabs.pandasecurity.com

- iseclab.org/papers/impersonation,

- stage.owasp.org/.../OWASP_Anti-Malware_- _K....,

- www.singipedia.com

- www.coe.int/moneyval

- www.coe.int/t/dghl/cooperation/.../projects/CARPO/carpo_en.asp

- www.interpol.int

- www.egmontgroup.org
- www.fatf-gafi.org
- ww.coe.int/t/dghl/.../greco/.../

5.7. Pomočni linkovi i informacije

- Vijeće Evrope www.coe.int/cybercrime
- The Scientific Working Group on Digital Evidence (SWGDE) Scientific Working Group on Digital Evidence (SWGDE) is an organization dedicated to creating consistent, quality standards for digital and multimedia evidence within the forensic community.http://www.swgde.org/
- The International Organization on Computer Evidence (IOCE).The International Organization on Computer Evidence (IOCE) provides an international forum for law enforcement agencies worldwide to exchange information on computer investigations and digital forensic issues.http://www.ioce.org
- HTCIA International Conference & Training Expo 2011 Report on Cyber Crime Investigation, Hershey Lodge, Hershey, PA, September 16-19, 2012 http://www.htcia.org/pdfs/2011survey_report.pdf i http://www.htcia.org/
- Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime NCJ 198421, February 2002, Grant Report, by Gordon, Gary R.; Hosmer, Chet D.; Rebovich, Don; Siedsma, Christine (113 pages) www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf
- Electronic Crime Scene Investigation: A Guide for First Responders NCJ 187736, July 2001, NIJ Guide, by National Institute of Justice (96 pages) http://www.ncjrs.gov/pdffiles1/nij/187736.pdf
- http://nij.ncjrs.gov/App/publications/Pub_search.aspx?searchtype=basic&category=99&location=top&PSID=30
- Forensic Examination of Digital Evidence: A Guide for Law Enforcement by National Institute of Justice - April 2004,
- http://www.ncjrs.gov/pdffiles1/nij/199408.pdf
- http://www.nij.gov/nij/pubs-sum/199408.htm
- http://www.nij.gov/nij/topics/forensics/evidence/digital/resources.htm#Training%20Resources%20List.,
- http://www.nij.gov/nij/topics/forensics/evidence/digital/welcome.htm.,
- www.ncjrs.gov/pdffiles1/nij/187736.pdf.,

- www.ncjrs.gov%2Fpdffiles1%2Fnij%2F187736.pdf.,
- www.moreilly.com%2FCISSP%2FDomA-2-Computer_Crime_investigation.pdf
- http://www.htcia.org/links.shtml.,
- http://www.cert.org/tech_tips/FBI_investigates_crime.html