



iPROCEEDS

Otkrivanje imovinske koristi stečene izvršenjem krivičnih dela putem interneta u Jugoistočnoj Evropi i Turskoj

www.coe.int/cybercrime

Verzija od 21. decembra 2017.

Kurs za obuku sudija i tužilaca

Napredni kurs za traženje i privremeno i trajno oduzimanje imovinske koristi stečene vršenjem krivičnih dela putem interneta

Priručnik za samostalnu obuku

Funded
by the European Union
and the Council of Europe



Implemented
by the Council of Europe

Kontakt:

Alexander Seger
Odeljenje za visokotehnološki kriminal
Generalni direktorat za ljudska prava i
vladavinu prava
Savet Evrope,
Strazbur, Francuska

Tel: +33-3-9021-4506

Faks: +33-3-9021-5650

Email: alexander.seger@coe.int

**Izjava o odricanju od
odgovornosti:**

Ovaj tehnički izveštaj nužno ne
odražava zvanične pozicije Saveta
Evrope ili donatora koji finansira ovaj
projekat.

Sadržaj

1	Uvod	7
1.1	Cilj kursa	9
1.2	Ciljna grupa polaznika	9
1.3	Kratak pregled sadržaja	10
1.3.1	Izazovi istraga na internetu	10
1.3.2	Prekogranične istrage	10
1.3.3	Virtuelne valute.....	10
1.3.4	Praktičan rad/Studije slučaja.....	10
2	Izazovi istraga na internetu	11
2.1	Tipologije i pranje novca putem interneta	11
2.1.1	Korišćenje internet bankarstva	11
2.1.2	Korišćenje drugih finansijskih usluga na internetu.....	12
2.1.3	Korišćenje usluga komunikacije putem interneta	14
2.1.4	Neprobojni hosting	16
2.1.5	Podzemna ekonomija	17
2.2	Identifikacija učinioca	18
2.2.1	Prevođenje mrežnih adresa (NAT)	18
2.2.2	<i>Carrier-grade</i> NAT (CGN).....	20
2.2.3	Korišćenje anonimizatora	21
2.2.4	Botnet mreža/maliciozni softver/daljinsko upravljanje ličnim računarom.....	24
2.2.5	Korišćenje otvorene, javne ili ukradene bežične mreže	25
2.2.6	Identifikacija vlasnika IP adrese	25
2.3	Rad sa provajderima internet usluga	27
2.3.1	Vrsta traženih podataka	27
2.3.2	Direktiva EU o zadržavanju podataka proglašena je nevažećom na osnovu odluke SPEU.....	28
2.3.3	Nacionalni pružaoci internet usluga.....	31
2.4	Multinacionalni pružaoci usluga.....	32
2.4.1	Nadležnost	33
2.4.2	Opšta pozicija	33
2.4.3	Zahtevi za zaštitu podataka	33
2.4.4	Hitni zahtevi	33
2.4.5	Obim zahteva	34
2.4.6	Obaveštavanje subjekta zahteva	34
3	Finansijske istrage.....	35
3.1	Uvod	35
3.2	Finansijske istrage i imovinska korist stečena izvršenjem krivičnih dela putem interneta	35

3.2.1	Elementi finansijske istrage	36
3.2.2	Visokotehnološki aspekti finansijske istrage	36
3.2.3	Finansijska istraga u Evropskoj uniji	37
4	PREKOGRANIČNA SARADNJA	40
4.1	Sažetak	40
4.1.1	Odgovarajuće mreže i organizacije za razmenu informacija i međunarodnu pravnu pomoć	41
4.1.2	Međunarodni pravni instrumenti	42
4.1.3	Odredbe o međunarodnoj saradnji	45
4.2	Ocene primene odredbi o međunarodnoj saradnji	47
4.2.1	Ocena vezana za pronalaženje i oduzimanje imovinske koristi	47
4.2.2	Ocena povezana sa visokotehnološkim kriminalom	50
4.3	Korišćenje modeli i obrazaca za međunarodnu pravnu pomoć	57
5	Virtuelne valute	59
5.1	Rekapitulacija osnovnog kursa	59
5.2	Uvod u virtuelne valute	60
5.2.1	Dodatna terminologija o virtuelnim valutama	60
5.2.2	Učesnici u sistemu virtuelne valute	62
5.2.3	Bitcoin	63
5.3	Rizici povezani sa virtuelnim valutama	65
5.4	Izazovi u istrazi	67
5.4.1	Znanje o tome da su korišćene virtuelne valute	67
5.4.2	Anonimnost transakcije	67
5.4.3	Identifikacija izvora sredstava	68
5.4.4	Unovčavanje/realizacija i konverzija imovinske koristi	68
5.5	Izazovi ograničenja raspolaganja /oduzimanja	69
5.5.1	Virtuelna valuta kao imovinska korist stečena krivičnim delom	69
5.5.2	Utvrđivanje postojanja virtuelne valute	69
5.5.3	Ograničavanje raspolaganja/preuzimanje kontrole nad virtuelnom valutom ..	69
5.5.4	Upravljanje imovinom	70
6	Praktičan rad/Studije slučaja	72
6.1	Pretraga literature	72
6.2	Studija slučaja 1: Razmatranje zakonskog osnova za radnje	72
6.3	Studija slučaja 2: Razmatranje interakcije između FOS i organa reda	75
6.4	Studija slučaja 3: Razmatranje interakcije između visokotehnološkog kriminala i pranja novca I	78
7	Aneks: Spisak relevantne literature	80
7.1	Savet Evrope	80
7.2	Evropska unija	82

7.3	Ujedinjene nacije	84
7.4	Radna grupa za finansijske mere u borbi protiv pranja novca	84
7.5	Sudska praksa.....	85
7.6	Druga literatura	86

1 Uvod

Pitanja visokotehnološkog kriminala, elektronskih dokaza, imovinske koristi i pranja novca presecaju različite institucije i, posebno, uključuju jedinice za visokotehnološki kriminal, jedinice za finansijske istrage, finansijsko-obaveštajne službe (FOS) i tužilaštva. Međutim, istrage u oblasti visokotehnološkog kriminala retko su praćene finansijskim istragama i obratno, istrage finansijskog ili drugih vrsta kriminala retko su praćene istragama u oblasti visokotehnološkog kriminala. U tom smislu, postoji potreba za delotvornijom međuagencijskom saradnjom između svih ovih institucija, od koje se očekuje da će imati najjači uticaj na traženje, kao i privremeno i trajno oduzimanje imovinske koristi stečene izvršenjem krivičnih dela putem interneta.

Tokovi novca stečenog visokotehnološkim kriminalom i drugim vrstama krivičnih dela izvršenih putem interneta ne zaustavljaju se na geografskim granicama. Stoga, u cilju sveobuhvatnog rešavanja ovih pojava, istražne radnje treba da se protežu preko granica i da funkcionišu u različitim jurisdikcijama. Delotvorna međunarodna saradnja takođe je od ključne važnosti za traženje, kao i privremeno i trajno oduzimanje imovinske koristi stečene izvršenjem krivičnog dela putem interneta. Povezivanje, praćenje imovinske koristi, mere za borbu protiv pranja novca i finansiranja terorizma, zajedno sa istragama u oblasti visokotehnološkog kriminala i računarskom forenzikom, pružaju dodatne mogućnosti. Na primer, privremene mere za zabranu raspolaganja sredstvima treba da prate zahtevi za brzu zaštitu elektronskih dokaza.¹ Ovo je jedan od razloga zbog kojih se u preporuci br. 36 Radne grupe za finansijske mere u borbi protiv pranja novca (FATF) predlaže primena Budimpeštanske konvencije o visokotehnološkom kriminalu i Varšavske konvencije Saveta Evrope.

Kako korišćenje i oslanjanje na informacionu tehnologiju postaje sve zastupljenije u društvu, sve su češći i napadi na računarske sisteme i njihovo iskorišćavanje. Broj i složenost krivičnih dela kod kojih se koriste računari velikom brzinom raste, ali izrada delotvornih kontramera kasni. Izvođenje učinilaca pred lice pravde zahteva dokaze o krivici van razumne sumnje, ali su dokazi koji se prikupljaju iz elektronskih uređaja nepostojani, često neopipljivi i verovatno se nalaze u drugoj jurisdikciji. To znači da ključnu važnost za identifikaciju, prikupljanje i zaštitu elektronskih dokaza imaju delotvorni i jasni postupci koji su usaglašeni sa zakonom. Krivični postupak sve više podrazumeva pronalaženje dokaza o visokotehnološkom kriminalu ili elektronskih dokaza u računarskim sistemima ili uređajima za čuvanje podataka. Ovo se na sličan način odnosi i na imovinsku korist.

S obzirom na to da se društva u čitavom svetu oslanjaju na informacione i komunikacione tehnologije, sudije i tužioci moraju biti pripremljeni za rad na predmetima iz oblasti visokotehnološkog kriminala i sa elektronskim dokazima. Iako su u mnogim zemljama organi zaduženi za sprovođenje zakona uspeali da ojačaju svoje kapacitete za vođenje istraga u oblasti visokotehnološkog kriminala i za obezbeđivanje elektronskih dokaza, zahtevi sudija i tužilaca bili su manje u fokusu. Iskustvo govori da se, u većini slučajeva, sudije i tužioci suočavaju sa teškoćama u borbi sa novim realnostima sajber sveta. Stoga su potrebni posebni naponi da se sudije i tužioci obukom, umrežavanjem i specijalizacijom osposobe da procesuiraju i presuđuju u predmetima visokotehnološkog kriminala i da koriste elektronske dokaze.

¹ Vidi stav 317 Izveštaja o istraživanju MONEYVAL-a, Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction, mart 2012. Dostupno na:
[http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL\(2013\)6_Reptyp_flows_en.pdf](http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2013)6_Reptyp_flows_en.pdf)

Savet Evrope je tokom 2009. godine, u saradnji sa radnom grupom koju je činilo više zainteresovanih strana, izradio koncept za podršku takvim naporima u okviru Projekta o visokotehnološkom kriminalu u saradnji sa Lisabonskom mrežom institucija za obuku u pravosuđu.

Cilj ovog koncepta bio je da se institucijama za obuku u pravosuđu pomogne da izrade programe obuke za sudije i tužioce o visokotehnološkom kriminalu i elektronskim dokazima i da se takva obuka uključi u redovnu početnu i stalnu obuku.

Ciljevi koncepta obuke za sudije i tužioce su:

- Da se institucije za edukaciju osposobe za sprovođenje početne i stalne obuke u oblasti visokotehnološkog kriminala na osnovu međunarodnih standarda
- Da najveći mogući broj budućih i postojećih sudija i tužilaca dobije osnovno znanje o visokotehnološkom kriminalu i elektronskim dokazima
- Da se obezbedi napredna obuka za dovoljno veliki broj sudija i tužilaca
- Da se podrži stalno usavršavanje i tehnička obuka sudija i tužilaca
- Da se kroz umrežavanje sudija i tužilaca doprinese povećanju znanja
- Da se olakša pristup različitim inicijativama i mrežama za obuku.

U tom smislu, u okviru Zajedničkog regionalnog projekta Evropske unije i Saveta Evrope CyberCrime@IPA (Regionalna saradnja u krivičnom pravosuđu: Jačanje kapaciteta u borbi protiv visokotehnološkog kriminala) izrađeni su materijali za obuku o visokotehnološkom kriminalu i elektronskim dokazima koje će koristiti institucije za edukaciju.

S obzirom na uspeh i dokazanu vrednost osnovne i napredne obuke za sudije i tužioce o visokotehnološkom kriminalu i elektronskim dokazima, kroz zajednički projekat Evropske unije i Saveta Evrope iPROCEEDS² izrađena su još dva modula za obuku: osnovni i napredni modul o istrazi, traženju, kao i privremenom i trajnom oduzimanju imovinske koristi od visokotehnološkog kriminala.

Uopšteno govoreći, aktivnosti kriminalaca i kriminalnih organizacija osmišljene su za sticanje dobiti. Prema procenama Ujedinjenih nacija, ukupan iznos imovinske koristi tokom 2009. godine iznosio je oko 2,1 bilion USD, ili 3,6% svetskog BDP-a, ali je samo vrlo mali deo tih sredstava oduzet³. Pronalaženje imovinske koristi paralelnim vođenjem finansijske i krivične istrage moglo bi da dovede i do otkrivanja dokaza o krivičnom delu pranja novca. Pranje novca omogućuje kriminalnim organizacijama da ostvare korist od nelegalnih aktivnosti i da finansiraju svoje operacije.

Finansijski uticaj visokotehnološkog kriminala i obim tako stečene imovinske koristi teško je kvantifikovati bez pouzdanih podataka i istraživanja, ali se iz predmeta vidi da se imovinska korist stečena visokotehnološkim kriminalom pere uz pomoć naprednih šema koje obuhvataju i tradicionalne i nove metode plaćanja⁴. Međutim, visokotehnološke

² Zajednički projekat Evropske unije i Saveta Evrope "Otkrivanje imovinske koristi stečene izvršenjem krivičnih dela putem interneta u Jugoistočnoj Evropi i Turskoj" – iPROCEEDS ima za cilj jačanje kapaciteta vlasti u IPA regionu za traženje, kao i privremeno i trajno oduzimanje imovinske koristi od visokotehnološkog kriminala i sprečavanje pranja novca putem interneta. <http://www.coe.int/en/web/cybercrime/iproceeds>

³ Explanatory memorandum to the Proposal for an EU directive on countering money laundering by criminal law (22.12.2016) (Eksplanatorni memorandum za predlog direktive EU o krivično-pravnoj borbi protiv pranja novca). Dostupno na: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0826>

⁴ Criminal Money Flows on the Internet – methods, trends and multi-stakeholder counteraction, MONEYVAL Research Report, mart 2012.

istrage su retko praćene finansijskim istragama i obrnuto, a istrage finansijskog ili drugih vrsta kriminala retko su praćene visokotehnološkim istragama.

Organizovane kriminalne grupe kriju i ponovo ulažu svoja sredstva u druge države, a ne u onu gde je izvršeno krivično delo iz kog potiče ta imovina. To nadležnim organima znatno otežava borbu protiv teškog i organizovanog prekograničnog kriminala. Slično tome, tokovi novca stečenog vršenjem visokotehnološkog i drugih vrsta kriminala putem interneta ne zaustavljaju se na geografskim granicama. Da bi se našlo sveobuhvatno rešenje za ovu pojavu, istražne radnje treba i da se sprovedu preko granica i da funkcionišu u različitim jurisdikcijama. Stoga je delotvorna međunarodna saradnja takođe od ključne važnosti za traženje, kao i privremeno i trajno oduzimanje imovinske koristi od visokotehnološkog kriminala.

Koncept otkrivanja imovinske koristi stečene izvršenjem krivičnog dela putem interneta, koji je predstavljen u okviru ovog kursa, spaja pristupe iz istraga visokotehnološkog i finansijskog kriminala i pranja novca u cilju veće efikasnosti i uspeha krivičnih istraga i krivičnog postupka, kako iz perspektive krivičnog gonjenja kriminalaca, tako i iz perspektive otkrivanja imovinske koristi.

1.1 Cilj kursa

Ovaj kurs ima za cilj da olakša dalju edukaciju zainteresovanog sudije ili tužioca koji je završio osnovni kurs o istragama, traženju, i privremenom i trajnom oduzimanju imovinske koristi stečene izvršenjem krivičnog dela putem interneta i koji želi da nastavi edukaciju iz ove oblasti. Cilj je povećanje znanja zainteresovanog sudije ili tužioca o pravnom i tehničkom okruženju koje se odnosi na imovinsku korist stečenu izvršenjem krivičnog dela putem interneta. Ovo se postiže detaljnijim proučavanjem izabranih tema od interesa u ovoj oblasti.

Na ovom kursu će detaljnije biti obrađene odabrane teme iz sledećih oblasti:

- Pravni i tehnički izazovi istraga koje uključuju tokove novca stečenog izvršenjem krivičnog dela putem interneta.
- Praktični aspekti prekograničnih istraga.
- Korišćenje virtuelnih valuta za potrebe kriminala i rizici u vezi sa njima.

Ovo prati praktičan rad u obliku pretrage literature i studija slučaja koje polaznik treba da razmotri.

1.2 Ciljna grupa polaznika

Ovaj kurs namenjen je sudijama i tužiocima koji su već završili osnovni kurs o traženju i privremenom i trajnom oduzimanju imovinske koristi stečene izvršenjem krivičnog dela putem interneta. Očekuje se da korisnici ovog priručnika već poznaju:

- Značenje visokotehnološkog kriminala i prirodu istrage u oblasti visokotehnološkog kriminala
- Prirodu finansijskih istraga
- Krivično delo pranja novca i ulogu finansijsko-obaveštajne službe (FOS)
- Da imaju osnovno tehničko znanje, npr. o prirodi IP adrese.
- Da imaju osnovno razumevanje osobenosti elektronskih dokaza.

Svi ovi preduslovi mogu se steći završavanjem "Osnovnog kursa Saveta Evrope o traženju, i privremenom i trajnom oduzimanju imovinske koristi stečene izvršenjem krivičnih dela putem interneta".

1.3 Kratak pregled sadržaja

1.3.1 Izazovi istraga na internetu

Na osnovnom kursu je predstavljen izvestan broj tipologija tokova novca stečenog izvršenjem krivičnih dela putem interneta i tipologija pranja novca. Cilj ovog dela je da se detaljnije razmotre neki izazovi sa kojima se možete suočiti u istragama kod nekih od ovde opisanih tipologija. Ovo uključuje diskusiju o izazovima u istrazi koji se povezuju sa identifikacijom učinioca na internetu, identifikaciji imovinske koristi stečene izvršenjem krivičnih dela putem interneta, kao i izazovima u vezi sa radom sa nacionalnim, međunarodnim i multinacionalnim provajderima internet usluga (ISP).

1.3.2 Prekogranične istrage

Koncept pronalaženja imovinske koristi stečene izvršenjem krivičnih dela na internetu spaja pristupe iz istraga visokotehnološkog kriminala, finansijskih istraga i istraga pranja novca u cilju povećanja efikasnosti i uspeha krivičnih istraga i krivičnog postupka, kako iz perspektive procesuiranja kriminalca tako i iz perspektive pronalaženja i oduzimanja imovinske koristi.

Iako se međunarodna pravna pomoć još uvek smatra glavnim sredstvom za izvršenje naredbi suda i za prikupljanje dokaza u inostranstvu, dužina tog postupka predstavlja značajnu prepreku. Međutim, korišćenje zajedničkih istraga i zajedničkih istražnih timova moglo bi da reši neke od izazova koji se odnose na efikasnost. Saradnja i razmena informacija između organa zaduženih za sprovođenje zakona (policije i tužilaca) preko je potrebna u prekograničnim predmetima. U tom smislu važnu ulogu imaju odgovarajuće mreže.

Za potrebe ovog naprednog kursa korisno je naglasiti neka od skorijih saznanja o preprekama koje su prepoznale međunarodne organizacije prilikom primene međunarodnih standarda u domaćem zakonodavstvu i praksi, kao i relevantne preporuke koje bi mogle da posluže kao izvor inspiracije.

1.3.3 Virtuelne valute

Nadovezujući se na osnovnu terminologiju koja se odnosi na virtuelne valute, o kojoj je bilo reči na uvodnom kursu, na ovom kursu se dalje razrađuje materija koja se odnosi na učesnike u ekosistemu virtuelnih valuta, uključujući i berze virtuelnih valuta, usluge u vezi sa novčanicima, itd. Opisuje se funkcionisanje virtuelne valute bitcoin, a potom sledi objašnjenje rizika i izazova u vezi sa istragama koje se odnose na korišćenje virtuelnih valuta, kao i traženje, oduzimanje i upravljanje njihovim sredstvima.

1.3.4 Praktičan rad/Studije slučaja

Da bi se polaznicima pomoglo da informacije sa ovog kursa smeste u kontekst svojih nacionalnih zakonodavstava, obezbeđena je vođena pretraga literature i nekoliko studija slučajeva, što će polaznicima omogućiti da, u vreme koje sami odaberu, dalje istražuju ovde otvorena pitanja.

2 Izazovi istraga na internetu

2.1 Tipologije i pranje novca putem interneta

Na osnovnom kursu je predstavljen izvestan broj tipologija tokova novca stečenog kriminalnim aktivnostima na internetu, kao i tipologija pranja novca putem interneta. Ovaj deo ima za cilj da detaljnije obradi neke od izazova sa kojima se možete suočiti u istragama kod nekih od ovih tipologija. Postoje dva vrlo velika i česta problema o kojima će se posebno govoriti u odvojenim delovima ovog kursa; izazovi u istragama koji se povezuju sa identifikacijom učinioca na internetu (vidi deo **Error! Reference source not found.**) i mnoštvo izazova koji se povezuju sa korišćenjem virtuelnih valuta (vidi deo **Error! Reference source not found.**).

2.1.1 Korišćenje internet bankarstva

Nekoliko tipologija koje su razmatrane na osnovnom kursu oslanjaju se na to da kriminalac ima pristup računu u banci. Ovo se posebno odnosi na tipologije elektronskih transfera, preuzimanja računa u bankama i međunarodnih transfera. Zahtevi koje zakonska regulativa postavlja pred finansijske institucije u smislu mera praćenja i poznavanja stranke, vođenja evidencija, i sl. dobro se razumeju⁵. Međutim, u pokušaju da zaobiđu ove kontrole, kriminalci se oslanjaju na činjenicu da se internet bankarstvo ne obavlja lično⁶. U odsustvu potrebe za direktnim kontaktom sa klijentom, kriminalac može da se, na primer, lažno predstavi kao legitiman klijent banke (npr. tako što će ukrasti ili koristiti lične podatke za internet bankarstvo) na način koji finansijska institucija može mnogo teže da utvrdi.

Postoje tri glavna traga koja treba pratiti prilikom vođenja istrage u takvim predmetima:

- Način na koji je bankarski račun kompromitovan (npr., fišingom, inficiranjem malicioznim softverom). Dokazi o tome mogu se dobiti od vlasnika računa, koji je najverovatnije oštećeni.
- Informacije o prijavljivanju u vezi sa kompromitovanim računom u banci. Ove informacije može da obezbedi finansijska institucija.
- Račun(i) u banci korišćen(i) za transfer novca sa kompromitovanog računa. Ovu informaciju ima finansijska institucija i ona bi mogla da pomogne prilikom identifikacije umešanih lica (mula za prenos novca) i praćenja novca u cilju konačnog oduzimanja.

U ostatku ovog dela, govoriće se o određenim problemima u istrazi koji se usled korišćenja usluga internet bankarstva usložnjavaju.

Prvo, teže je utvrditi prirodu odnosa, ukoliko postoji, između vlasnika bankarskog računa i osumnjičenog. Na primer:

1. Da li vlasnik bankarskog računa zna za aktivnosti osumnjičenog?

⁵ Međunarodni standardi za borbu protiv pranja novca i finansiranja terorizma i širenja oružja za masovno uništenje, Radna grupa za finansijske mere u borbi protiv pranja novca (FATF) Preporuke, 2012. Dostupno na:

<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>

⁶ FATF Report, Money Laundering Using New Payment Methods (Izveštaj FATF-a, Pranje novca korišćenjem novih metoda plaćanja), oktobar 2010. Dostupno na: <http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf>

2. Da li osumnjičeni ima direktnu kontrolu nad bankarskim računom ili rukovodi aktivnostima vlasnika bankarskog računa?
3. Da li je moguće identifikovati lice koje je izvršilo neku konkretnu transakciju na tom računu?

S obzirom na ova i mnoga druga pitanja, trebalo bi da bude jasno da priroda internet bankarstva, odnosno to što se ono ne odvija licem u lice, čini utvrđivanje činjenica u istrazi većim izazovom.

Drugo, korišćenje usluga internet bankarstva takođe dovodi do nekih izazova koji se odnose na identifikaciju same sumnjive aktivnosti. Kada se u nekoj filijali osumnjičeni predstavi i pokuša da izvrši transakciju, postoji barem neka mogućnost da će blagajnik prepoznati da li je aktivnost koja se obavlja očigledno sumnjiva. U internet okruženju, obrada transakcija je u velikoj meri automatizovana. U kombinaciji sa strukturiranjem sredstava u cilju izbegavanja ograničenja koja dovode do prijavljivanja, može da se poveća rizik da će sumnjive transakcije ostati neprimećene. Da bi se borile protiv ovoga, finansijske institucije često instaliraju automatizovani softver za praćenje transakcija, čija je funkcija da otkrije transakcije koje odstupaju od profila transakcija koje se obično obavljaju na datom računu.

Neki, mada ne svi, softveri za nadzor i otkrivanje prevara takođe će proveriti IP adresu sa koje se navodno prijavljuje na neki konkretan bankarski račun na internetu. Ako je, na primer, u pitanju neka IP adresa sa koje nikad ranije nije vršeno prijavljivanje na taj račun, moglo bi se posumnjati da je taj bankarski račun na internetu možda kompromitovan. Međutim, sa praktičnog aspekta za finansijske institucije, postoji osetljiva ravnoteža koju treba napraviti između otkrivanja i sprečavanja prevare, sa jedne strane, i neometanja legitimnih bankarskih aktivnosti globalno pokretnih klijenata, sa druge.

Pored toga, čak i ako je bankarski račun nekog klijenta na internetu kompromitovan, to neće uvek biti očigledno na osnovu IP adrese koja se koristi za prijavljivanje. Razlog za to je mogućnost da će, u slučaju kada je računar klijenta zaražen nekim malicioznim softverom, kriminalac imati kontrolu nad klijentovim računarom. Ovo će kriminalcu omogućiti da se na račun klijenta prijavi sa IP adrese klijentovog računara, i tako spreči aktiviranje upozorenja zbog prijavljivanja sa neuobičajene IP adrese.

Treće, postavlja se i pitanje koji su još dokazi potrebni za dokazivanje aktivnosti osumnjičenog i da li su oni dostupni. IP adrese s kojih je vršeno prijavljivanje na određeni račun najverovatnije su evidentirane kod finansijske institucije, ali ne uvek na odmah dostupan način. Mogu biti potrebni znatni naponi da bi se utvrdilo koje IP adrese su korišćene za koja prijavljivanja od strane kojih računa. Razlog za ovo je složenost infrastrukture internet bankarstva, a naročito to što dnevnički možda nisu sačuvani ili međusobno povezani na način koji nudi lak pristup traženim informacijama. Pored toga, kada i ako korišćena IP adresa može biti identifikovana, povezivanje osumnjičenog sa tom IP adresom predstavlja poseban izazov.

2.1.2 Korišćenje drugih finansijskih usluga na internetu

Druge (nebankarske) finansijske usluge na internetu igraju ulogu u nekoliko tipologija obrađenih na osnovnom kursu naročito korišćenje sistema plaćanja na internetu, kupovina preko interneta i korišćenje platformi za kockanje, odnosno trgovinu putem interneta. Ponovo, priroda odnosa između usluge i korisnika usluge, koja ne zahteva lični kontakt, kriminalcima daje mogućnost eksploatacije ovakvih vrsta usluga.

Ove usluge će na kraju morati da ostvare neku vrstu interakcije sa tradicionalnim sektorom finansijskih usluga. Ovo se najčešće dešava prilikom korišćenja platnih kartica za "punjenje" računa kod pružaoca finansijskih usluga putem interneta. Kada se sredstva sa platne kartice prenesu pružaocu usluge, priroda daljih interakcija između korisnika i pružaoca finansijskih usluga putem interneta biće neprozirna za tradicionalni finansijski sistem. Stoga se preporučuje da usluge plaćanja preko interneta podležu obavezi usaglašenosti sa zakonom i nadzoru⁷. Način regulisanja ove oblasti može se razlikovati od jedne do druge jurisdikcije.

Uzmimo u obzir, na primer, pojam mikroplaćanja⁸. Finansijski ne bi imalo smisla da neki pružalac usluga plaćanja putem interneta odmah naplati svako mikroplaćanje sa kreditne kartice korisnika zato što bi naknada za korišćenje platne kartice obrisala svaku dobit tog pružaoca platnih usluga iz te transakcije. Umesto toga, pružaoci platnih usluga obično nakupe izvestan broj plaćanja tokom nekog vremenskog perioda i samo jednom naplate sve aktivnosti korisnika u datom vremenskom periodu. Pružalac platne usluge stoga prihvata određeni rizik od prevare, ali pošto su iznosi pojedinačnih plaćanja obično vrlo mali, ukupni gubici obično će takođe biti mali.

Jedan model mikroplaćanja ponekad nude mobilni operateri. U tim slučajevima, korisnik vrši mikroplaćanja uz pomoć svog telefona ili telefonskog broja, a naplata se vrši preko sledećeg telefonskog računa tog korisnika.

U tim slučajevima, za istražitelja je najvažnije da razjasni prirodu nelegalne aktivnosti (prevare, neovlašćenog pristupa), vrstu podataka koji se mogu prikupiti i odakle se mogu prikupiti da bi se dokazala kriminalna radnja i pratio tok novca.

U većini slučajeva, oštećeni se naknadno upozoravaju na prevare kod kojih je korišćen njihov bankarski račun ili kreditne kartice. Ipak, pružaoci platnih usluga mogu da prepoznaju nelegalne aktivnosti i da sačuvaju te podatke, koji se kasnije mogu dostaviti istražiteljima.

Glavni izazovi koji se pojavljuju kod korišćenja platnih usluga putem interneta odnose se na činjenicu da se tražene evidencije obično nalaze u drugoj jurisdikciji. Uključivanje multinacionalnih pružalaca usluga i postupak međunarodne pravne pomoći mogu da znatno uspole istragu i povećaju njenu složenost.

Slični problemi se pojavljuju kod upotrebe platformi koje olakšavaju kupovinu putem interneta. Kako je rečeno na osnovnom kursu, kupovina roba ili usluga preko interneta i njihovo otpremanje kriminalcu ili muli predstavlja dobar način da se ukradeni lični podaci za plaćanje pretvore u vrednost u stvarnom svetu. U tim slučajevima, istraga se u potpunosti oslanja na evidencije platformi za kupovinu, kao i na njihovu sposobnost da prepoznaju sumnjivu aktivnosti. Još jednom, u većini istraga će se ispostaviti da se sedište većine platformi za kupovinu preko interneta nalazi u drugoj jurisdikciji. Da bi se od tih organizacija prikupili dokazi biće potrebno da se toj jurisdikciji uputi zahtev za međunarodnu pravnu pomoć.

Platforme za kockanje putem interneta takođe donose neke jedinstvene izazove koji uglavnom proističu iz nedoslednosti u regulisanju tih subjekata širom sveta. Na primer, u nekim jurisdikcijama, kockanje putem interneta je nelegalno, tako da saradnja sa

⁷ FATF Report, Money Laundering Using New Payment Methods, oktobar 2010. Dostupno na: <http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf>

⁸ <https://en.wikipedia.org/wiki/Micropayment>

operaterom kompanije za kockanje putem interneta u takvim slučajevima može da znači priznavanje takvih subjekata i zato može da predstavlja pravni izazov. U okviru EU, na primer, 20 država članica dozvoljavaju kockanje putem interneta, a sedam ne. Neke su u skorijem zakonodavstvu odlučile da dozvole ili zabrane kockanje putem interneta, dok ga druge dozvoljavaju ili zabranjuju "pasivno", tako što i dalje primenjuju zakonodavstvo koje je, često mnogo godina ranije, usvojeno za klasično kockanje. Od dvadeset država članica koje dozvoljavaju kockanje preko interneta, trinaest imaju liberalizovano tržište, šest imaju državne monopole, a jedna je izdala dozvolu za jedan privatni monopol⁹.

2.1.3 Korišćenje usluga komunikacije putem interneta

Internet je, pre svega, platforma za komunikaciju i kriminalci koriste usluge komunikacije za omogućavanje svojih aktivnosti. U kontekstu tokova novca koji potiče od kriminala, posebno na internetu, usluge komunikacije putem interneta omogućuju im da regrutuju mule, da s njima komuniciraju i da njima upravljaju. Usluge kao što je elektronska pošta, komunikacioni servis IRC (eng.: Internet relay chat), razmena trenutnih poruka i telefonske usluge koje su dostupne na internetu kriminalci mogu koristiti za organizovanje svojih aktivnosti.

Tehničke teškoće mogu se pojaviti i kod identifikacije lica koja učestvuju u komunikaciji i kod utvrđivanja sadržaja komunikacije. Pitanje identifikacije osumnjičenih na internetu detaljno je obrađeno u delu **Error! Reference source not found..**

Poslednjih godina, trend među pružaocima internet usluga je sve veće fokusiranje na garancije privatnosti njihovih korisnika. Ovo se pokazalo u mnogim slučajevima, kao što je veće korišćenje šifrovanja. Šifrovanje se, široko gledano, sprovodi na tri različita načina¹⁰:

- **Šifrovanje celog diska ili uređaja:** U slučaju laptopa ili ličnog računara, tehnologije za šifrovanje celokupnog sadržaja hard diska dostupne su već neko vreme. Takođe je već neko vreme moguće da se, jednako tome, šifrue memorija mobilnog uređaja, kao što je pametni telefon. Negde 2014. godine, tehnološke kompanije kao što su Apple i Google počele su da na svojim pametnim telefonima omogućavaju podrazumevano šifrovanje uređaja. Dešifrovanje i pristup uređaju obično zahtevaju lozinku ili PIN. Legitiman uslov za takvo šifrovanje je zaštita ličnih podataka vlasnika pametnog telefona od gubitka ili krađe uređaja.
- **Šifrovanje "s kraja na kraj":** Ovaj izraz se primenjuje na šifrovanje poruka koje se šalju preko neke platforme za razmenu poruka tako da ih mogu pročitati samo pošiljalac i primalac poruka. Mnogi servisi za razmenu poruka, uključujući *iMessage*, *WhatsApp* i *Facebook Messenger* nude varijacije šifrovanja poruka "s kraja na kraj". Ako uzmemo *iMessage* kao primer, upotreba šifrovanja "s kraja na kraj" znači da čak ni *Apple*, koji pruža tu uslugu, nema pristup sadržaju poruka.

⁹ EU Parliament Study by the Policy Department, Economic and Scientific Policy, titled "Online Gambling, focusing on integrity and a code of conduct for gambling" (Studija Parlamenta EU koju je izradilo Odeljenje za politiku i ekonomsku i naučnu politiku, pod naslovom "Kockanje na internetu, fokusiranje na integritet i kodeks ponašanja za kockanje"). IP/A/IMCO/FWC/2006-186/C1/SC2. Dostupno na:

[http://www.europarl.europa.eu/RegData/etudes/etudes/join/2008/408575/IPOL-IMCO_ET\(2008\)408575_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2008/408575/IPOL-IMCO_ET(2008)408575_EN.pdf)

¹⁰ Encryption a Matter of Human Rights (Šifrovanje kao pitanje ljudskih prava), izveštaj *Amnesty Internationala*, mart 2016. Dostupno na:

<http://www.amnestyusa.org/sites/default/files/encryption-a-matter-of-human-rights-pol-40-3682-2016.pdf>

- **Šifrovanje prenosa podataka:** Ovaj oblik šifrovanja odnosi se na podatke koji se šifruju radi prenosa između dve strane. Ovih dana se to najčešće koristi da označi šifrovanje saobraćaja na nekom internet sajtu. Šifrovanje prenosa podataka jedna je od osnovnih bezbednosnih kontrola koja olakšava savremeni svet elektronske trgovine i elektronskog bankarstva tako što onemogućava napadače da presretnu komunikaciju između stranke i banke ili internet sajta za elektronsku trgovinu.

Kada se koristi šifrovanje prenosa podataka, posebne dokazne radnje kao što je tajni nadzor komunikacije mogu ipak biti tehnički moguće, uz saradnju relevantnih strana kao što je vlasnik internet sajta, odnosno pružalac internet usluga. Dobijanje pristupa šifrovanom uređaju ili komunikaciji koja je šifrovana "s kraja na kraj" predstavlja veći izazov i često će zahtevati pristup uređaju ili ličnom računaru osumnjičenog.

STUDIJA SLUČAJA: *APPLE* PROTIV FBI-ja¹¹

FBI je pokušavao da otključa *iPhone* 5C koji je koristilo jedno od lica koja su izvršila napad vatrenim oružjem u San Bernardinu u Kaliforniji u decembru 2015. godine, kada je poginulo 14 ljudi.

Odgovarajući na zahtev Ministarstva pravde SAD, federalni sudija-magistrat je 16. februara 2016. godine naredio *Appleu* da napravi prilagođenu verziju svog operativnog sistema iOS, koji bi omogućio istražiteljima u tom predmetu da zaobiđu bezbednosne karakteristike tog telefona. Generalni direktor *Apple*a, Tim Cook, odgovorio je otvorenim pismom u kojem je naveo da zahtev ovog državnog organa predstavlja "kršenje privatnosti" sa "zastrašujućim" posledicama. Cook je rekao:

"Kad je FBI tražio ono što imamo, to smo mu obezbedili. Apple je postupio u skladu sa validnim sudskim nalogima i nalogima za pretres, kao što smo uradili i u predmetu iz San Bernardina. Takođe smo Appleove inženjere stavili na raspolaganje za davanje saveta FBI-ju i ponudili smo naše najbolje ideje o izvesnom broju opcija za istragu koje imaju na raspolaganju... Ali sada američki državni organi od nas traže nešto što jednostavno nemamo i nešto što smatramo previše opasnim za izradu. Tražili su nam da napravimo program za neovlašćeni ulaz u sistem iPhonea."

Apple se žalio na naredbu suda i federalni sud je zakazao ročište za 22. mart 2016. godine. Brojni nezavisni stručnjaci za tehnologiju, profesori prava, tehnološke kompanije i organizacije za ljudska prava podržale su stav *Apple*a o ovom pitanju. Rašireno gledište među protivnicima zahteva FBI-ja, uključujući i *Amnesty International*, je da bi, ako bi *Apple* bio primoran da izmeni svoj softver kako bi ovaj telefon bio otključan, to napravilo presedan koji bi mogao da omogući državnim organima SAD – a potencijalno i organima drugih država – da primoraju tehnološke kompanije da oslabe ili na drugi način zaobiđu šifrovanje tako što bi obaveštajnim i drugim bezbednosnim službama obezbedili program za neovlašćeni ulaz u sistem.

Reagujući na ovaj slučaj, visoki komesar UN za ljudska prava naveo je sledeće: "Uspeh predmeta protiv *Apple*a u SAD napraviće presedan koji može da onemogući *Appleu* ili nekoj drugoj velikoj međunarodnoj kompaniji za informacione tehnologije da štiti privatnost

¹¹ *Ibid.*

svojih klijenata bilo gde u svetu---to je potencijalni poklon autoritarnim režimima, kao i hakerima sa kriminalnim namerama. Vlasti u drugim državama su već napravile niz udruženih napora da nateraju kompanije za informacione tehnologije i komunikaciju, kao što su *Google* i *Blackberry*, da svoje klijente izlože masovnom nadzoru.”

FBI je 28. marta rekao da je otključao ovaj *iPhone* uz pomoć trećeg lica i Ministarstvo pravde je povuklo zahtev.¹²

2.1.4 Neprobojni hosting

U uslovima korišćenja većine pružalaca usluga interneta i web hostinga zabranjuju se nelegalne aktivnosti na njihovim mrežama ili servisima. Oni će, zato, obično sarađivati sa zahtevima za davanje informacija i zahtevima za obaranje nelegalnih domena ili internet sajtova koje upućuju organi zaduženi za sprovođenje zakona.

Neprobojni hosting, s druge strane, je naziv koji se daje pružaocima hosting usluga koji ne sarađuju sa zahtevima za davanje informacija ili za rušenje internet sajtova koje upućuju organi zaduženi za sprovođenje zakona. Ovakvi pružaoci se često nalaze u drugim zemljama (u odnosu na zemlju u kojoj se vodi istraga). U većini slučajeva kompanije za neprobojni hosting pokušaću da se brane time što nemaju zakonsku odgovornost za kriminalne radnje koje izvrše njihovi klijenti koristeći njihovu infrastrukturu.

Ove usluge se često koriste za rasturanje nelegalnih materijala, izradu neželjene elektronske pošte, kao serveri za komandu i kontrolu malicioznog softvera i za druge oblike kriminalne infrastrukture^{13, 14, 15}.

Fišing internet sajtovi čija su meta klijenti internet bankarskih (i drugih) usluga često koriste neprobojni hosting da bi napravili internet sajtove koji liče na legitimne sajtove. Oni se često obaraju ili blokiraju na osnovu neovlašćenog korišćenja žiga finansijske institucije. Internet sajtove koji ne koriste žig legitimne organizacije može biti teže oboriti.

Zakonodavstva nekih zemalja podržavaju blokiranje sadržaja za koji se zna da je nelegalan od strane nacionalnih internet provajdera, korišćenjem različitih tehnika za tehničko filtriranje¹⁶.

Informacije o korisnicima i uslugama koje kompanije za neprobojni hosting obezbeđuju vlastima nisu od velike koristi za istragu zbog toga što su podaci o tim licima najčešće lažni. Međutim, metoda plaćanja za iznajmljene usluge mogla bi biti važan trag koji bi mogao da pomogne prilikom utvrđivanja izvora kriminalne aktivnosti.

¹² FBI says it has cracked terrorist's iPhone without Apple's help (FBI kaže da je ušao u *iPhone* teroriste bez pomoći kompanije *Apple*), CNN, 29. mart 2016., <http://money.cnn.com/2016/03/28/news/companies/fbi-apple-iphone-case-cracked/index.html>

¹³ <http://www.cio.com/article/2428317/infrastructure/in-china---700-puts-a-spammer-in-business.html>

¹⁴ [http://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658_2.html?sid=ST2008111801165&s_pos=](http://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658_2.html?sid=ST2008111801165&s_pos=15)
¹⁵ https://en.wikipedia.org/wiki/Bulletproof_hosting

¹⁶ T-CY(2006)04 Strengthening Co-operation between law enforcement and the private sector, examples of how the private sector has blocked child pornographic sites (T-CY(2006)04 Jačanje saradnje između organa zaduženih za sprovođenje zakona i privatnog sektora, primeri slučajeva kada je privatni sektor blokirao sajtove sa dečjom pornografijom), februar 2006. Dostupno na: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e6ed1>

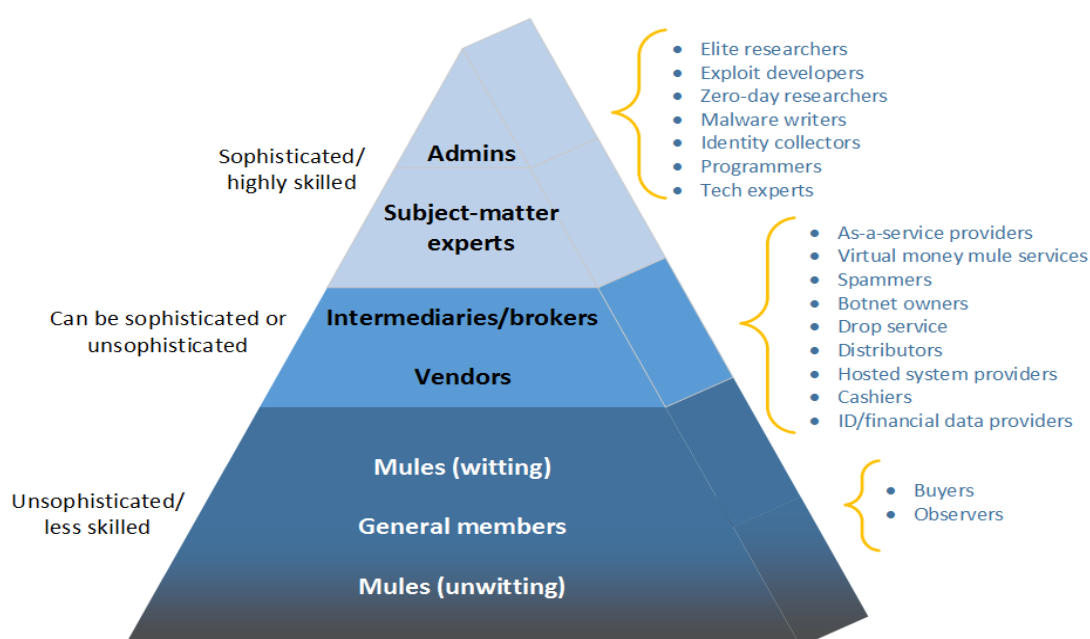
Na zakonodavnoj strani takođe postoje teškoće kod utvrđivanja nadležnosti za izvršene nelegalne aktivnosti pošto može postojati više korišćenih izvora, odredišta ili drugih koordinacionih mesta/entiteta.

U zemljama gde postoji neprobojni hosting, u istrazi se može koristiti tajno praćenje. Ovo će pomoći prilikom prikupljanja informacija o izvoru, odredištu i prirodi kriminalne radnje.

2.1.5 Podzemna ekonomija

Podzemna ekonomija je ime koje se daje uslugama koje koriste kriminalci da bi razmenjivali usluge i informacije jedni s drugima. Postoji mnogo primera podzemnih foruma, kao što je Silk Road i DarkMarket.¹⁷

Po svojoj organizaciji, podzemna ekonomija je strukturirana za vršenje krivičnih dela. Često se koristi poslovni model pod nazivom "Crime-as-a-Service" (kriminal kao usluga).



Grafikon 1: Učesnici modela kriminalnog poslovanja na Darkwebu

Slika: Empact training

Podzemni forumi koji su uglavnom posvećeni prevarama sa kreditnim karticama i prodaji ukradenih podataka sa kreditnih kartica često se nazivaju "carding forumi".

U većini slučajeva ovi forumi su otvoreni samo za određene "klijente" na osnovu lozinki ili drugih mera obezbeđenja.

Istrage koje se odnose na ove vrste foruma obično su veoma duge i složene i kod njih se službe za prikrivene islednike često polako infiltriraju na forume i prelaze na pozicije od autoriteta odakle će dobiti pristup informacijama koje će omogućiti optuživanje administratora i operatera foruma. To što su potrebne tako složene istrage znači da u većini istraga neće biti moguće ubaciti se u neki podzemni forum kako bi se prikupili dokazi za istragu o nekoj pojedinačnoj kriminalnoj radnji ili pranju novca putem interneta.

¹⁷ Za informacije o Darknet tržištima, vidi: <https://www.deepdotweb.com/>

Takođe, iz perspektive istrage, važno je imati odgovarajuće propise koji inkriminišu takve nelegalne aktivnosti i dozvoljavaju vođenje tajnih operacija i korišćenje prikupljenih dokaza na sudu. Ova istraga je mešavina klasičnih dokaznih radnji i tehnika koje se sprovode na internetu.

U slučajevima kada su vlasnici ili operateri nekog poznatog podzemnog foruma prisutni u nacionalnoj jurisdikciji ili kada se host tog podzemnog foruma nalazi u okviru nacionalne jurisdikcije, odgovarajuće materijalne odredbe nacionalnog zakonodavstva mogu se koristiti kao osnova za krivični postupak u takvim predmetima. Relevantne odredbe će zavisiti od specifičnosti tog predmeta ali bi mogle da budu ekvivalentne, na primer, članu 6 Budimpeštanske konvencije.

PITANJA ZA RAZMIŠLJANJE

1. **Koji uslovi moraju biti ispunjeni pre nego što se može odobriti nadzor nad bankarskim računom osumnjičenog?**
2. **Kakva ravnoteža je potrebna da bi se zaštili interesi potencijalno nevinog trećeg lica čiji je bankarski račun kompromitovan?**
3. **Koje odredbe u nacionalnom zakonodavstvu vaše zemlje možete koristiti da primorate osumnjičenog da dešifruje šifrovan uređaj ili datoteku?**
4. **Koje mere u nacionalnom zakonodavstvu vaše zemlje možete koristiti da primorate nacionalnog internet provajdera da blokira ili filtrira nelegalni sadržaj?**

2.2 Identifikacija učinioca

Setite se sa osnovnog kursa da je ključna karakteristika koja se koristi za identifikaciju osumnjičenog na internetu njegova IP adresa.

Cilj ovog dela je da detaljnije opiše neke praktične izazove koji se mogu pojaviti kada pokušate da povežete neku IP adresu sa nekim licem. Drugim rečima, u situacijama kada možete da povežete neku kriminalnu radnju na internetu sa nekom konkretnom IP adresom i pokušavate da identifikujete lice koje je u stvarnom svetu imalo kontrolu nad tom IP adresom u vreme kada se odigrala kriminalna radnja na internetu.

Takođe se, naravno, može pojaviti i suprotan problem kada imate osumnjičenog u stvarnom svetu i pokušavate da identifikujete IP adresu koju to lice koristi na internetu. Ova situacija je umnogome lakša za rešavanje i mogu se koristiti tradicionalne dokazne radnje (kao što su posebne dokazne radnje).

2.2.1 Prevođenje mrežnih adresa (NAT)

Da bi se preko interneta komuniciralo potrebne su IP adrese izvora i odredišta. U prošlosti (pre uvođenja NAT-a), svaki računar je trebalo da ima dodeljenu jedinstvenu IP adresu. Problem je što su IP adrese neefikasno dodeljivane i zbog toga ponestaju. Dugoročno rešenje za nestašicu IP adresa je uvođenje druge verzije IP-a, IP verzije 6, koja ima

mnogo veći broj dostupnih IP adresa. U međuvremenu se koristi nekoliko tehnika za produženje životnog veka IP verzije 4, od kojih je jedna i NAT.

Postoje određeni opsezi IP adresa koji su rezervisani. Drugim rečima, oni ne treba da se koriste na internetu. Umesto toga, oni treba da se koriste u privatnim mrežama kao što su interni opsezi u kancelarijama. Rezervisani opsezi su:

1. 10.0.0.0 – 10.255.255.255
 - a. Drugim rečima, bilo koja IP adresa koja počinje sa "10."
2. 192.168.0.0 – 192.168.255.255
 - a. Drugim rečima, bilo koja IP adresa koja počinje sa "192.168."
3. 172.16.0.0 – 172.31.255.255
 - a. Drugim rečima, bilo koja IP adresa koja počinje sa "172." i koju prati broj između "16" i "31".
 - b. Ovaj rezervisani opseg se koristi ređe od ostala dva.

Najčešća primena NAT-a odnosi se na to kada neka organizacija dodeli IP adrese iz jednog od ovih opsega svim ličnim računarima u firmi. Potom, kada jedan od ličnih računara na njihovoj mreži želi da komunicira sa nekom IP adresom na internetu, njihov ruter zameniće internu IP adresu jednom adresom iz malog opsega pravih internet IP adresa. U većini slučajeva, ishod ovog procesa biće da svi IP podaci sa svih ličnih računara u mreži te firme ostatku interneta izgledaju kao da dolaze sa jedne IP adrese.

Korišćenje NAT-a je takođe veoma često, gotovo sveprisutno u stvari, u kućnim širokopolasnim internet konfiguracijama. Ovo znači da kućni korisnik može da koristi više uređaja na svojoj kućnoj mreži, ali da njegov pružalac internet usluga treba da dodeli samo jednu IP adresu njegovoj konekciji.

Na internetu se mogu naći mnogi odlični tehnički opisi načina na koji funkcioniše NAT¹⁸, ¹⁹, ²⁰. Zainteresovani čitalac se poziva da, po potrebi, pregleda neke od ovih referenci u cilju daljeg informisanja.

Korisno je razmotriti kako upotreba NAT-a utiče na istrage na internetu. Možda se može identifikovati javna IP adresa koja se koristi tokom određene kriminalne radnje, ali ako se koristi NAT, ta IP adresa može da predstavlja aktivnost mnogih nezavisnih korisnika na internetu. Zato je u istrazi potrebno napraviti još jedan korak kako bi se utvrdila veza između aktivnosti na internetu i ličnog računara individualnog korisnika koji koristi rezervisanu adresu iza NAT rutera.

Postoji slaba mogućnost da neka organizacija koja koristi NAT možda ima dnevničke datoteke ulaznog i izlaznog saobraćaja koje bi mogle da se koriste za utvrđivanje unutrašnje IP adrese koja je bila odgovorna za stvaranje konkretnog segmenta saobraćaja koji predstavlja predmet istrage. Međutim, ovo je malo verovatno. Pored toga, kada su u pitanju korisnici iz malih firmi ili kućni korisnici, koji koriste standardnu opremu i usluge koje pruža njihov internet provajder, takve evidencije nisu dostupne.

U istrazi zato mora da se koristi alternativni mehanizam za povezivanje IP adrese osumnjičenog sa nekim konkretnim računarom. Mogu da postoje određene karakteristike saobraćaja koje omogućavaju identifikaciju unutrašnje IP adrese. Na primer, određene

¹⁸ <http://computer.howstuffworks.com/nat.htm>

¹⁹ <http://www.faqs.org/rfcs/rfc1631.html>

²⁰ <https://www.youtube.com/watch?v=QBqPzHEDzvo>

aplikacije u sam saobraćaj uključuju unutrašnju IP adresu ličnog računara koji stvara saobraćaj. Alternativno, pored IP adrese, mogu da postoje i druge prepoznatljive karakteristike koje se mogu koristiti. One bi mogle da uključuju korisnička imena, adrese elektronske pošte, tehničke informacije o izvornom uređaju i tako dalje. Na ovaj način se, kroz detaljnu analizu stručnjaka, može utvrditi izvor saobraćaja.

Ako se kriminalna radnja odigrava u realnom vremenu, mogu se primeniti posebne dokazne radnje kako bi se presreo izlazni saobraćaj i na taj način identifikovao unutrašnji lični računar. U takvim slučajevima, može biti potrebno da se obezbedi saradnja te organizacije kako bi se identifikovalo odgovarajuće mesto na njenoj mreži gde bi se instalirala stanica za praćenje. Za ovo će obično biti potrebna saradnja zaposlenih u informatičkom odeljenju, odnosno sistem administratora, ali treba imati u vidu da se unapred ne može nikako znati da osumnjičeni nije neko od zaposlenih u informatičkom odeljenju, odnosno neko od sistem administratora, koji bi na taj način saznao za istragu.

Ukratko, NAT predstavlja izazov za povezivanje neke konkretne IP adrese sa aktivnošću nekog korisnika iz stvarnog sveta. Da bi se istraga dovršila i osumnjičeni identifikovao, obično će biti potrebne dodatne informacije (pored IP adrese) prikupljene iz analize aktivnosti na internetu ili, alternativno, dodatne dokazne radnje.

2.2.2 *Carrier-grade NAT (CGN)*

Korišćenje *carrier grade* NAT-a, ili CGN-a, postavlja dodatne izazove. CGN je tehnika uz pomoć koje internet provajder može da koristi NAT za prevođenje velikog broja IP adresa pretplatnika u mali broj stvarnih internet IP adresa.

U tim slučajevima, CGN znači da, pored NAT-a do kojeg može doći dok se saobraćaj kreće iz male ili kućne kancelarije ka mreži internet provajdera, do drugog NAT-a može doći u okviru mreže internet provajdera pre nego što se prenese na internet^{21, 22}.

CGN se razlikuje od "prostog" NAT-a koji je opisan u prethodnom delu, jer ne samo da se privatna (unutrašnja) IP adresa zamenjuje javnom (spoljašnjom) IP adresom, već se i privatni (unutrašnji) broj TCP/IP porta zamenjuje javnim (spoljašnjim) brojem porta. U suštini, CGN preslikava TCP ili UDP sesije sa unutrašnjeg adresnog prostora na spoljašnji adresni prostor. Ova tehnika omogućava CGN-u da prevaziđe neke od problema skaliranja kod "prostog" NAT-a, ali dovodi do problema sa aspekta istrage – naime, u velikoj većini slučajeva, organizacije će u dnevniku evidentirati IP adresu sa koje primaju konekcije, ali neće evidentirati broj unutrašnjeg porta. Pošto CGN omogućava da potencijalno više hiljada korisnika koristi istu javnu IP adresu, sama IP adresa neće biti dovoljna za povezivanje aktivnosti sa konkretnim korisnikom.

Stoga se broj porta ne može pretpostaviti; da bi se identifikovao osumnjičeni biće potrebne druge dodatne informacije (pored IP adrese) dobijene iz analize aktivnosti na internetu.

U svojoj Proceni pretnji od organizovanog kriminala na internetu iz 2016. godine²³, Europol daje sledećih nekoliko preporuka za rešavanje izazova koje pred istragu postavlja CGN:

²¹ Osnovne informacije, drugi linkovi se mogu naći na: https://en.wikipedia.org/wiki/Carrier-grade_NAT.

²² <http://www.networkworld.com/article/2237054/cisco-subnet/understanding-carrier-grade-nat.html>

²³ Internet Organised Crime Threat Assessment (IOCTA), Europol, 2016. Dostupno na: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016> i 2017, vidi : <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>

- Da bi bili u stanju da, koristeći CGN, prate pojedinačnog krajnjeg korisnika do IP adrese na mreži, organi zaduženi za sprovođenje zakona moraju da, koristeći odgovarajuće pravne dokumente, traže dodatne informacije od pružalaca usluga:
- IP adrese izvorišta i odredišta
- Broj izvorišnog porta
- Tačno vreme konekcije (u sekund).
- Međutim, nepostojanje usklađenih standardnih zahteva za zadržavanje podataka u Evropi znači da provajderi usluga sadržaja, interneta i hostovanja podataka nemaju nikakvu zakonsku obavezu da zadržavaju ovu vrstu informacija, što znači da se čak i širim zahtevom neke službe zadužene za sprovođenje zakona od provajdera ne bi dobile informacije koje se mogu koristiti.
- Potrebne su regulatorne/zakonodavne izmene da bi se obezbedilo da provajderi usluga sadržaja sistematski zadržavaju neophodne dodatne podatke (izvorišni port) koje organi zaduženi za sprovođenje zakona zahtevaju da bi identifikovali krajnje korisnike.
- Alternativno, do praktičnih rešenja se može doći kroz saradnju između pružalaca elektronskih usluga i organa zaduženih za sprovođenje zakona. Neki pružaoci elektronskih usluga u Evropi ne čuvaju relevantne informacije (izvorišni port). Neki portal na nivou Evrope mogao bi da održava ažurirani spisak ovih pružalaca usluga i spisak kontaktnih tačaka kojima se treba obratiti ukoliko se istraga otegne zbog CGN-a.

2.2.3 Korišćenje anonimizatora

Anonimizator je alat koji pokušava da onemogući praćenje aktivnosti na internetu. On funkcioniše kao posrednik između ličnog računara i ostatka interneta i pristupa internetu u ime korisnika, istovremeno krijući informacije kojima se može identifikovati taj korisnik.

Anonimizatori se mogu podeliti u dve široke kategorije;

- **Anonimizatori sa specifičnim protokolom:** Oni rade samo sa jednim konkretnim protokolom. Primer bi bio anonimni rimejler (server za prosleđivanje elektronske pošte) ili internet proksi za anonimizaciju.
- **Anonimizatori nezavisni od protokola:** Oni funkcionišu tako što formiraju IP tunel kroz koji će biti prosleđen sav korisnički saobraćaj. Iz perspektive primaoca će izgledati kao da IP saobraćaj dolazi od nekog drugog, a ne od prvobitnog pošiljaoca. Jedan od primera bio bi Tor (raniji naziv na engleskom "The Onion Router").

Neki primeri su razmotreni u studijama slučaja u tekstu ispod.

U istragama predmeta u kojima je korišćen anonimizator, a pružalac usluge ne želi ili ne može da pruži podršku istrazi, za dalji rad mogu biti potrebne alternativne (netehničke) dokazne radnje.

STUDIJA SLUČAJA: ANONIMNI RIMEJLER

Svrha anonimnog rimejlara je da prima poruke, uklanja informacije koje služe za

identifikaciju i potom ih prosleđuje nameravanom primaocu na takav način da primalac ne može da vidi odakle je ta poruka prvobitno došla.

Postoji nekoliko načina na koje se ovo može postići:

- Pseudonimni rimejleri; Uklanjaju adresu elektronske pošte pošiljaoca, daju pseudonim pošiljaocu i šalju poruku nameravanom primaocu. Primalac će moći da odgovori tako što će poslati elektronsku poštu tom pseudonimu, a rimejler će je proslediti prvobitnom pošiljaocu.
- Sajferpank rimejleri (poznati i kao Tip I): Šalju poruku primaocu i istovremeno uklanjaju adresu pošiljaoca. Primalac ne može da odgovara na elektronsku poštu poslatu preko ove vrste servera. Pošiljalac će obično predati poruku rimejleru u šifrovanom obliku. Rimejler će je dešifrovati i poslati primaocu. Ova vrsta rimejlara ne vodi dnevnik transakcija.
- Miksmaster rimejleri (poznati i kao Tip II): Pošiljalac sastavlja elektronsku poruku i šalje je rimejleru. Poruka se prosleđuje više puta preko peer-to-peer (P2P) mreže rimejlara dok konačno ne stigne kod primaoca. Primalac ne može da odgovori na tu poruku osim ako se adresa na koju treba poslati odgovor ne nalazi u telu poruke. Da bi korisnik mogao da koristi miksmaster rimejler, treba da instalira poseban softver na svom ličnom računaru.
- Miksminion rimejleri (poznati i kao Tip III): Oni su slični miksmaster rimejlerima, ali su kod njih rešeni određeni tehnički problemi. Posebno je omogućeno da primalac odgovori preko mreže rimejlara iako ne zna ko je pošiljalac.

Moguće je više rimejlara povezati u lanac, tako da čak ni rimejleri ne znaju ko šalje poruku. Takođe se može koristiti internet baziran interfejs do rimejlara, nasuprot korišćenju standardne aplikacije ili aplikacije prilagođene potrebama koja je instalirana na korisnikovom ličnom računaru.

STUDIJA SLUČAJA: ANONIMIZACIJA WEB PROKSIJA

Proksi server za anonimizaciju pokušava da korisnikovu aktivnost pretraživanja interneta učini anonimnom. Proksi za anonimizaciju će obično prihvatati i prosleđivati zahteve korisnika. Iz perspektive internet servera koji prima zahtev, taj zahtev izgleda kao da dolazi sa proksija za anonimizaciju. Ako proksi za anonimizaciju nema dostupne zapise kojima se povezuju izlazni zahtevi sa konkretnim izvorišnim IP adresama, to neće biti moguće na osnovu analize IP podataka.

Korišćenje web proksija podržano je u gotovo svakom standardnom pretraživaču,

zato što postoje mnogi legitimni razlozi zbog kojih bi korisnici možda poželjeli da konfiguriraju proksi²⁴. Korišćenje ovih servisa obično ne zahteva mnogo više od konfigurisanja malog broja opcija u softveru standardnog pretraživača.

Međutim, sadržaj samog internet saobraćaja ipak može da sadrži detalje koji bi mogli da pomognu da se identifikuje osumnjičeni. Na primer, ako bi se osumnjičeni prijavio na neki internet sajt preko proksija za anonimizaciju, IP adresa sa koje se prijavio možda neće biti dostupna, ali bi analizom internet saobraćaja moglo da se otkrije korisničko ime i/ili lozinka koju koristi.

STUDIJA SLUČAJA: TOR (RANIJI NAZIV NA ENGLISKOM: "THE ONION ROUTER")

Tor je softverski alat koji usmerava internet saobraćaj preko mreže ličnih računara čiji su vlasnici volonteri i koji se besplatno koriste, i sastoji se od nekoliko hiljada releja. Njihov cilj je da otežaju praćenje aktivnosti na internetu do prvobitnog korisnika.

Rutiranje se obavlja putem više slojeva šifrovanja i potom prosleđivanja saobraćaja preko više nasumično izabranih releja. Svaki relej dešifruje po jedan šifrovani sloj, čime se otkriva samo sledeći sloj koji treba da se prenese i preostali šifrovani podaci se propuštaju na njega. Poslednji relej dešifruje podatke iz najdubljeg sloja i šalje ih na nameravano odredište ne otkrivajući ili ne znajući izvornu IP adresu. Rutiranje komunikacije je, dakle, delimično sakriveno od svakog skoka u Tor mreži, što znači da ne postoji ni jedna pojedinačna tačka u kojoj bi se partnerima u komunikaciji moglo ući u trag na način koji identifikuje ili se oslanja na izvor i odredište komunikacije.

Korisnik Tor mreže na svom ličnom računaru instalira poseban softver koji će presresti jedan deo ili sav izlazni mrežni saobraćaj i proslediti ga Tor mreži, umesto da ga pošalje direktno na nameravano odredište. Kada se saobraćaj nalazi unutar Tor mreže, on se šalje od rutera do rutera dok ne dođe do poslednjeg rutera u mreži (gde dolazi do finalnog dešifrovanja i otkrivanja originalnog saobraćaja). Ovaj ruter je poznat kao izlazni čvor. Iz perspektive odredišta, deluje kao da saobraćaj potiče iz izlaznog čvora.

Na osnovu gore navedenog opisa može delovati da Tor mreža dozvoljava samo anonimizaciju komunikacije koju je započeo klijent. Međutim, Tor takođe podržava i rad servera preko Tor mreže tako da IP adresa servera ne bude vidljiva njegovim korisnicima. Da bi se ovo postiglo, serverima se daju posebne

²⁴ Na primer, neka organizacija možda želi da spreči zaposlene da tokom radnog vremena gledaju određene internet stranice. U takvim slučajevima, proksi može da bude konfigurisan na ličnom računaru zaposlenog, a direktan pristup internetu je u tom slučaju blokiran *firewallom*. Svi *web* zahtevi zato moraju da prođu kroz taj proksi, koji je onda u poziciji da spreči ili dozvoli zahteve u skladu sa politikom koju je definisala organizacija.

adrese, koje su poznate kao etapne (eng. *onion*) adrese, i njima se može pristupiti preko Tor mreže na način koji ne otkriva lokaciju servera²⁵. Skriveni servis oglašava njegovo postojanje i onda Tor mreža na decentralizovan način utvrđuje "tačke za sastanak" da bi omogućila vezu između skrivenih servisa i korisnika od kojih ni jedan ne zna identitet onog drugog.

Iako je direktno utvrđivanje IP adrese osumnjičenog koji koristi Tor mrežu gotovo nemoguće, postoje specijalizovane tehnike za identifikaciju drugih informacija koje mogu da unaprede istragu. Na primer, može da se desi da se zbog pogrešne konfiguracije servera mogu otkriti informacije o pravom izvoru skrivenog servisa. Stranice za slučaj greške koje prave mnogi uobičajeni internet serveri (tj. poruka o grešci koja se prikazuje korisniku kad god njegov zahtev izazove grešku) sadrže i IP adresu servera, što znači da se IP adresa možda može otkriti stvaranjem stanja greške na serveru.

2.2.4 Botnet mreža/maliciozni softver/daljinsko upravljanje ličnim računarom

Kada se lični računar nekog lica zarazi malicioznim softverom, softver može biti instaliran na računaru koji osumnjičenom dozvoljava da njime upravlja i da ga koristi za vršenje kriminalnih radnji. Između ostalog, osumnjičeni bi mogao da u zaraženom računaru instalira proksi i da preko njega usmerava sav svoj saobraćaj.

U tim slučajevima, internet saobraćaj koji se povezuje sa kriminalnom aktivnošću izgledaće kao da dolazi sa IP adrese nevinog lica. Međutim, moguće su tehničke mere koje bi mogle da omogućе identifikaciju stvarnog izvora saobraćaja. Na primer, praćenjem IP saobraćaja koji putuje ka zaraženom računaru i iz njega, može biti moguće identifikovati IP adresu osumnjičenog koji kontroliše taj računar. Ovo je najverovatnija mogućnost kada kriminalac zarazi mali broj računara i komunicira sa njima pojedinačno.

Međutim, ne treba potcenjivati složenost komandno-kontrolne (C&C) infrastrukture koju kriminalci koriste za upravljanje mrežama zaraženih računara (koje se ponekad nazivaju botnet mreže). Hakeri koji upravljaju botnet mrežama koriste mnoge tehnike da bi prikrili svoje aktivnosti²⁶,²⁷ i da bi omogućili svom kontrolnom saobraćaju da prolazi kroz *firewall*²⁸.

Analizom računara nekog lica moglo bi se otkriti prisustvo malicioznog softvera, što bi podržalo tvrdnju da je treće lice moglo da izdaleka kontroliše taj računar. Međutim, nije nemoguća ni situacija da osumnjičeni namerno zarazi svoj računar malicioznim softverom kako bi mu odbrana bila da nije odgovoran za radnje izvršene na tom računaru ili uz njegovu pomoć. Zbog toga, izazov koji predstavlja "postavljanje osumnjičenog za tastaturu" može da zahteva dodatne netehničke mere, kao što je tajni nadzor kojim bi se sa određenom merom izvesnosti utvrdilo koje lice je izvršilo koje radnje ili, ekvivalentno tome, kako bi se određeno lice isključilo kao izvršilac tih krivičnih dela.

²⁵ Još detalja o radu skrivenih servisa možete naći na: <https://www.torproject.org/docs/hidden-services.html>

²⁶ https://en.wikipedia.org/wiki/Fast_flux

²⁷ https://en.wikipedia.org/wiki/Domain_generation_algorithm

²⁸ http://www.pcworld.idq.com.au/article/417011/malware_increasingly_uses_dns_command_control_channel_avoid_detection_experts_say/

Inspektori su takođe suočeni sa izazovima u vezi s tim kako da upozore korisnika na infekciju i koji su pravi instrumenti koje treba da koriste kako bi uklonili maliciozni softver. Trenutak kada korisnike treba obavestiti da su im računari zaraženi je važan i o tome se mora odlučiti na osnovu statusa istrage. Uklanjanje malicioznog softvera iz zaraženih mašina treba obaviti na takav način da se izbegne nelegalan pristup ili tajni nadzor komunikacije bez odgovarajućeg pristanka/ovlašćenja.

2.2.5 Korišćenje otvorene, javne ili ukradene bežične mreže

Otvorene bežične mreže su specijalno napravljene tako da dozvole svakome da se na njih poveže i koristi internet. Otvorene bežične mreže predstavljaju rizik jer kriminalci mogu da koriste internet konektivnost tako da se njihove aktivnosti mogu povezati jedino sa izvorom otvorene bežične mreže i ni sa kim više. Neke, mada ne sve, otvorene bežične mreže zahtevaju prijavljivanje i/ili prave dnevnike.

Sličan problem se pojavljuje u slučajevima kada napadač može da pogodi ili "provali" lozinku za prijavljivanje na zatvorenu bežičnu mrežu. Jedan često pominjan scenario koji se pojavljuje kod upotrebe hakovanih pristupnih tačaka bežičnog interneta i/ili ukradenog pristupa bežičnom internetu je kada napadač parkira automobil ispred neke poslovne zgrade i koristi njen bežični internet da vrši kriminalne radnje. U takvim slučajevima, malo je verovatno da će biti dostupni bilo kakvi identifikujući zapisi o povezivanju sa bežičnom mrežom (naročito u slučaju manjih preduzeća) i zato neće postojati način da se nastavi sa istragom i da se locira osumnjičeni. Može se desiti da osumnjičeni koristi istu lokaciju više puta, u kom slučaju nadzor te lokacije može da dovede do identifikacije osumnjičenog.

Sličan problem se pojavljuje zbog toga što postoje mnoga mesta na kojima je moguć relativno anoniman pristup internetu, kao što su biblioteke, univerziteti ili internet kafei.

Glavna karakteristika ovog problema je mogućnost da osumnjičeni dobije praktično anoniman pristup internetu tako što će se koristiti internet konektivnost, a u nekim slučajevima i računare čiji je vlasnik neko treće lice.

Slično onome što je rečeno na kraju prethodnog dela, analiza mreže tog lica mogla bi da otkrije postojanje otvorenog bežičnog interneta, što bi podržalo tvrdnju da je bežični internet moglo da koristi neko treće lice. Međutim, takođe se može zamisliti mogućnost da osumnjičeni namerno otvori svoju bežičnu mrežu kako bi mu odbrana bila da nije odgovoran za radnje izvršene putem bežičnog interneta. Ponovo, mogu biti potrebne dodatne netehničke mere, kao što je tajni nadzor, da bi se sa određenom merom izvesnosti utvrdilo koje lice je izvršilo koje radnje ili, ekvivalentno tome, isključila mogućnost da je neko konkretno lice izvršilo ta krivična dela.

Tajni nadzor komunikacije putem interneta je još jedna tehnika koja se može upotrebiti da bi se utvrdila umešanost različitih lica u kriminalne aktivnosti.

2.2.6 Identifikacija vlasnika IP adrese

WHOIS je besplatni servis koji pruža informacije o vlasniku naziva nekog domena, što uključuje njegovo ime, prezime i kontaktne podatke.

Prema ICANN-u²⁹, svetskom administratoru naziva domena, "servis WHOIS je besplatan, javno dostupan imenik koji sadrži kontaktne i tehničke informacije registranata registrovanih naziva domena. Svako kome je potrebno da sazna ko stoji iza naziva domena neke internet stranice može da uputi zahtev za dobijanje te informacije preko WHOIS-a.

Podatke prikupljaju i stavljaju na raspolaganje registri nacionalnih domena i ovlašćeni registri pod uslovima iz svojih ugovora sa ICANN-om. WHOIS nije jedinstvena baza podataka sa centralnim upravljanjem. U stvari, podaci o registraciji drže se na različitim mestima i vodi ih više registara nacionalnih domena i ovlašćenih registara. Oni određuju sopstvena pravila za servis WHOIS, koja su u skladu sa minimumom zahteva koji su utvrđeni u njihovim ugovorima sa ICANN-om".

WHOIS se koristi da bi se saznalo kome je dodeljena neka konkretna IP adresa. Problem je što baza podataka WHOIS nije uvek tačna. Registri nacionalnih domena imaju obavezu da povremeno šalju poruke onima koji su kod njih registrovani, ali njihova dužnost nije da proveravaju tačnost podataka koje registrant dostavi. Ovo je poseban problem kada treba da se ustanovi ko je vlasnik nekog konkretnog naziva domena.

U slučaju IP adresa, prepoznat je još jedan sistemski problem, a to je sublokacija IP adresa³⁰. Problem se pojavljuje ako internet provajder kome je dodeljen niz IP adresa potom dodeli neke od tih IP adresa nekom subprovajderu ali nema tačne ili ažurirane informacije o tome ko koristi koje IP adrese. Poseban problem je to što provajder možda neće uvek prijaviti sublokaciju registru baze podataka WHOIS, što znači da baza podataka WHOIS neće sadržavati tačne informacije o krajnjem upravljaču date IP adrese.

Podaci iz WHOIS-a mogu se smatrati posebnim oblikom informativnih podataka o pretplatnicima, koji su javno dostupni na internetu uz neograničen pristup. Međutim, u svetlu činjenice da je 25. maja 2018. godine stupila na snagu Opšta uredba EU o zaštiti podataka (GDPR) pristup WHOIS-u će se promeniti da bi se obezbedila usaglašenost sa GDPR-om.³¹

PITANJA ZA RAZMIŠLJANJE

- 1. Da li nalog za nadzor neke IP adrese može biti formulisan tako da ne utiče na prava nevinih trećih lica?**
- 2. Kako bi se moglo utvrditi da li je neku aktivnost koja se povezuje sa određenom IP adresom izvršio držalac te IP adrese ili je izvršena izdaleka s obzirom na činjenicu da je njegov računar zaražen malicioznim softverom?**
- 3. Koji uslovi se moraju ispuniti da bi se dobila naredba na osnovu koje bi se**

²⁹ Internet korporacija za dodeljena imena i brojeve (eng. Internet Corporation for Assigned Names and Numbers), međunarodna organizacija zadužena za definisanje politika i povezanih ugovora sa registrima nacionalnih internet domena i ovlašćenim registrima.

³⁰ <https://blog.apnic.net/2016/11/28/sub-allocation-system-undermines-integrity-whois-accuracy/>

³¹ Za dodatnu literaturu o pristupu WHOIS vidi: <https://www.icann.org/news/blog/data-protection-privacy-update-seeking-input-on-proposed-interim-model-for-gdpr-compliance>

omogućilo utvrđivanje IP adrese koju koristi konkretni osumnjičeni iz stvarnog sveta?

4. Koji uslovi moraju biti ispunjeni da bi se dobila naredba kojom bi se omogućila identifikacija nosioca IP adrese u stvarnom svetu koji je umešan u kriminalne radnje?

2.3 Rad sa provajderima internet usluga

2.3.1 Vrsta traženih podataka

Za potrebe krivične istrage mogu biti potrebne tri vrste podataka:

- Podaci o pretplatnicima
- Podaci o saobraćaju
- Podaci iz sadržaja.

U mnogim jurisdikcijama, uslovi za pristupanje informacijama o pretplatnicima uglavnom su blaži od onih za podatke o saobraćaju, a najstroži režim se primenjuje na podatke iz sadržaja. Vrsta podataka koja se zahteva očigledno utiče na prirodu zahteva koji treba uputiti multinacionalnom pružaocu usluga da bi se dobio pristup tim podacima. Neki, mada ne svi, multinacionalni pružaoci usluga imaju neki oblik ubrzane dobrovoljne saradnje putem koje se mogu obezbediti podaci o pretplatniku dok se čeka prijem formalnih pravnih dokumenata.

2.3.1.1 Podaci o pretplatniku

Podaci o pretplatniku su najčešće tražene informacije u domaćim i međunarodnim krivičnim istragama i bez njih je često nemoguće nastaviti sa istragom³². Termin podaci o pretplatniku definisan je u članu 18 stav 3 Budimpeštanske konvencije na sledeći način:

"U smislu ovog člana, izraz "podaci o pretplatniku" označava svaki podatak sadržan u obliku računarskog podatka ili u bilo kom drugom obliku, koje poseduje davalac usluga i koji se odnose na pretplatnika tih usluga, osim podataka o saobraćaju ili podataka iz sadržaja koji se prenosi, na osnovu kojih može da se ustanovi:

- a) vrsta korišćene komunikacijske usluge, tehnički detalji i vremenski period korišćenja usluge;*
- b) identitet pretplatnika, poštanska adresa ili geografsko odredište, broj telefona i ostali brojevi pristupa, podaci o računima i plaćanjima, dostupni na osnovu ugovora ili sporazuma o korišćenju usluge;*
- c) svaka druga informacija o mestu postavljanja komunikacione opreme, dostupne na osnovu ugovora ili sporazuma o korišćenju usluge.*

Podatke o pretplatniku će verovatno imati pružaoci usluga iako se ti podaci u stvarnosti mogu čuvati u serverima u drugim jurisdikcijama. Zbog toga ne mora uvek biti jasno kome treba uputiti zahtev za dobijanje podataka o pretplatniku.

2.3.1.2 Podaci o saobraćaju

³² T-CY Report on Rules on obtaining subscriber information adopted at the on 12th plenary (Izveštaj T-CY o pravilima za dobijanje podataka o pretplatnicima, usvojen na 12. plenarnom zasedanju), 2-3. decembra 2014. godine. Dostupno na: <https://rm.coe.int/16802e7ad1>

Dnevničke datoteke koje evidentiraju aktivnosti operativnog sistema nekog računara ili drugog softvera ili komunikaciju između računara od ključne su važnosti za predmete visokotehnološkog kriminala i mogu biti jednako važne u predmetima koji uključuju imovinsku korist od krivičnih dela izvršenih putem interneta. "Podaci o saobraćaju" definišu se u članu 1 tačka d) Budimpeštanske konvencije na sledeći način:

"Podatak o saobraćaju" označava svaki računarski podatak koji se odnosi na komunikaciju preko računarskog sistema, proizvedenu od računarskog sistema koji je deo lanca komunikacije, a u kojoj su sadržani podaci o poreklu, odredištu, putanji, vremenu, datumu, veličini, trajanju ili vrsti predmetne usluge."

2.3.1.3 Podaci iz sadržaja

Konačno, podaci iz sadržaja takođe su često potrebni u krivičnim istragama. Prema stavu 209 Eksplanatornog izveštaja Budimpeštanske konvencije:

"Podaci iz sadržaja nisu definisani u Konvenciji, ali odnose se na komunikacijski sadržaj komunikacije; tj. značenje ili smisao komunikacije, ili poruku ili informaciju koja se prenosi komunikacijom (osim podataka o saobraćaju)."

Treba takođe napraviti razliku između "sačuvanih" podataka iz sadržaja, koji se već nalaze u računarskom sistemu i "budućih" podataka iz sadržaja koji još uvek nisu dostupni i treba da budu prikupljeni, na primer, putem tajnog nadzora komunikacije. Tajni nadzor na osnovu naredbe suda može izvršiti policija ili neko specijalizovano telo direktno ili uz pomoć pružaoca usluge. Njegova upotreba je često ograničena na teška krivična dela.

2.3.2 Direktiva EU o zadržavanju podataka proglašena je nevažećom na osnovu odluke SPEU

Kao što je gore opisano, identifikacija učinilaca u sajber svetu često zavisi od pristupa podacima koje drže privatni provajderi internet usluga. Povezivanje IP adrese sa podacima o nekom licu (pretplatnikom na neku IP adresu, nalogom za elektronsku poštu ili *Facebook* nalogom) i interakcija osumnjičenog sa drugim mogućim osumnjičenima (podaci o saobraćaju), pa čak i sadržaj takve interakcije, predstavljaju ključni deo otkrivanja učinioca, drugih osumnjičenih i obezbeđenja dokaza o krivičnom delu.

Sve je ovo moguće samo ako privatna kompanija zadrži potrebne podatke (podatke o pretplatniku, podatke o saobraćaju i/ili podatke iz sadržaja). Zakonska obaveza zadržavanja podataka za potrebe organa za sprovođenje zakona osporena je pred Sudom pravde Evropske unije (SPEU)³³. U odluci ovog suda u spojenim predmetima C-93/12 i C-594/12 (*Digital Rights* Irska i Seitlinger i drugi), Direktiva o zadržavanju podataka 2006/24/EC³⁴ proglašena je nevažećom. Ova odluka je dovela do poništavanja relevantnog nacionalnog zakonodavstva u nekim zemljama EU, gde su provajderi imali obavezu da zadržavaju podatke o saobraćaju tokom izvesnog perioda koji je varirao od 6 meseci do 2 godine.

³³ Presuda Suda pravde Evropske unije u spojenim predmetima C-293/12 i C-594/12. *Digital Rights* Irska i Seitlinger i drugi. Dostupno na: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>

³⁴ Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Direktiva 2006/24/EC od 15. marta 2006. o zadržavanju generisanih ili obrađenih podataka u vezi s obezbeđenjem javno dostupnih elektronskih komunikacionih servisa ili mreža za javnu komunikaciju i izmenama i dopunama Direktive 2002/58/EC). (nevažeća)

Usled toga, provajderi više nemaju obavezu da čuvaju (zadržavaju) podatke o saobraćaju za potrebe istraga teškog kriminala u periodu koji je prethodno zahtevalo nacionalno zakonodavstvo, već čuvaju podatke samo u periodu koji je potreban za ispostavljanje računa ili za druge komercijalne svrhe. U praksi bi ovo značilo oko 1-3 meseca. EU još uvek nije usvojila novi pravni instrument, a mnoge države još uvek definišu odgovarajuća zakonska rešenja za rešavanje pravnih problema. Izgleda, međutim, da poseban izazov predstavlja odgovor na očekivanje Suda da se izbegne da, na generalizovan način, budu pokrivena sva lica, sva sredstva elektronske komunikacije i svi podaci o saobraćaju bez ikakve razlike, ograničenja ili izuzetaka koji se prave u svetlu cilja borbe protiv teškog kriminala,

Jedan od mogućih pristupa moglo bi biti regulisanje naloga za predaju u cilju čuvanja podataka (o saobraćaju) posle izdavanja zakonskog zahteva za ograničeni vremenski period.

Pošto su se razlozi za odstupanje zasnivali na gledištu suda da ova direktiva prekoračuje ograničenja načela srazmernosti, jer na ozbiljan način ometa osnovna prava poštovanja privatnog života i zaštite ličnih podataka, ova odluka mogla bi da ima uticaj i na države koje nisu članice EU, naročito ako bi nacionalno zakonodavstvo bilo osporeno pred nacionalnim ustavnim sudovima ili u slučaju pojedinačne predstavke Evropskom sudu za ljudska prava zbog kršenja člana 8 Konvencije o ljudskim pravima.

Glavne tačke sudske odluke bi zato mogle biti relevantne za nacionalnog zakonodavca. Sud je utvrdio da direktiva na posebno ozbiljan način ometa osnovna prava na poštovanje privatnog života i zaštitu ličnih podataka. Takođe je verovatno da će ona kod zainteresovanih lica takođe izazvati osećaj da su njihovi privatni životi predmet stalnog nadzora.

Sud je napomenuo da direktiva ne reguliše sadržaj komunikacija i da zadržavanje podataka u cilju njihovog mogućeg prenošenja nadležnim nacionalnim organima zaista ispunjava cilj od opšteg interesa, i to borbu protiv teškog kriminala i, najzad, i javnu bezbednost. Međutim, navodi se da je ona prekoračila ograničenja koja se odnose na usklađenost sa načelom srazmernosti, i da kontrola diskrecionog prava zakonodavca treba da bude stroga.

Iako se zadržavanje podataka koje zahteva direktiva može smatrati adekvatnim za postizanje cilja kome ona stremlji, široko i naročito ozbiljno mešanje direktive u osnovna prava poštovanja privatnog života i zaštite ličnih podataka prekoračilo je ograničenja koja se odnose na usklađenost sa načelom srazmernosti, kao što je:

- Nije dovoljno zaokružena da bi obezbedila da ometanje bude stvarno ograničeno na ono što je striktno neophodno,
- Uopšteno se odnosi na sva lica, sva sredstva elektronske komunikacije i sve podatke o saobraćaju bez ikakve razlike, ograničenja ili izuzetaka koji se prave u svetlu cilja borbe protiv teškog kriminala,
- Ne postoji objektivni kriterijum na osnovu koga nadležni nacionalni organi imaju pristup podacima i mogu da ih koriste samo u cilju prevencije, otkrivanja ili krivičnog gonjenja u vezi sa delima koja se mogu smatrati dovoljno teškim da opravdavaju takvo ometanje. Ona samo pominje 'teška krivična dela',
- Pristup podacima ne zavisi od prethodne kontrole suda ili nekog nezavisnog upravnog tela,

- Ona definiše period zadržavanja od najmanje šest meseci, ne praveći nikakvu razliku između kategorija podataka koji se odnose na relevantna lica ili moguću korisnost podataka,
- Određen je rok između najmanje šest meseci i najviše 24 meseca, ali nema objektivnih kriterijuma na osnovu kojih se mora utvrditi rok za zadržavanje kako bi bio ograničen na ono što je striktno neophodno,
- Nedostaju joj dovoljne zaštitne mere koje bi obezbedile delotvornu zaštitu podataka od rizika od zloupotrebe,
- Ona ne obezbeđuje nepovratno uništenje podataka na kraju perioda zadržavanja.

Ako želite da pročitate nešto više o uticaju ove odluke, Franziska Boehm i Mark D. Cole su u svom članku "Zadržavanje podataka posle presude Suda pravde Evropske unije" od 30. juna 2014³⁵ istakli neke od relevantnih aspekata. Oni su naglasili da, ne samo što se izjave Suda ne odnose isključivo na slučaj same Direktive, već i utvrđuju opšta načela za slične mere za zadržavanje podataka. Ova načela obuhvataju sledeće tačke:

- Prikupljanje, zadržavanje i prenošenje podataka svako za sebe predstavljaju kršenje članova 7 i 8 i zahtevaju strog test neophodnosti i srazmernosti.
- Sud jasno odbacuje blanketno zadržavanje podataka lica koja nisu osumnjičena kao i nedefinisan ili čak dug period zadržavanja zadržanih podataka.
- Sud vidi osetljiv problem u tome što se podaci koji su prvobitno prikupljeni za druge svrhe kasnije koriste za potrebe organa zaduženih za sprovođenje zakona. Potrebna je veza između ugrožavanja javne bezbednosti i podataka koji su zadržani za tu svrhu.
- Ta veza u znatnoj meri utiče na odnos između privatnih i javnih aktera. Organima zaduženim za sprovođenje zakona dozvoljeno je da pristupe podacima koji su prikupljeni za druge svrhe samo u posebnim slučajevima.
- Sud izričito zahteva delotvorna procesna pravila, kao što je nezavisan nadzor i kontrola pristupa.
- Prikupljanje i korišćenje podataka za potrebe organa zaduženih za sprovođenje zakona nosi sa sobom rizik stigmatizacije zbog ubacivanja podataka u baze podataka ovih organa. Ovaj rizik treba razmotriti i uzeti u obzir prilikom razmatranja drugih postojećih ili planiranih mera za zadržavanje podataka na nivou organa reda i država članica EU.

Da bi rešilo probleme koji su istaknuti u presudi SPEU, Ujedinjeno Kraljevstvo je 29. novembra 2016. godine donelo Zakon o istražnim ovlašćenjima iz 2016. Pored ostalih važnih tehnika, on provajdere internet usluga obavezuje da zadrže 'podatke o konekcijama' u periodu od 12 meseci. Ovo je blaži oblik ometanja od evidentiranja svih podataka o pretraživanju i osmišljen je da bi se izašlo u susret zabrinutosti koju je SPEU izrazio u vezi sa nesrazmernim ometanjem. Zakon takođe donosi nova ovlašćenja koja, sa snagom naloga, omogućavaju rukovođeni nadzor i zadržavanje podataka o pretraživanju koje je izvršio osumnjičeni, itd.

³⁵ Data Retention after the Judgement of the Court of Justice of the European Union (Zadržavanje podataka posle presude Suda pravde Evropske unije), Prof. Dr. Franziska Boehm et al., Munster/Luksemburg, 30. juna 2014. Dostupno na: http://www.janlabrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf

2.3.3 Nacionalni pružaoci internet usluga

Podaci koje pružalac internet usluga zadržava važni su za identifikaciju učinioca i njegovih saučesnika, njihove povezanosti u vremenu i prostoru i dokaze o sadržaju komunikacije (sadržaju elektronske pošte, objavama na društvenim mrežama kao što je *Facebook*).

Obaveze pružalaca internet usluga regulisane su nacionalnim odredbama o zadržavanju podataka (o saobraćaju) i uslovima za pristupanje takvim podacima i za njihovo korišćenje za potrebe krivične istrage. Podaci mogu biti kategorizovani kao podaci o pretplatnicima, podaci o saobraćaju i podaci iz sadržaja.

Podaci o pretplatnicima se, u smislu privatnosti, smatraju manje osetljivim i njima se manje narušava privatnost nego što je to slučaj sa podacima o saobraćaju i podacima iz sadržaja. Oni predstavljaju najčešće tražene informacije u domaćim i međunarodnim krivičnim istragama koje se odnose na visokotehnološki kriminal i elektronske dokaze. Bez ovih informacija često je nemoguće nastaviti sa istragom.

Podatke o pretplatnicima obično drže privatni pružaoci internet usluga i oni se mogu dobiti na osnovu naloga za predaju (podataka) izdatog od strane policije ili tužioca. Međutim, u slučaju dinamičkih IP adresa, mnoge države zahtevaju naredbu suda, pošto su tu uključeni i neki podaci o saobraćaju. U većini država naredba suda se zahteva za: pristupanje podacima o saobraćaju (za pitanje zadržavanja podataka vidi prethodni deo); kod naredbe o zaštiti podataka (da se podaci o saobraćaju nadalje čuvaju); za nadzor nad podacima o saobraćaju i; za pristupanje podacima iz sadržaja, a naročito za tajni nadzor komunikacija (obično se smatra da ovo poslednje najviše narušava privatnost i zato podleže posebnim zaštitnim merama, uslovima i načelu srazmernosti).

Pored zakonskih zahteva, važni su i praktični i tehnički aranžmani za prenošenje podataka između pružalaca internet usluga i organa zaduženih za sprovođenje zakona, naročito u slučaju nadzora i prenošenja podataka uživo, što omogućuje brzu obradu podataka.

Još jedna oblast saradnje između organa zaduženih za sprovođenje zakona i ISP je pitanje blokiranja i obaranja internet stranica u slučaju krivičnih dela ili nedozvoljenog sadržaja. U ovom kontekstu se najčešće pominje dečja pornografija, ali mogu biti relevantni i drugi oblici, kao što je govor mržnje, javno podsticanje na vršenje terorističkih dela ili kršenje prava intelektualne svojine. Iako bi za takvu meru obično bila potrebna naredba suda, vlasnik ili urednik internet stranice podstiču se da "dobrovoljno" deluju zbog kršenja internog kodeksa ponašanja. Iako bi takav pristup mogao biti najefikasniji, naročito u slučaju *prima facie* kršenja zakona (kao što je pornografski materijal), on bi mogao da dovede do nekih problema koji se odnose na moguće ometanje slobode govora, kako je utvrđeno u Studiji Saveta Evrope o filtriranju, blokiranju i obaranju nelegalnih sadržaja na internetu iz 2016. godine³⁶.

PITANJA ZA RAZMIŠLJANJE

1. Šta se podrazumeva pod terminom "podaci o pretplatniku"?

³⁶ Council of Europe Study on filtering, blocking and take-down of Illegal Content on the Internet (Studija Saveta Evrope o filtriranju, blokiranju i obaranju nelegalnih sadržaja na internetu), jun 2016. Dostupno na: <https://www.coe.int/en/web/cybercrime/-/study-on-filtering-blocking-and-take-down-of-illegal-content-on-the-internet>

2. Šta se podrazumeva pod terminom "podaci o saobraćaju"?
3. Šta se podrazumeva pod terminom "podaci iz sadržaja"?
4. Koje posledice odluka SPEU o zadržavanju podataka ima na identifikaciju osumnjičenog iz stvarnog sveta na osnovu IP adrese koja se povezuje sa kriminalnom aktivnošću?

2.4 Multinacionalni pružaoci usluga

U predmetima koji uključuju imovinsku korist stečenu vršenjem krivičnih dela putem interneta, kao i u mnogim krivičnim istragama visokotehnološkog kriminala, ključne dokaze imaju organizacije iz privatnog sektora, kao što su *Facebook*, *Google*, *Microsoft*, *Twitter*, *Yahoo!* i drugi. Saradnja između nadležnih organa i ovih multinacionalnih pružalaca usluga je, zato, neophodna da bi se obezbedili elektronski dokazi. U priručniku kao što je ovaj nije moguće obezbediti informacije o svakom od različitih multinacionalnih pružalaca usluga sa kojima bi potencijalni čitalac možda imao potrebu da stupi u kontakt; detalji koji se odnose na postupanje sa zahtevima organa zaduženih za sprovođenje zakona obično se kod svakog pružaoca usluga mogu naći na njegovoj internet prezentaciji. Zbog toga je uložan napor da se kategorizuju ključni aspekti mera multinacionalnih pružalaca usluga za sprovođenje zakona.

Cilj je da se obezbedi okvir za razmatranje načina na koji treba raditi sa konkretnim pružaocem usluga u budućnosti. Drugo, to će takođe pomoći da se razjasne faktori koje će multinacionalni pružaoci usluga uzeti u obzir kada budu razmatrali pristigle zahteve organa zaduženih za sprovođenje zakona, a, samim tim, i faktori koje treba uzeti u obzir kada se formuliše zahtev koji treba uputiti pružaocu usluga kako bi se maksimalno povećala mogućnost obezbeđenja uspešnog ishoda.

Grupa za dokaze u kladu (CEG) pripremila je obiman dokument o pitanju pristupanja organa zaduženih za sprovođenje zakona podacima koje drže multinacionalni pružaoci usluga³⁷. U delu **Error! Reference source not found.** biće detaljnije obrađeni mnogi interesantni aspekti. Da naglasimo neke od njih:

- CEG zaključuje da međunarodna pravna pomoć ostaje glavno sredstvo za pribavljanje elektronskih dokaza iz stanih jurisdikcija radi korišćenja u domaćim krivičnim postupcima. Ovo se naročito odnosi na podatke iz sadržaja.
- Pristup podacima o pretplatniku manje narušava privatnost i treba da bude olakšan. Član 18 o domaćem nalogu za predaju podataka treba da se koristi i za multinacionalne provajdere koji rade na teritoriji neke države – pripremljen je nacrt Smernice br. 10 o nalogima za predaju podataka o pretplatnicima.
- Priznata je direktna dobrovoljna saradnja pružalaca internet usluga iz SAD sa stranim organima zaduženim za sprovođenje zakona, gde se ima u vidu i veliko povećanje broja zahteva za međunarodnu pravnu pomoć.
- CEG je predložio da se razmotri izrada dodatnog protokola kako bi se rešili neki postojeći izazovi, odnosno da se olakša režim za pristup podacima o pretplatnicima i da se pod određenim uslovima dozvole direktni zahtevi pružiocima internet usluga.

³⁷ T-CY (2016)5, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY (T-CY (2016)5, Pristup krivičnog pravosuđa elektronskim dokazima koji se drže u kladu: preporuke koje treba da razmotri T-CY), Finalni izveštaj, 16. septembar 2016. Dostupno na: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>

2.4.1 Nadležnost

Organu krivičnog pravosuđa često nije očigledno u kojoj jurisdikciji su traženi podaci pohranjeni i/ili koji pravni režim se primenjuje na podatke³⁸. Pružalac usluga može da ima sedište u jednoj jurisdikciji, a da primenjuje pravni režim druge jurisdikcije, dok se podaci čuvaju u trećoj jurisdikciji. Ako mesto gde se nalaze podaci određuje nadležnost, moguće je i da pružalac usluga ne mora odmah da zna gde se nalaze podaci. Čak i ako je mesto na kome se nalaze podaci poznato, nije jasno čija pravila treba primeniti da bi organi krivičnog pravosuđa dobili zakonit pristup. Može se tvrditi da nadležnost može odrediti mesto gde se nalazi sedište pružaoca usluge, ili njegove filijale, ili mesto na kome se nalaze podaci ili zakon države u kojoj se osumnjičeni pretplatio na uslugu, ili lokacija ili državljanstvo osumnjičenog³⁹.

2.4.2 Opšta pozicija

U svim slučajevima (osim u slučaju hitnih zahteva, kako se navodi u tekstu dole), biće potrebno sprovesti postupak međunarodne pravne pomoći kako bi se dobio pristup podacima iz sadržaja.

Što se tiče podataka o pretplatniku, multinacionalni pružaoci internet usluga mogu biti podeljeni u dve velike kategorije; one koji odgovaraju na pravne zahteve iz jurisdikcija izvan Sjedinjenih Američkih Država i onih koji traže da im neki sud iz SAD uruči zahtev za međunarodnu pravnu pomoć.

2.4.3 Zahtevi za zaštitu podataka

Neki pružaoci usluga će prihvatiti zahteve za zaštitu podataka i na taj način će zaštititi podatke tokom nekog vremenskog perioda (obično negde oko 90 dana) do prijema formalne pravne dokumentacije. Ako se traži zaštita podataka u periodu dužem od 90 dana, zahtev za produženje treba poslati pružaocu usluge pre isteka devedesetodnevog perioda.

2.4.4 Hitni zahtevi

U slučajevima kad postoji neposredan rizik od štete, smrti ili teške telesne povrede, većina multinacionalnih pružalaca usluga sarađivaće sa zahtevima organa reda za dobijanje informacija kada se može dokazati da pružalac usluga ima informacije koje mogu biti neophodne za sprečavanje štete, smrti ili teške telesne povrede. Jedan praktični izazov u ovom smislu, koji je naglašen na drugom mestu u okviru ovog kursa⁴⁰, je da mnoge zemlje nemaju usvojeno zakonodavstvo koje dozvoljava otkrivanje podataka domaćim organima krivičnog pravosuđa u hitnim situacijama. Pre svega, i naročito, SAD imaju takvu odredbu koja omogućuje multinacionalnim pružiocima usluga sa sedištem u SAD da odgovaraju na hitne zahteve, ali kada sedište pružaoca usluga nije u SAD, ili u malom

³⁸ Discussion paper prepared by the T-CY Cloud Evidence Group, Criminal justice access to data in the cloud: challenges (Dokument za diskusiju koju je pripremila Radna grupa T-CY za pristup dokazima u kladu, Pristup krivičnog pravosuđa podacima koji se drže u kladu: izazovi), maj 2015. Dostupno na:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59>

³⁹ T-CY (2016)5, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY (Pristup krivičnog pravosuđa elektronskim dokazima koji se drže u kladu: preporuke koje treba da razmotri T-CY), finalni izveštaj, 16. septembar 2016. Dostupno na:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>

⁴⁰ Vidi deo 4.2.2.2.2

broju drugih zemalja, pravni osnov za otkrivanje informacija može da predstavlja dodatan praktični izazov.

2.4.5 Obim zahteva

Većina multinacionalnih pružalaca usluga odbijaće preširoke zahteve za dobijanje informacija. Definicija prihvatljivog obima obično ne postoji, osim što se navede da "preširoki ili nejasni zahtevi neće biti obrađeni". Zato, da biste imali najveću šansu za uspešan odgovor, zahteve treba formulisati tako da budu što uži i, kad god je to moguće, treba navesti naloge koje subjekat ima prema jedinstvenom identifikatoru koji se koristi na konkretnoj razmatranoj platformi.

Ne mora uvek biti očigledno koji jedinstveni identifikator se koristi na nekoj određenoj platformi. U mnogim slučajevima, ali ne uvek, dovoljno je korisničko ime i/ili adresa elektronske pošte koja se povezuje sa konkretnim nalogom.

2.4.6 Obaveštavanje subjekta zahteva

U mnogim slučajevima, kada se primi zahtev od nekog organa zaduženog za sprovođenje zakona u vezi sa korisnikom usluga multinacionalnog provajdera, politika tog provajdera je da obavesti subjekta zahteva o postojanju tog zahteva. Ovo će biti učinjeno osim ako zakon ili naredba suda ne zabranjuju obaveštavanje.

Zbog toga, ako istraga može biti ugrožena zbog obaveštavanja subjekta, naredba koja predstavlja osnov za zahtev za dobijanje informacija od pružaoca usluga mora da uključi i zabranu obaveštavanja subjekta zahteva.

Pored toga, neki pružaoci usluga dalje navode da, ako im se u zahtevu organa zaduženih za sprovođenje zakona skrene pažnja na stalno kršenje njihovih uslova korišćenja, oni mogu preduzeti mere za sprečavanje budućih zloupotreba, što uključuje i postupke kojima se korisnik može upozoriti da pružalac usluga zna za to ponašanje.

PITANJA ZA RAZMIŠLJANJE

- 1. Zašto je važno da se pružaocu usluga posebno naredi da zaštiti podatke koji se traže u krivičnom postupku do prijema formalne dokumentacije za otkrivanje dokaza?**
- 2. Koji uslovi moraju biti ispunjeni pre nego što se u naredbu koja pružaoca usluge obavezuje da dostavi informacije koje se odnose na njegovog korisnika može uključiti klauzula kojom se pružalac usluge sprečava da (direktno ili indirektno) obavesti subjekta tog zahteva?**
- 3. Koje mogućnosti postoje u slučaju kad se zna da je nalog kod multinacionalnog pružaoca usluga povezan sa kriminalnom aktivnošću u vašoj jurisdikciji, ali, bez dobijanja informacije od pružaoca usluge, nije moguće znati da li se držalac tog naloga nalazi u vašoj jurisdikciji ili ne?**
- 4. S obzirom na dužinu trajanja postupka međunarodne pravne pomoći, koje mogućnosti postoje (ako postoje) za brže obezbeđenje pristupa podacima iz sadržaja koje drži multinacionalni pružalac usluga?**

3 Finansijske istrage

3.1 Uvod

Koncept pronalaženja imovinske koristi stečene izvršenjem krivičnih dela putem interneta spaja pristupe visokotehnološke istrage, finansijske istrage i istrage pranja novca sa ciljem povećanja efikasnosti i uspeha krivičnih istraga i krivičnog postupka, kako iz perspektive procesuiranja kriminalca, tako i iz perspektive pronalaženja i trajnog oduzimanja imovinske koristi.

Priručnik sa osnovnog kursa sadrži osnovna i detaljna objašnjenja finansijske istrage, uključujući i definisanje njenog obima i elemenata. Ovde će ukratko biti obrađena definicija finansijske istrage, kao i njeni elementi i neke specifičnosti koje se odnose na krivična dela izvršena putem interneta, uključujući i istrage u oblasti visokotehnološkog kriminala, a biće obezbeđeno i više detalja o skorijem razvoju koncepta finansijske istrage u EU.

3.2 Finansijske istrage i imovinska korist stečena izvršenjem krivičnih dela putem interneta

Finansijska istraga može imati više značenja, od istrage finansijskog kriminala do, na primer, istrage u cilju oporezivanja. Međunarodni pravni instrumenti ne daju definiciju finansijske istrage, ali u okviru zabrane raspolaganja i trajnog oduzimanja imovinske koristi, kao primer se može koristiti opisna definicija Radne grupa za finansijske mere u borbi protiv pranja novca (FATF).

Takođe treba napomenuti i da termin finansijska istraga može da se odnosi na istragu u cilju pronalaženja imovinske koristi, kako u okviru krivičnog postupka, tako i u okviru (posebnog) građansko-pravnog (*in rem*) postupka. Treba napomenuti i da finansijska istraga može, ali nužno ne mora, da se vodi istovremeno sa istragom pranja novca.

Finansijska istraga je metod vođenja istrage i treba je voditi paralelno sa krivičnom istragom dela kojim je pribavljena imovinska korist, pa čak i u fazi sudskog postupka, sa glavnim (mada ne i isključivim) ciljem da se pronađe i zabrani raspolaganje imovinskom korišću sa ciljem njenog trajnog oduzimanja.

FATF je finansijsku istragu⁴¹ definisao kao istragu o finansijskim poslovima koji se povezuju sa kriminalnom aktivnošću, u cilju

- Otkrivanja veličine kriminalnih mreža ili razmera kriminala
- Otkrivanja i pronalaženja imovinske koristi, terorističkih sredstava ili bilo koje druge imovine koja jeste ili bi mogla da bude predmet oduzimanja
- Pribavljanja dokaza koji se mogu koristiti u krivičnim postupcima.

Pošto imovinska korist teži da bude barem delimično legalizovana i ponovo korišćena u legalnoj ekonomiji, finansijska istraga mogla bi biti u vezi sa i/ili dovesti do istrage pranja novca. Finansijska istraga može da dovede do sumnje da je izvršeno krivično delo pranja novca ili, alternativno, kada finansijsko-obaveštajna jedinica (FOS) analizira sumnjive transakcije ili vrši istragu krivičnog dela pranja novca, imovinska korist od (predikatnog)

⁴¹ FATF (2012), Interpretative Note to Recommendation 30 (Interpretativna beleška uz preporuku br. 30), 2. stav. Vidi takođe: FATF Report on Operational issues. Financial investigation guidance (Izveštaj FATF-a o operativnim pitanjima, Smernice za finansijske istrage), 2012.

krivičnog dela mogla bi da postane predmet trajnog oduzimanja (kao predmet krivičnog dela pranja novca).

3.2.1 Elementi finansijske istrage

Finansijska istraga može se najbolje definisati ako se definišu njeni elementi⁴² i utvrde relevantne međunarodne i nacionalne zakonske odredbe koje treba primeniti u praksi.

Kako je opisano na osnovnom kursu, elementi finansijske istrage su:

1. Otkrivanje krivičnog dela i njegovog učinioca (paralelno sa krivičnom istragom)
2. Utvrđivanje (vrednosti) imovinske koristi
3. Utvrđivanje imovine koja može biti trajno oduzeta
4. Naredba o zabrani raspolaganja imovinom – privremene mere za obezbeđenje trajnog oduzimanja.

Rezultat finansijske istrage i, potencijalno, naredbe o zabrani raspolaganja bilo bi trajno oduzimanje imovinske koristi.

3.2.2 Visokotehnološki aspekti finansijske istrage

Na osnovnom kursu je detaljnije izloženo da se ova četiri elementa finansijske istrage mogu primeniti i u visokotehnološkim istragama i/ili istragama krivičnih dela izvršenih putem interneta, što uključuje i imovinu proisteklu iz krivičnih dela izvršenih na internetu.

Kod istraga krivičnih dela izvršenih putem interneta postoje neke specifičnosti koje treba imati u vidu:

- Ko je učinilac i gde se nalaze dokazi za to krivično delo?
 - Ovo pitanje se odnosi na probleme identifikacije osumnjičenog korišćenjem IP adrese, pristupa podacima o pretplatniku, podacima o elektronskoj komunikaciji ili podacima sa društvenih mreža i, potencijalno, podacima o saobraćaju i podacima iz sadržaja; saradnje, kako sa nacionalnim, tako i sa međunarodnim pružiocima internet usluga; izrade zahteva za zaštitu podataka i naredbe suda za privremeno oduzimanje i dostavljanje elektronskih dokaza.
- Šta predstavlja imovinsku korist?
 - Ovo pitanje ima veze sa imovinom i sistemima plaćanja, kao što je elektronski novac, virtuelne valute (npr. bitcoin) i plaćanja putem internet bankarstva; bankarskim računima pronađenim u inostranstvu; višestrukim transakcijama različitih vrsta, verovatno strukturiranim kako bi se sakrili izvori sredstava; tipologijama pranja novca.
- Šta se može trajno oduzeti/šta može biti imovina osumnjičenog?
 - Kada se razmatraju tokovi novca na internetu, postavlja se i pitanje nadležnosti. Oštećeni i učinioci često se ne nalaze u istoj zemlji. Treba razmotriti trajno oduzimanje imovinske koristi od visokotehnološkog kriminala putem korišćenja pristupa finansijske istrage ili pranja novca. Fokus i meta treba da bude najmanje direktna imovinska korist (plaćena iznuda ili prevarne transakcije) i zabrana raspolaganja vrednošću na identifikovanim bankarskim računima koji su korišćeni za izvršenje krivičnog dela (iznuda preko interneta, računarska prevara).

⁴² Više detalja možete naći u Priručniku osnovnog kursa (1.1.3).

- Važnost vođenja finansijske istrage paralelno sa istragama u oblasti visokotehnološkog kriminala da bi se otkrila imovinska korist (bankarski računi i tok novca, transferi virtuelnih valuta) i postojeća imovina učinioca.
- Naredba o zabrani raspolaganja imovinom
 - Brzo delovanje je ključno u slučajevima elektronskog bankarstva i interneta uopšte. Traženje krivičnog dela pranja novca i korišćenje ovlašćenja i međunarodnih veza finansijsko-obaveštajne službe može biti jedno od mogućih rešenja. Ubrzo potom treba da uslede naredba suda i međunarodna pravna pomoć. Treba razmotriti i korišćenje Interpolovog kanala za međunarodnu pravnu pomoć, Varšavske konvencije i dodatnih mogućnosti koje pruža Budimpeštanska konvencija, bilateralnih sporazuma i reciprociteta.
- Trajno oduzimanje
 - U međunarodnim predmetima pojavljuju se pitanja koja se odnose na međunarodnu pravnu pomoć u vezi sa različitim režimima trajnog oduzimanja i deljenja imovine.

3.2.3 Finansijska istraga u Evropskoj uniji

Holandsko predsedništvo EU je 2016. godine kao jedan od svojih prioriteta postavilo pitanje pronalaženja i oduzimanja imovinske koristi i finansijsku istragu. Predstavljena je procena potreba koje se tiču alata i metoda finansijske istrage u Evropskoj uniji, kao i 'Šest stvari koje treba znati o finansijskoj istrazi'⁴³.

U proceni potreba⁴⁴ naglašeno je da se:

- **Finansijske istrage mogu se primeniti na sva krivična dela koja dovode do stvaranja imovinske koristi:** one nisu ograničene na borbu protiv finansijskog/privrednog kriminala, uključujući pranje novca ili prikupljanje dokaza prevashodno u cilju oduzimanja imovine.
- **Finansijske istrage mogu se voditi u svim fazama krivične istrage i sudskog postupka:** od identifikacije kriminalnog ponašanja, prikupljanja obaveštajnih podataka i prikupljanja dokaza (izgradnje predmeta), pa sve do procesuiranja, izricanja osuđujuće presude i trajnog oduzimanja imovine.

U 'Šest stvari koje treba znati o finansijskoj istrazi' takođe se naglašava da, pošto je finansijska dobit često glavni motiv za vršenje krivičnih dela, imovinska korist se troši na robu i pranjem ubacuje u privredu, često uz korišćenje legitimnih privrednih društava i lica koja ovo olakšavaju. Finansijska istraga je još jedan istražni instrument koji stoji na raspolaganju organima zaduženim za sprovođenje zakona i može se sprovesti da bi se glavni članovi neke kriminalne organizacije poslali iza rešetaka i da bi im se oduzeo novac i imovina. Ako vođama oduzmete finansijska sredstva, znatno ćete im otežati dalje

⁴³ Brochure: The 6 need-to-knows about Financial Investigation (Brošura: Šest stvari koje treba znati o finansijskoj istrazi), februar 2016. Dostupno na: <https://english.eu2016.nl/documents/publications/2016/02/10/brochure-the-6-need-to-knows-about-financial-investigation>

⁴⁴ Needs assessment on tools and methods of financial investigation in the European Union (Procena potreba o sredstvima i metodama finansijskih istraga u Evropskoj uniji), ECORYS, decembar 2015. Dostupno na: https://www.wodc.nl/binaries/2612-summary_tcm28-74130.pdf

bavljenje kriminalom. Ovo finansijsku istragu čini vrlo delotvornim sredstvom za sprečavanje organizovanog kriminala i terorizma.

U 'Stvarima koje treba znati' takođe se naglašava sledeće:

- **Finansijska istraga može se primeniti na sve vrste krivičnih dela:** finansijska istraga može i treba da bude primenjena na sve vrste teškog i organizovanog kriminala, kao što je trgovina ljudima – i krijumčarenje, prevara, trgovina narkoticima i oružjem, i terorizam. Opšta je zablude da je finansijska istraga ograničena na borbu protiv krivičnih dela protiv privrede kao što su prevara, poreska krivična dela, korupcija ili pranje novca.
- **Finansijska istraga tokom čitavog krivičnog postupka:** u idealnom slučaju, finansijske istrage se vode u svim fazama krivičnih istraga i sudskih postupaka. Od proaktivne identifikacije krivičnog dela ili kriminalnih mreža, preko istraga u predmetima i prikupljanja dokaza, sve do procesuiranja i osude učinilaca i trajnog oduzimanja imovine. Međutim, u mnogim slučajevima, finansijski istražitelji ulaze u krivičnu istragu tek u finalnoj fazi da bi ušli u trag, identifikovali i trajno oduzeli imovinsku korist. U takvom slučaju prilika je propuštena. Finansijske istrage treba da počnu što je pre moguće.
- **Neophodna je široka zastupljenost poznavanja finansijskog aspekta:** poznavanje finansijskog aspekta potrebno je na svim nivoima sistema za sprovođenje zakona – od osnovnog znanja o finansijskom aspektu na nivou rada policije u zajednici do visokospecijalizovanog stručnog znanja u oblasti forenzičkog računovodstva koje je potrebno za probijanje pravne ličnosti iza složenih prekograničnih struktura za pranje novca. Važno je da istražitelji u krivičnom postupku znaju da finansijski dokazi treba da se prikupe na mestu izvršenja krivičnog dela i da pozovu specijalizovane finansijske stručnjake kad je to potrebno. Pored toga, stručno znanje tužilaca i sudija o finansijskom aspektu od suštinske je važnosti za razumevanje i ocenjivanje dokumentacije koju pripremaju finansijski istražitelji.
- **Prekogranična saradnja ključna je za uspeh u finansijskim istragama:** istražitelji treba da budu upoznati kako sa neformalnim putevima razmene informacija (CARIN, Europol, INTERPOL) radi vođenja istraga, tako i sa formalnim putevima, npr. zahtevima za međunarodnu pravnu pomoć.
- **Važnost multidisciplinarnе saradnje:** najbolji rezultati se dobijaju kada organi javne vlasti koji su uključeni u finansijske istrage, kao što su organi zaduženi za sprovođenje zakona, javni tužioci, finansijsko-obaveštajne službe (FOS) i poreski organi, udruže svoja stručna znanja, rade zajedno i dele informacije. Pored toga, postoji sve veća svest i želja da privatni partneri, kao što su banke, agencije za nepokretnosti i drugi profesionalni pružaoci usluga mogu i treba da daju vredan doprinos finansijskim istragama.

PITANJA ZA RAZMIŠLJANJE

1. Koje praktične ili zakonske prepreke, ako postoje, možete da navedete, koje bi mogle da spreče paralelno vođenje finansijske istrage i istrage iz oblasti visokotehnološkog kriminala?
2. Koje praktične ili zakonske prepreke, ako postoje, možete da navedete, koje bi mogle da spreče utvrđivanje imovinske koristi koja se drži na internetu ili u virtuelnom obliku?
3. U kom trenutku tokom krivičnog postupka (istraga, sudski postupak, itd.)

može da se pokrene finansijska istraga?

4. Koji uslovi moraju biti ispunjeni pre nego što se odobri zabrana raspolaganja imovinom?

4 PREKOGRANIČNA SARADNJA

4.1 Sažetak

Internet, pored svojih pozitivnih aspekata, pruža prilike za zloupotrebu od strane kriminalaca koji mogu djelovati na skoro nevidljive načine, brzo i anonimno, krijući svoj identitet, dokaze i tragove o imovinskoj koristi. Ovo svojstvo interneta predstavlja izazov za organe reda.

Važno je prepoznati prednosti različitih mogućnosti međunarodne saradnje kroz kombinovanje tri aspekta istrage o imovinskoj koristi stečenoj krivičnim delima izvršenim putem interneta: istraga o visokotehnološkom kriminalu, paralelna finansijska istraga i istraga o pranju novca⁴⁵. Varšavska konvencija i Budimpeštanska konvencija Saveta Evrope su važni instrumenti koji se bave ovim aspektima.

Ovaj osnovni kurs predstavlja ključne aspekte međunarodne saradnje, kao što su prednosti kombinovanja različitih vidova međunarodne saradnje na polju visokotehnološkog kriminala i elektronskih dokaza, kao i finansijska istraga i sprečavanje i istraga pranja novca, praveći razliku između međunarodne saradnje na polju razmene (operativnih) informacija i međunarodne pravne pomoći u svrhu prikupljanja dokaza, relevantne međunarodne mreže i organizacije za razmenu informacija, odgovarajuće odredbe Budimpeštanske i Varšavske konvencije, itd.

Istovremeno, postoji nekoliko izazova vezanih za međunarodnu saradnju, a naročito za međunarodnu pravnu pomoć, koje je potrebno razmotriti.

Budimpeštanska i Varšavska konvencija uvode različite načine međunarodne saradnje koje treba primeniti pri kombinovanju paralelnih istraga- istrage o (visokotehnološkom) kriminalu i finansijske istrage. Međutim, međunarodna saradnja se suočava sa konkretnim pravnim i praktičnim izazovima koji se odnose na svaki od ovih ugovora kao rezultat realnih okolnosti, kao što su priroda elektronskih dokaza, klauz tehnologija, ali i identifikacija imovinske koristi stečene krivičnim delima izvršenim putem interneta, privremeno i trajno oduzimanje imovine u inostranstvu, uzimajući u obzir različite režime oduzimanja i pravne razlike između strana. Odgovarajuća tela Saveta Evrope, kao što su Komitet eksperata za primenu evropskih konvencija o saradnji u krivičnim stvarima (PC-OC) i Komitet Konvencije o visokotehnološkom kriminalu (T-CY), definisala su ove izazove i započela njihovo rešavanje.

Prilikom kombinovanja aspekata istrage o visokotehnološkom kriminalu, finansijske istrage i sprečavanja i istrage pranja novca, korisno je biti svestan svih ovih različitih aspekata, prednosti i postojećih izazova vezanih za različite vidove saradnje koje nude Budimpeštanska i Varšavska konvencija.

Iako se međunarodna pravna pomoć još uvek smatra osnovnim sredstvom za izvršavanje sudskih naloga i prikupljanje dokaza u inostranstvu, dužina procedure predstavlja veliku prepreku. Međutim, saradnjom kroz zajedničke istrage i zajedničke istražne timove moguće je otpočeti sa rešavanjem nekih od ovih izazova kada je reč o efikasnosti. Saradnja između snaga reda (policija i tužilaštvo) i razmena informacija ne mogu se zaobići u prekograničnim predmetima. Odgovarajuće međunarodne mreže i organizacije igraju važnu ulogu u ovom pogledu, a takođe pomažu i u izgradnji poverenja. Kanali

⁴⁵ Međutim, treba uočiti da uprkos mogućim efikasnim instrumentima za sprečavanje i suzbijanje pranja novca u nekoliko zemalja, krivično gonjenje dela pranja novca još uvek predstavlja izazov.

saradnje i instrumenti koje oni nude od suštinske su važnosti za razmenu informacija i dokaza u krivičnim istragama.

4.1.1 Odgovarajuće mreže i organizacije za razmenu informacija i međunarodnu pravnu pomoć

Međunarodna saradnja- razmena (operativnih) informacija Policija policiji, tužilac tužiocu	
Mreža 24/7	Mreža (kontakt tačke u policiji i/ili tužilaštvu) Član 35 Budimpeštanske konvencije
EGMONT grupa	Mreža finansijsko-obaveštajnih službi (FOS) – sprečavanje pranja novca, privremeno obustavljanje sumnjivih transakcija. Član 46 Varšavske konvencije
Mreža CARIN	Kamdenska međuagencijska mreža za oduzimanje imovinske koristi (Camden Asset Recovery Inter-Agency Network) Mreža stručnjaka za oduzimanje imovinske koristi
INTERPOL	Kanal za razmenu informacija i prenos zahteva za međunarodnu pravnu pomoć
Europol (EC3)	EU i relevantni sporazumi sa zemljama koje nisu članice EU
Eurojust	Evropska pravosudna mreža za visokotehnološki kriminal (2016) EU i relevantni sporazumi sa zemljama koje nisu članice EU
Međunarodna saradnja – međunarodna pravna pomoć (MPP) Zvanična saradnja- dokazi	
MPP: zvanična saradnja, rezultat zahteva za MPP može se koristiti kao dokaz na sudu. Uobičajeni kanali komunikacije idu preko naznačenih centralnih organa, često ministarstava pravde ili ministarstva inostranih poslova.	
Direktna saradnja: sudija sudiji, tužilac tužiocu (EU, bilateralni sporazumi); Varšavska (član 34) i Budimpeštanska (član 27/9) konvencija takođe predviđaju direktnu saradnju između nadležnih pravosudnih organa i organa tužilaštva u hitnim slučajevima, pri čemu se zvanični zahtev prenosi takođe i preko centralnih organa.	
Ostale opcije	zajednički istražni timovi (ZIT) paralelna istraga prenos sudskog postupka

Kriminalci kriju (ili drže) svoju imovinu u inostranstvu. U istrazi krivičnih dela izvršenih putem interneta od strane međunarodne kriminalne grupe, neophodno je proveriti da li počinioци imaju bilo kakvu imovinu u inostranstvu. U takvim predmetima, saradnja između **policija i tužilaštava** je veoma važna. Osoba za kontakt u policiji strane zemlje može pružiti informaciju o tome koji podaci o imovini mogu da se pribave iz javnih izvora, kroz policijsku saradnju ili zamolnicom. Te informacije mogu znatno olakšati i ubrzati pribavljanje podataka. Takva saradnja je operativna i isključuje izvršavanje sudskih naloga.

Operativni kontakti i saradnja mogu takođe dovesti do obrazovanja zajedničkih istražnih timova, što u principu može doprineti delotvornijem pristupu u pogledu međunarodne pravne pomoći. Takvi kontakti i saradnja mogu dovesti i do dogovora o paralelnim istragama u prekograničnim predmetima gde postoji više počilaca i žrtava.

Međunarodna pravna pomoć je zvanična saradnja i rezultat zahteva za takvom saradnjom se može koristiti kao dokaz na sudu. Uobičajeni kanali komunikacije idu preko naznačenih centralnih organa, često ministarstava pravde. Mogući kanali takođe mogu biti ministarstvo inostranih poslova ili INTERPOL, Europol ili Eurojust u hitnim slučajevima.

U okviru EU, međunarodna pravna pomoć teče direktno preko nadležnih organa (tužilac/sud). Varšavska konvencija (član 34) i Budimpeštanska konvencija (član 27/9) takođe predviđaju takve pristupe u hitnim slučajevima, pri čemu se zvanični zahtevi istovremeno prenose i preko centralnih organa.

4.1.2 Međunarodni pravni instrumenti

Visokotehnološki kriminal	Finansijska istraga
Savet Evrope	
Budimpeštanska konvencija o visokotehnološkom kriminalu i Protokol o ksenofobiji i rasizmu ⁴⁶	Varšavska konvencija o pranju, traženju, zapleni i oduzimanju prihoda stečenih kriminalom i o finansiranju terorizma ⁴⁸
Smernice T-CY ⁴⁷	Strazburška konvencija o pranju, traženju, zapleni i oduzimanju prihoda stečenih kriminalom iz 1990. ⁴⁹
EU	
Direktiva 2013/40/EU Evropskog parlamenta i Saveta od 12. avgusta 2013. o napadima na informacione sisteme i o zameni Okvirne odluke Saveta 2005/222/JHA ⁵⁰	Direktiva 2014/42/EU o zabrani raspolaganja imovinom i privremenom oduzimanju predmeta krivičnih dela u Evropskoj uniji ⁵¹
Direktiva 2016/1148 Evropskog parlamenta i Saveta od jula 2016. godine o bezbednosti mrežnih i informacionih sistema ("NIS")	Zajednička akcija 98/699/JHA o pranju novca, identifikaciji, ulaženju u trag, zabrani raspolaganja imovinom, privremenom i

⁴⁶Convention on Cybercrime, ETS 185, 21.11.2001 and Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (Dodatni protokol uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema), ETS 189, 28.01.2003.

⁴⁷<https://www.coe.int/en/web/cybercrime/guidance-notes>

⁴⁸Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, CETS 198, 16.05.2005.

⁴⁹Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, Strasbourg, ETS 141, 08.11.1990.

⁵⁰Ova Direktiva uvodi nova pravila usaglašavanja inkriminacije i zakonskih kazni za nekoliko krivičnih dela usmerenih protiv informacionih sistema. Ona takođe poziva zemlje EU da koriste iste kontakt tačke koje koriste Savet Evrope i G8, kako bi brzo odreagovale na pretnje koje uključuju naprednu tehnologiju. Dostupno na: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040>

⁵¹Dostupno na: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0042>

direktiva) od 6. jula 2016. ⁵²	trajnom oduzimanju predmeta krivičnog dela i imovinske koristi ⁵³
Zaključci Saveta Evropske unije o unapređenju krivičnog pravnog sistema u sajber prostoru i Zaključci Evropske pravosudne mreže za visokotehnološki kriminal ⁵⁴ , juni 2016.	Okvirna odluka 2001/500/JHA o pranju novca, identifikaciji, ulaženju u trag, zabrani raspolaganja imovinom, privremenom i trajnom oduzimanju predmeta krivičnog dela i imovinske koristi ⁵⁵
	Direktiva kojom se menja i dopunjava Direktiva (EU) 2015/849 o sprečavanju korišćenja finansijskog sistema u svrhu pranja novca ili finansiranja terorizma, i kojom se menja i dopunjava Direktiva 2009/101/EC ⁵⁶
	Okvirna odluka 2005/212/JHA o oduzimanju imovinske koristi, predmeta krivičnog dela i imovine proistekle iz izvršenja krivičnog dela ⁵⁷
	Okvirna odluka 2003/577/JHA o izvršavanju naloga za zamrzavanje imovine ili dokaza u Evropskoj uniji ⁵⁸
	Okvirna odluka 2006/783/JHA o primeni principa uzajamnog priznavanja na naloge za trajno oduzimanje ⁵⁹
	Odluka Saveta 2007/845/JHA koja se odnosi na saradnju između kancelarija država članica za oduzimanje imovine na

⁵² NIS Direktiva se može videti na: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L.2016.194.01.0001.01.ENG>

⁵³ Da bi se unapredila saradnja između država Evropske unije (EU) u borbi protiv organizovanog kriminala, ova zajednička akcija obezbeđuje, u okviru rada Evropske pravosudne mreže, pripremu vodiča o identifikaciji, ulaženju u trag, zabrani raspolaganja imovinom ili privremenom i trajnom oduzimanju predmeta krivičnog dela i imovinske koristi, koji su korisnicima laki za korišćenje. Dostupno na: <http://eur-lex.europa.eu/legal-content/NLN/TXT/?uri=uriserv:l33073>

⁵⁴ Zaključci su usredsređeni na: saradnju sa pružaoциma usluga, koja omogućava brzo otkrivanje podataka; mogli bi se predvideti manje rigorozni pravni postupci za pribavljanje određenih kategorija podataka, naročito podataka vezanih za pretplatnike. Procedure međunarodne pravne pomoći (MPP) vezane za elektronske podatke treba ubrzati i pojednostaviti; obim zahteva za MPP između nadležnih organa treba smanjiti kroz povećanje saradnje sa pružaoциma usluga. Treba efikasno koristiti procedure uzajamnog priznavanja kako bi se obezbedila delotvorna zaštita i pribavljanje elektronskih dokaza. Utvrđivanje povezujućih činilaca za sprovođenje nadležnosti u sajber prostoru, uključujući i u slučajevima gde lokacija podataka (još uvek) nije poznata ili je nestalna. Dostupno na: <http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace/>.

⁵⁵ Council Framework Decision 2001/500/JHA of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (OJ L 182, 5.7.2001, p.1). Dostupno na: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001F0500>

⁵⁶ Ona takođe ima za cilj regulisanje virtuelnih valuta time što obavezuje pružaoce usluga zamene valuta i usluga čuvanja novčanika (custodial wallet providers, prim.prev.) da, između ostalog, sarađuju sa svojom nacionalnom finansijsko-obaveštajnom službom (FOS). Dostupno na: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:0450:FIN%20>

⁵⁷ Council Framework Decision 2005/212/JHA of 24 February 2005 on confiscation of crime-related proceeds, instrumentalities and property (OJ L 68, 15.3.2005, p.49). Dostupno na: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:068:0049:0051:en:PDF>

⁵⁸ Council Framework Decision 2003/755/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence (OJ L 196, 2.8.2003, p.45). Dostupno na: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003F0577>

⁵⁹ Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders (OJ L 328, 24.11.2006, p.59). Dostupno na: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32006F0783>

	polju ulaženja u trag i identifikacije imovinske koristi ili druge imovine proistekle iz izvršenja krivičnog dela- (na osnovu ove odluke je uvedena obaveza osnivanja ARO kancelarije/ kancelarija (Kancelarija za povraćaj imovine) ⁶⁰
	Direktiva 2014/41/EU o evropskom nalogu za istragu u krivičnim stvarima ⁶¹
UN	
Rezolucije o borbi protiv krivičnog dela zloupotrebe informacionih tehnologija (Rezolucije 55/63 i 56/121) ⁶²	Konvencija UN protiv nezakonitog prometa opojnih droga i psihotropnih supstanci iz 1988. ⁶³
Rezolucija Generalne skupštine UN 64/211 (mart 2010) o stvaranju globalne kulture bezbednosti sajber prostora ⁶⁴	Konvencija UN protiv transnacionalnog organizovanog kriminala iz 2000. ⁶⁵
	Konvencija UN protiv korupcije iz 2003. ⁶⁶
Ostalo (regionalni ugovori)	
Konvencija Afričke unije o bezbednosti sajber prostora i zaštiti ličnih podataka ⁶⁷	
Arapska konvencija o borbi protiv krivičnih dela vezanih za informacione tehnologije ⁶⁸	
Sporazum Komonvelta nezavisnih država o saradnji u borbi protiv krivičnih dela vezanih za kompjuterske informacije ⁶⁹	
Sporazum Šangajske organizacije za saradnju na polju međunarodne informacione bezbednosti ⁷⁰	

U okviru EU, princip uzajamnog priznavanja, za razliku od međunarodne pomoći, uveden je 2003. godine za izvršavanje naloga za zabranu raspolaganja imovinom, a 2006. godine za naloge za trajno oduzimanje imovine. Mogućnost odbijanja izvršenja takođe je bila ograničena, uz odstupanja, na principe dvostruke kažnjivosti i dvostruke zabrane

⁶⁰Ovom odlukom se utvrđuju zahtevi za osnivanje nacionalnih ARO kancelarija u zemljama EU. Dostupno na: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007D0845>

⁶¹The European Investigation Order (EIO) Directive uspostavlja sveobuhvatan nov sistem koji omogućava državama EU da pribave dokaze u drugim državama EU u krivičnim predmetima koji uključuju više od jedne zemlje. Dostupno na: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041>

⁶²Dostupno na: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf

⁶³United Nations Convention against Illicit Traffic in Narcotic Drugs and Pshychotropic Substances, Vienna, 19.12.1988. (član 5).

⁶⁴Dostupno na: <https://ccdcoe.org/sites/default/files/documents/UN-091221-CultureOfCSandCI.pdf>

⁶⁵United Nations Convention Against Transnational Organised Crime, New York, 15.11.2000 (članovi 12-14).

⁶⁶United Nations Convention Against Corruption, New York, 31.10.2003 (članovi 31, 54-57).

⁶⁷<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

⁶⁸http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences

⁶⁹http://itlaw.wikia.com/wiki/Agreement_on_Cooperation_Among_the_States_Members_of_the_Commonwealth_of_Independent_States_in_Combating_Offences_Relating_to_Computer_Information

⁷⁰<https://ccdcoe.org/sco.html>

raspolaganja imovinom. EU je učinila dalje korake da bi olakšala saradnju uvođenjem evropskog istražnog naloga.

4.1.3 Odredbe o međunarodnoj saradnji

Međunarodni pravni instrumenti se bave aspektima inkriminacije ponašanja, procesnim (istražnim instrumentima) i međunarodnom saradnjom, uključujući pravnu osnovu za međunarodnu pravnu pomoć (MPP). Varšavska i Budimpeštanska konvencija predviđaju načine saradnje koji se mogu primenjivati i kombinovati kako bi se postigli najefikasniji rezultati prilikom sprovođenja paralelne finansijske istrage i istrage o (visokotehnološkom) kriminalu. Saradnja podleže nacionalnim odredbama uz garanciju odlaganja ili odbijanja zahteva (Varšavska konvencija, Odeljak 5, član 27, i Budimpeštanska konvencija, član 25/4 i 27/4 i 5). Glavne oblasti saradnje su naglašene u daljem tekstu:

Odredbe o međunarodnoj saradnji	
Budimpeštanska konvencija	Varšavska konvencija
Osnovni principi	
<p>(Članovi 23-25)</p> <p>Strane će pružati uzajamnu pomoć u cilju istrage ili sudskog postupka u vezi sa:</p> <ul style="list-style-type: none"> - visokotehnološkim kriminalom (članovi 2-10) - ili radi prikupljanja dokaza u elektronskom obliku o krivičnom delu. 	<p>(Član 15)</p> <p>Strane će međusobno sarađivati u cilju istrage i sudskog postupka, čiji je cilj trajno oduzimanje predmeta krivičnog dela i imovinske dobiti.</p> <p>Zahtev za:</p> <ul style="list-style-type: none"> - trajno oduzimanje određenih predmeta - ili za plaćanje novčanog iznosa koji odgovara vrednosti imovinske dobiti - i za pomoć u istrazi i privremenim merama u cilju trajnog oduzimanja.
Spontano informisanje	
<p>(Član 26)</p> <p>Strana može, u okvirima domaćeg zakona i bez prethodnog zahteva, proslediti drugoj strani informacije pribavljene u okviru sopstvene istrage, kada smatra da bi otkrivanje takvih informacija moglo pomoći strani primaocu da pokrene ili sprovede istragu ili sudski postupak u vezi sa krivičnim delima utvrđenim u skladu sa ovom konvencijom, ili bi moglo da dovede do toga da ta strana uputi zahtev za saradnju u skladu sa ovim poglavljem.</p>	<p>(Član 20)</p> <p>Slična odredba</p>
Privremene mere	

<p align="center">(Članovi 29-30)</p> <p>Hitna zaštita sačuvanih kompjuterskih podataka. Hitno otkrivanje zaštićenih podataka o saobraćaju.</p>	<p align="center">(Članovi 21-22)</p> <p>Zabrana raspolaganja ili privremeno oduzimanje imovine, kako bi se sprečio svaki promet, prenos ili raspolaganje imovinom i spontano pružile sve informacije koje su relevantne za privremene mere.</p>
<p align="center">Pomoć u istrazi</p>	
<p align="center">(Članovi 31-34)</p> <p>Medjunarodna pomoć u pogledu istražnih ovlašćenja:</p> <ul style="list-style-type: none"> - pristup sačuvanim kompjuterskim podacima; - prekogranični pristup sačuvanim kompjuterskim podacima uz saglasnost, ili tamo gde su dostupni javnosti; - prikupljanje podataka o saobraćaju u realnom vremenu; i - presretanje podataka iz sadržaja. 	<p align="center">(Članovi 16-19)</p> <p>Strane će pomoći u identifikaciji i ulaženju u trag predmeta krivičnog dela i imovinske koristi, što podrazumeva obezbeđivanje dokaza o postojanju, lokaciji ili kretanju, prirodi, pravnom statusu ili vrednosti gore navedene imovine. Takva pomoć takođe uključuje zahtev za:</p> <ul style="list-style-type: none"> - informacijama o bankovnim računima; - informacijama o bankarskim transakcijama; i - praćenje bankarskih transakcija.
	<p align="center">Trajno oduzimanje</p>
	<p align="center">(Članovi 23-25)</p> <ul style="list-style-type: none"> - Izvršavanje naloga za trajno oduzimanje; ili - podnošenje zahteva svojim nadležnim organima u cilju pribavljanja naloga za trajno oduzimanje i izvršavanja tog naloga, uključujući zahtev za plaćanje novčanog iznosa koji odgovara vrednosti imovinske koristi, ili trajno oduzimanje određene stavke iz imovine.
	<p align="center">(Član 23/5)</p> <p>Mere koje su ekvivalentne trajnom oduzimanju:</p> <ul style="list-style-type: none"> - sankcije nekrivične prirode (trajno oduzimanje koje nije zasnovano na osuđujućoj presudi); - pravila za podelu imovine (naknada žrtvama, legitimnim vlasnicima).
<p align="center">Mreže saradnje</p>	
<p align="center">Mreža 24/7 (član 35)</p> <p>Svaka strana će odrediti kontaktnu tačku koja je na raspolaganju 24/7, kako bi osigurala pružanje pomoći bez odlaganja u</p>	<p align="center">Saradnja između FOS (članovi 46-47)</p> <p>FOS razmenjuju, spontano ili na zahtev, sve dostupne informacije koje mogu biti</p>

<p>cilju</p> <ul style="list-style-type: none"> - istrage ili sudskog postupka koji se tiču krivičnih dela vezanih za računarske sisteme i podatke, - ili prikupljanja dokaza u elektronskom obliku o krivičnom delu. <p>Takva pomoć uključuje olakšavanje, ili, ukoliko to dozvoljava domaći zakon i praksa, direktno sprovođenje sledećih mera:</p> <ul style="list-style-type: none"> - pružanje tehničkih saveta; - zaštita podataka (član 29 i 30); - prikupljanje dokaza, - pružanje pravnih informacija, - i lociranje osumnjičenih. 	<p>relevantne</p> <ul style="list-style-type: none"> - za obradu ili analizu informacija, ili - za istragu od strane FOS u pogledu finansijskih transakcija vezanih za pranje novca i fizička ili pravna lica o kojima je reč. <p>Ovlašćenje FOS da privremeno obustave sumnjive transakcije.</p>
--	---

PITANJA ZA RAZMIŠLJANJE

1. Koji uslovi moraju biti zadovoljeni pre nego što informacije mogu spontano da se podele sa drugom jurisdikcijom?
2. Koje osnove postoje u vašem nacionalnom zakonodavstvu za odbijanje saradnje na osnovu međunarodnog zahteva za pomoć?
3. Koji uslovi moraju biti ispunjeni kako bi se pribavio nalog za ubrzavanje otkrivanja zaštićenih podataka o saobraćaju?
4. Koje praktične mere postoje kako bi se obezbedilo upravljanje, raspolaganje i podela trajno oduzete imovine sa drugom jurisdikcijom? Da li takvi dogovori moraju da se sklapaju od slučaju do slučaja?

4.2 Ocene primene odredbi o međunarodnoj saradnji

Važno je uvideti i razumeti mogućnosti i prepreke na putu međunarodne saradnje u oblasti finansijske istrage i istrage o visokotehnološkom kriminalu i elektronskim dokazima, kako ih definišu međunarodne organizacije.

4.2.1 Ocena vezana za pronalaženje i oduzimanje imovinske koristi

GENVAL

U EU⁷¹, u kontekstu pete runde uzajamnih evaluacija „finansijskog kriminala i finansijskih istraga“, Radna grupa za opšta pitanja uključujući evaluaciju (GENVAL) je u svom završnom izveštaju⁷² iz 2012. godine naglasila ključne izazove koji se odnose na ovu oblast, i to:

⁷¹Vidi takođe: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/financial-investigation/index_en.htm

⁷² EU GENVAL 2012 Final report on fifth round of mutual evaluation – “Financial crime and financial investigations” (Konačni izveštaj EU GENVAL o petoj rundi uzajamne evaluacije- Finansijski kriminal i finansijske istrage” iz 2012. godine. Dostupno na: <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012657%202012%20REV%202>

1. upravljanje predmetom (uključujući upravljanje vremenom i resursima) i saradnja između nadležnih organa, kako na nacionalnom, tako i na međunarodnom nivou,
2. komplikovana i različita pravna pravila i tradicije, na nacionalnom nivou i na nivou EU, zajedno sa ponekad slabom implementacijom,
3. dokazi i pitanje elektronskih podataka, i
4. vreme; finansijske istrage često oduzimaju mnogo vremena i mogu zahtevati velike resurse, u pogledu vremena, ljudstva i finansijskih sredstava.

Ovaj izveštaj takođe sadrži nekoliko preporuka državama članicama i EU, koje mogu biti relevantne za bilo koju jurisdikciju:

- Finansijska istraga treba da se sprovodi u svim predmetima koji se odnose na teška krivična dela i organizovani kriminal (što uključuje terorizam), a ne isključivo u slučaju privrednog i finansijskog kriminala. Stoga treba razraditi sveobuhvatnu politiku u pogledu finansijskog kriminala i finansijskih istraga, koja bi pokrivala sve relevantne organe, uključujući i tužilaštvo, i koja bi imala za cilj ubrzavanje složenih i dugačkih istraga na polju finansijskog kriminala. Ona treba da odražava odgovarajuće prioritete dogovorene na nivou EU i da postavi temelje proaktivnih istraga. Treba posvetiti više pažnje potencijalnoj koristi od međunarodne saradnje, naročito na nivou EU.
- Politika koja se odnosi na finansijski kriminal i finansijske istrage treba da se odražava u dugoročnoj nacionalnoj strategiji. Kad god je to moguće, koncept policijskog delovanja na polju finansijskog kriminala, vođenog obaveštajnim podacima, treba da bude uključen u tu strategiju, kako bi se omogućilo postojanje proaktivnih mera policijskog rada na osnovu rezultata analize. Ovu strategiju treba kombinovati sa redovnim razmatranjem i metodologijom evaluacije, kao i propisnim mehanizmom izveštavanja za tela o kojima je reč. U postavljanju takve strategije, treba razmotriti određene osnovne kriterijume, pravila i smernice, kako bi se pojasnila raspodela zadataka između različitih organa sa selektivnim nadležnostima, kao i uključivanje ključnih prioriteta, kao što su međunarodni predmeti koji se odnose na teška krivična dela. Prema tome, ovu strategiju treba da podrži propisno upravljanje u okviru policije, kako bi se unapredio proaktivni pristup vođen obaveštajnim podacima.
- Države članice treba da primenjuju sve zakone EU vezane za uzajamno priznavanje i pravosudnu saradnju u krivičnim stvarima. Takođe, države članice i odgovarajuća tela EU treba da razmatraju primenu relevantnih okvirnih odluka i primenu mehanizama međunarodne pravne pomoći. Na taj način, države članice treba da prepoznaju i da se uhvate u koštac sa preprekama na putu efikasne proaktivne razmene podataka sa stranim organima reda, telima EU i drugim relevantnim akterima. Treba pojačati spontanu razmenu informacija u skladu sa Odlukom Saveta 2007/845/JHA od 6. decembra 2007. godine, koja se odnosi na saradnju između kancelarija država članica za oduzimanje imovine na polju ulaženja u trag i identifikacije imovinske koristi ili druge imovine proistekle iz izvršenja krivičnog dela, i unaprediti primenu Okvirne odluke Saveta 2006/960/JHA od 18. decembra 2006. godine o pojednostavljivanju razmene informacija i obaveštajnih podataka između organa reda država članica EU.

Upitnik PC-OC

Komitet eksperata Saveta Evrope za primenu evropskih konvencija o saradnji u krivičnim stvarima (PC-OC) usredsredio je pažnju na oblast pronalaženja i oduzimanja imovinske koristi 2014. godine. Odgovori na upitnik PC-OC⁷³ pokazali su, između ostalog, da postoje razlike između strana u primeni odredbi Strazburške i Varšavske konvencije, koje su relevantne za međunarodnu saradnju.

Slede neki od aspekata koji su obuhvaćeni upitnikom:

- Države nisu uvek u mogućnosti da osiguraju sprovođenje zahteva utemeljenih na takozvanom sistemu trajnog oduzimanja zasnovanog na vrednosti. Ovaj sistem se u obe konvencije opisuje kao sistem na osnovu koga je moguće sarađivati, pored takozvanog sistema trajnog oduzimanja zasnovanog na predmetu. U oba sistema, neophodna je osuđujuća krivična presuda. U sistemu trajnog oduzimanja zasnovanog na vrednosti, izračunava se imovinska korist. Na kraju, na osnovu ovih obračuna, sudija nameće obavezu plaćanja novčanog iznosa koji je ekvivalentan pribavljenoj imovinskoj koristi. Nalog za trajno oduzimanje se onda može izvršiti nad svom imovinom koja pripada osuđenom licu. U tom pogledu, ne zahteva se dokaz da je ta imovina direktno stečena izvršenjem krivičnog dela.
- Nekoliko država priznaje mogućnost privremenog i trajnog oduzimanja imovine koja pripada *de facto* optuženom/osuđenom licu, ali se zakonski smatra da pripada trećem licu, uglavnom takozvanom fiktivnom vlasniku.
- Samo pojedine države su u poziciji da pružaju međunarodnu pravnu pomoć u svrhu ili vezano za trajno oduzimanje koje se ne zasniva na osuđujućoj presudi, kao i druge mere (na primer građansko-pravno oduzimanje). Ovo uključuje fazu prikupljanja informacija, u toku koje se često zahtevaju krivične informacije radi korišćenja u okviru postupka, traženja i privremenog i trajnog oduzimanja imovinske koristi, koji se ne zasnivaju na osuđujućoj presudi.
- Pojedine države su u poziciji da pružaju pomoć u krivičnim, građanskim i upravnim postupcima vezanim za odgovornost pravnih lica u svrhu privremenog ili trajnog oduzimanja imovinske koristi.
- Samo pojedine države su u poziciji da pruže pomoć u postupcima vezanim za virtuelne valute kao što su bitcoini, naročito kada je reč o privremenom i trajnom oduzimanju.

MONEYVAL

Komitet eksperata Saveta Evrope za evaluaciju mera za borbu protiv pranja novca i finansiranja terorizma - MONEYVAL⁷⁴ je stalno nadzorno telo Saveta Evrope, kome je poveren zadatak da ocenjuje poštovanje ključnih međunarodnih standarda za borbu protiv pranja novca i finansiranja terorizma, i delotvornost njihove primene, kao i zadatak davanja preporuka nacionalnim organima u pogledu neophodnog poboljšanja njihovih sistema.

⁷³Upitnik o korišćenju i efikasnosti instrumenata Saveta Evrope kada je reč o međunarodnoj saradnji na polju privremenog i trajnog oduzimanja imovinske koristi, uključujući upravljanje trajno oduzetom imovinom i podelu imovine, PC-OC Mod (2015) 06Rev4, 19.5.2016. Dostupno na: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680666607>

⁷⁴Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL): http://www.coe.int/t/dqhl/monitoring/moneyval/default_en.asp?expandable=0

Kroz dinamični proces uzajamnih evaluacija, ocena stručnjaka iz iste oblasti i redovnog praćenja njegovih izveštaja, MONEYVAL ima za cilj da unapredi kapacitete nacionalnih organa kako bi se efikasnije borili protiv pranja novca i finansiranja terorizma.

Izveštaji o evaluacijama se objavljuju na internetu.⁷⁵

4.2.2 Ocena povezana sa visokotehnološkim kriminalom

4.2.2.1 GENVAL

Sedma runda međusobnih evaluacija u EU je posvećena praktičnoj primeni i delovanju evropskih politika o sprečavanju i borbi protiv visokotehnološkog kriminala. Završeni Izveštaji o evaluaciji su objavljeni i mogli bi poslužiti drugim zemljama da preispitaju svoje zakone, propise i strategiju o visokotehnološkom kriminalu.⁷⁶

U isto vreme, nacrt konačnog izveštaja ukazuje na neke problematične aspekte povezane sa međunarodnom saradnjom, naime prosečno vreme odgovora na zahtev za međunarodnu pravnu pomoć iznosi nekoliko meseci i može varirati zavisno od toga da li se MPP pruža na osnovu međunarodnog sporazuma ili reciprociteta. U ovom drugom slučaju, vreme za odgovor je još duže. Međutim, s obzirom na specifičnosti visokotehnološkog kriminala, "dužina postupka međunarodne pravne pomoći čini formalne kanale za MPP prilično nedelotvornim, sa negativnim posledicama po sprovođenje i uspešnost istraga, pošto su digitalni dokazi nepostojani i sa njima se mora postupati brzo i efikasno, pošto odlaganja mogu za rezultat imati gubitak podataka. Shodno tome, postoji generalna potreba da se ubrza postupanje sa zahtevima za MPP u istragama visokotehnološkog kriminala". U nacrtu izveštaja se takođe napominje da treba naći međunarodna rešenja za unapređenje postupaka međunarodne pravne pomoći sa trećim zemljama, na primer korišćenje obrasca zahteva za nalog za ubranu dostavu (podataka) sa kojim su se saglasile vlasti koje ga izvršavaju u datoj državi je pomenuto kao najbolja praksa koja je identifikovana u jednoj državi članici. U istom tonu, na razvoj neformalnih i ličnih kontakata sa nadležnim organima trećih zemalja pre slanja zahteva za MPP je ukazano kao na korisnu praksu koja bi mogla dovesti do bolje i brže saradnje u izvršenju formalnih zahteva.⁷⁷

Države članice su predložile sledeće preporuke:

- Države članice treba da unaprede kvalitet zahteva za MPP koje upućuju drugim zemljama, pogotovo da obezbede da su dovoljno kompletni i da ispituju načine za ubrzavanje i poboljšanje kvaliteta odgovora na zahteve za MPP.
- Državama članicama se preporučuje da poboljšaju delotvornost procesa komunikacije sa drugim državama članicama i trećim zemljama uspostavljanjem sistema registracije MPP i upravljanja MPP koji omogućava da se predmet prati od registracije do trenutka kada odgovor bude poslat državi molilji.
- Države članice se podstiču da češće koriste alate Eurojust-a, EJN-a i Europol-a i da razviju neformalne kontakte sa nadležnim stranim organima kako bi dobile brže odgovore na zahteve za MPP od trećih zemalja.

⁷⁵ Vidi: <http://www.coe.int/en/web/moneyval/jurisdictions>

⁷⁶ Usvojeni izveštaji se mogu naći na: <http://www.coe.int/da/web/octopus/blog/-/blogs/genval-evaluation-reports-on-cybercrime>

⁷⁷ Draft Final report of the seventh round of mutual evaluations on "The practical implementation an operation of the European policies on prevention and combating cybercrime", June 2017. Vidi str. 82-88. Dostupno na: <http://data.consilium.europa.eu/doc/document/ST-9986-2017-INIT/en/pdf>

- EU treba da razmotri mere za koordinaciju kako bi se uspostavio delotvoran način komunikacije i izvršenja zahteva za MPP od strane njenih država članica ka zemljama koje nisu članice EU, ili uspostavio okvir za direktnu saradnju sa relevantnim internet provajderima van EU.
- EU treba da radi na rešenjima za unapređenje i ubrzanje procesa komunikacije između država članica i trećih zemalja, naročito Sjedinjenih Država, posebno u pogledu razmene operativnih podataka i zahteva za MPP i njihovo izvršenje.

4.2.2.2 T-CY

Komitet Konvencije o visokotehnološkom kriminalu Saveta Evrope (T-CY) prati primenu Budimpeštanske konvencije o visokotehnološkom kriminalu i formuliše dodatne standarde i smernice čiji je cilj olakšavanje efektivnog korišćenja i primene Budimpeštanske konvencije, takođe u svetlu razvoja zakona, politika i tehnologije.

4.2.2.2.1 Međunarodna pravna pomoć

Međunarodna pravna pomoć je i dalje glavni način pribavljanja dokaza iz stranih jurisdikcija za korišćenje u krivičnom postupku. U decembru 2014. godine, T-CY je uradio procenu funkcionisanja odredbi o međusobnoj pravnoj pomoći te konvencije.⁷⁸ U njoj se zaključuje, između ostalog, da se postupak međunarodne pravne pomoći (MPP) generalno smatra neefikasnim, a posebno kada se radi o pribavljanju elektronskih dokaza. Vreme odgovora na zahteve od šest do 24 meseca je izgleda norma. Od mnogih zahteva, a tim i istraga, se odustaje. To negativno utiče na pozitivne obaveze vlada da štite društvo i pojedince od visokotehnološkog kriminala i drugih krivičnih dela koja uključuju elektronske dokaze.

Izveštaj o proceni dalje zaključuje da ne postoji jednako česta ili hitna potreba za svim vrstama podataka: u smislu vrste podataka koja se zahteva, podaci o pretplatnicima su izdvojeni kao najčešće tražene informacije. Veliki broj zahteva za takvim informacijama veoma opterećuje organe nadležne za obradu i izvršenje zahteva za MPP i usporava – i često sprečava – krivične istrage. Ovo sugerise da bi rešenja problema podataka o pretplatnicima učinilo međunarodnu pravnu pomoć efikasnijom.

T-CY izveštaj je identifikovao sledeće probleme na koje se nailazi:

- Vreme, količina posla i kompleksnost postupka potrebni da bi se pripremio ili izvršio zahtev za MPP
- Kašnjenja (6 – 24 meseca) u odgovorima na zahteve generalno ili u vezi sa konkretnim zemljama
- Kašnjenja u dostavljanju podataka o pretplatnicima
- Odbijanje saradnje za „lakša“ dela od strane nekih zemalja
- Odbijanje saradnje ili neodgovaranje nekih zemalja na zahtev
- Problem saradnje sa kontakt tačkama raspoloživim non-stop (24/7)
- Nema potvrde da je zahtev za MPP primljen ili da su podaci zaštićeni
- Nejasni kriterijumi za „hitne“ zahteve
- Problem jezika, kvaliteta prevoda, terminologije koja se koristi
- Primljeni zahtevi preširoki, traži se velika količina podataka
- Neusklađenosti između sistema, kao što su istražna ovlašćenja
- Zakonska ograničenja (zaštita podataka)

⁷⁸ T-CY(2013)17rev, 3 December 2014, T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime . Dostupno na: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>

- Odbijane saradnje strane države bez zahteva za MPP. Međutim, zahtev za MPP iziskuje dovoljno informacija i dokaza koji ne mogu biti prikupljeni bez saradnje strane države (začarani krug)
- Zahtev možda ne ispunjava zakonski prag ili formalne uslove zamoljene države ili zahtev nije kompletan ili je traženi prag/standard suviše visok
- Neadekvatnost zakona
- Uslov dvostruke kažnjivosti nije ispunjen
- Zahtevu za MPP nije prethodio zahtev za zaštitu podatka kako bi se obezbedilo da su podaci i dalje raspoloživi
- Podaci nisu zaštićeni u stranoj državi uprkos zahtevu za zaštitu
- Podaci više nisu raspoloživi u stranoj ili u sopstvenoj državi
- Različite politike provajdera za stavljanje podataka na raspolaganje
- Osoba za kontakt u hitnim slučajevima ili nadležni organ u stranoj državi nepoznati
- Teško je utvrditi organ koji je nadležan npr. pružaoca *web hosting* usluga
- Preopterećenost prevelikim brojem zahteva
- Ograničene tehničke veštine i razumevanje u vezi sa elektronskim dokazima u zamoljenoj državi.
- Ograničena ovlašćenja pravosudne policije
- „Osnovana sumnja“ kao prag.

T-CY je usvojio set preporuka kako bi postupak međunarodne pravne pomoći u vezi sa visokotehnološkim kriminalom i elektronskim dokazima bio efikasniji putem delotvornijeg korišćenja postojećih odredbi Budimpeštanske konvencije o visokotehnološkom kriminalu i drugih sporazuma, ali takođe i nuđenjem dodatnih rešenja ⁷⁹, kao što su:

- Strane ugovornice treba u potpunosti da primenjuju ovlašćenja za zaštitu [kompjuterskih] podataka iz Budimpeštanske konvencije (Pr. 1.), prate delotvornost postupka MPP (Pr. 2.), rasporede više bolje obučanih službenika i više resursa za MPP (Pr. 3. i 4.), jačaju ulogu i kapacitete kontakt tačaka raspoloživih non-stop (24/7) (Pr. 5.), utvrde postupke za hitne situacije (Pr. 8.), i tako dalje.
- Strane ugovornice treba da razmotre – moguće kroz Protokol uz Budimpeštansku konvenciju – omogućavanje ubrzanog otkrivanja podataka o pretplatnicima (Pr. 19.), mogućnost međunarodnih naloga za predaju podataka (Pr. 20.), direktnu saradnju između pravosudnih organa (Pr. 21.), praksu direktnog pribavljanja informacija od stranih pružalaca usluga (Pr. 22.), zajedničke istrage i/ili zajedničke istražne timove strana ugovornica (Pr. 23.), dozvoljavanje da se zahtevi šalju na engleskom jeziku (Pr. 24.).

4.2.2.2.2 Dodatni izazovi u praksi

Neki dodatni izazovi i aspekti, takođe povezani sa međunarodnom saradnjom, će biti dalje razrađeni:

Uslovi za pristup podacima o sadržaju sa trenutno aktivnog kompjutera osumnjičenog, čak i ako se podaci čuvaju u inostranstvu, i povezana pitanja pristanka i nadležnosti

U poslednjem izveštaju Grupe za dokaze u klauđu T-CY (CEG) o pristupu krivičnog pravosuđa elektronskim dokazima koji se drže u klauđu: Preporuke za razmatranje od

⁷⁹ Vidi str. 125-127 i T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime.

strane T-CY⁸⁰ navedeno je da po pravilu, ovlašćenja organa zaduženih za sprovođenje zakona su obično određena teritorijalnim principom. Prema ovom principu, nijedna država ne može sprovoditi svoju nadležnost na teritoriji neke druge suverene države. Pristup krivičnog pravosuđa podacima na serverima ili generalno kompjuterskim sistemima koji se nalaze u drugim jurisdikcijama bez uključivanja vlasti tih jurisdikcija izaziva zabrinutost.

Međutim, u situacijama kada je kompjuter koji je na mestu izvršenja krivičnog dela ili je od nekog lica koje je pod istragom aktivan (to jest, trenutno u funkciji), organi krivičnog pravosuđa bi tehnički mogli da pristupe podacima uključujući one koji se čuvaju na serverima u kladu) bez znanja jurisdikcije u kojoj se nalazi server i gde se podaci čuvaju. Član 32(b) Budimpeštanske konvencije nudi rešenje samo za veoma ograničen broj situacija kako je opisano u Smernici koju je T-CY usvojio u decembru 2014. godine.⁸¹

Zbog ograničenja člana 32, tačka b) Budimpeštanske konvencije (dobrovoljni pristanak osumnjičenog da se pristupi podacima iz naloga elektronske pošte tokom aktivne istrage) neke države u praksi primenjuju unilateralna rešenja. Čini se da je široko rasprostranjena praksa da organi za sprovođenje zakona u konkretnoj krivičnoj istrazi pristupaju podacima ne samo na uređaju osumnjičenog već i na povezanim uređajima kao što su nalozi elektronske pošte ili drugih usluga u kladu ako je uređaj otvoren ili ako su podaci za pristup zakonito pribavljeni čak i ako znaju da se povezuju sa nekom drugom, poznatom zemljom.

CEG je proučila doktrinu dalekosežnosti antimonopolskog prava EU (Predmeti *ICI* 48/69; *Woodpulp* 89/85) i primetila da Evropska komisija preporučuje da organi za zaštitu konkurencije pristupaju serverima bilo gde u svetu da bi prikupili dokaze u antimonopolskim postupcima. Da bi imali efektivna ovlašćenja za prikupljanje elektronskih dokaza, važno je da organi u vršenju svojih inspekcijских ovlašćenja budu u stanju da prikupljaju digitalne informacije koje su dostupne preduzeću ili licu čije prostorije su predmet inspekcije bez obzira na to gde se čuvaju, uključujući na serverima i drugim medijima za čuvanje podataka se nalaze van teritorije odnosno organa za zaštitu konkurencije ili van Evropske unije. Uslove i zaštitne mere za takav pristup podacima treba definisati protokolom.

CEG je zaključila da će biti potrebno da se okvirom prekograničnog pristupa definišu uslovi i zaštitne mere za takav pristup podacima kako bi se zaštitila prava pojedinaca i sprečilo zadiranje u ovlašćenja i prava drugih vlada ili njihovih podanika.

Pristup podacima o pretplatnicima

Podaci o pretplatnicima su manje osetljivi u pogledu privatnosti i najčešće potraživani. Policijski ili tužilački nalog za predaju podataka može biti dovoljan u mnogim državama, međutim neke od njih zahtevaju sudski nalog u slučaju dinamičke IP adrese, pošto su time obuhvaćeni i neki podaci o saobraćaju.

Konačni izveštaj CEG o pristupu krivičnog pravosuđa elektronskim dokazima koji se drže u kladu stoga preporučuje:

- Pošto su podaci o pretplatnicima manje osetljivi u pogledu privatnosti nego podaci o saobraćaju i podaci iz sadržaja, uslovi za naloge za predaju za

⁸⁰ T-CY (2016)5, 16. septembar 2016, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY. Dostupno na: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>

⁸¹ T-CY Guidance Note # 3 on Transborder access (Smernica T-CY br. 3 o prekograničnom pristupu) (član 32), 3. decembar 2014., Dostupno na: <https://rm.coe.int/16802e726a>

podatke o pretplatnicima treba da budu predmet blažih zaštitnih mera nego druge vrste podataka ili druge vrste intruzivnih ovlašćenja.

- Lakši režim za predaju podataka o pretplatnicima će olakšati domaće istrage i međunarodnu saradnju u kontekstu klauda.

Ispitani su uslovi korišćenja domaćeg naloga za predaju (član 18. Budimpeštanske konvencije) za podatke o pretplatnicima u slučaju multinacionalnih pružalaca usluga, koji pružaju usluge na teritoriji neke države, bez obzira na sedište u inostranstvu i lokaciju podataka.

Organ krivičnog pravosuđa može ili da utvrdi nadležnost za sprovođenje zakona fokusirajući se na lokaciju kompjuterskog sistema ili uređaja za čuvanje podataka (to je pokriveno odredbama za pretraživanje i zaplenu iz člana 19. Budimpeštanske konvencije) ili fizičkog ili pravnog lica (uključujući pružaoce usluga) koji poseduje ili kontroliše podatke koji se potražuju.⁸² Ovo drugo je pokriveno članom 18. o nalogima za predaju.

Međunarodna pravna pomoć pretpostavlja da je lokacija podataka koji se potražuju poznata i da je stoga moguće znati kojoj državi i kom nadležnom organu se upućuje zahtev za međunarodnu pravnu pomoć. Međutim, često nije očigledno organima krivičnog pravosuđa u kojoj jurisdikciji se podaci čuvaju i/ili koji pravni režim se primenjuje na podatke. Pružalac usluga može imati sedište u jednoj jurisdikciji a primenjivati pravni režim druge jurisdikcije dok se podaci čuvaju u trećoj jurisdikciji. Podaci mogu biti preslikani u nekoliko jurisdikcija ili se kretati između njih. Ako lokacija podataka određuje nadležnost, lako je zamisliti da pružalac usluga klauda sistematično seli podatke da bi sprečio pristup krivičnog pravosuđa.

Pošto Internet nema granice kao takve, podatke o pretplatnicima potrebne u istrazi može držati pružalac usluga „koji pruža usluge na teritoriji“ strane ugovornice iako se sam provajder može nalaziti i informacije koje se potražuju mogu čuvati na serverima u drugim jurisdikcijama.

CEG smatra da logično tumačenje člana 18, stav 1, tačka b) Budimpeštanske konvencije nudi rešenje. Nadležni organi strane ugovornice treba da budu u mogućnosti da traže podatke o pretplatnicima od provajdera koji pruža usluge na njenoj teritoriji bez obzira na to gde se informacije čuvaju i gde se nalazi provajder. Smernica br. 10 o Nalogima za predaju podataka o pretplatnicima⁸³ koju je usvojio T-CY se zalaže za takvo tumačenje i primenu člana 18. Budimpeštanske konvencije. Takvom primenom se efektivno izbegava zahtev za međunarodnu pravnu pomoć.

U Smernici se podvlači da se nalog iz člana 18, stav 1, tačka b) može primeniti u konkretnim slučajevima u pogledu konkretnih pretplatnika, ako pružalac usluga poseduje ili kontroliše podatke o pretplatnicima i ako pružalac usluga „svoje usluge pruža na teritoriji strane ugovornice“, to jest, kada:

- pružalac usluga omogućuje licima na teritoriji strane ugovornice da se pretplate na njegove usluge (i, na primer, ne blokira pristup takvim uslugama); i

⁸² Vidi na primer, European Union Directive 2016/1148 on the security of network and information systems ("NIS Directive") of 6 July 2016, Član 18 Nadležnost i teritorijalnost.

⁸³ Guidance Note #10: Production orders for subscriber information (Article 18 Budapest Convention) (smernica broj 10: Nalozi za predaju podataka o pretplatnicima (Član 18 Budimpeštanske konvencije), koju je T-CY usvojio pisanom procedurom 28. februara 2017. Dostupno na: <https://rm.coe.int/doc/09000016806f943e>

- orijentiše svoje aktivnosti prema pretplatnicima (na primer, obezbeđujući lokalno reklamiranje ili reklamiranje na jeziku teritorije te strane ugovornice), ili koristi podatke o pretplatnicima (ili povezanim podacima o saobraćaju) tokom svojih aktivnosti, ili stupa u interakciju sa pretplatnicima u strani ugovornici, i
- podaci o pretplatnicima koji treba da se predaju su povezani sa uslugama pružaoca koje se pružaju na teritoriji strane ugovornice.

Takođe, odluka Vrhovnog suda Belgije je potvrdila takvo tumačenje presudom da pružalac usluga koji posluje na teritoriji neke države podleže i obavezan je važećim nacionalnim zakonima i propisima. Vrhovni sud Belgije u predmetu *Yahoo!*⁸⁴ je presudio da nalog za predaju podataka o pretplatnicima provajderu koji nudi usluge i time je „prisutan“ na teritoriji strane ugovornice predstavlja domaći nalog (kao u članu 18, stav 1, tačka b)) i nije predmet međunarodne saradnje ili vršenja ekstra-teritorijalne nadležnosti. *Yahoo! Inc.* se žalio na raniju odluku Apelacionog suda Antverpena od 20. novembra 2013. godine, između ostalog, iz razloga što prema međunarodnom običajnom pravu, država nema ekstrateritorijalnu nadležnost za prinudno sprovođenje.

Belgijski Vrhovni sude je presudio sledeće:

- generalno, država može sprovoditi prinudne mere samo na svojoj teritoriji a inače bi izvršila povredu suverenosti druge države.
- „Država uvodi prinudne mere na svojoj teritoriji u meri u kojoj postoji dovoljna teritorijalna povezanost između te mere i te teritorije.“
- Članom 46bis §2 belgijskih Pravila krivičnog postupka „samo se namerava operaterima i pružaocima usluga aktivnim u Belgiji nametnuti mera sa ciljem pribavljanja samo identifikacionih podataka povodom krivičnog dela ili prestupa čija istraga spada u nadležnost belgijskih tužilaštava. Ova mera ne zahteva prisustvo belgijske policije ili vršilaca pravosudne funkcije, niti agenata koji nastupaju u njihovo ime u inostranstvu. Ova mera ne zahteva nikakvu materijalnu radnju ili akt u inostranstvu. Ova mera stoga ima ograničen obim i posledicu, a njeno izvršenje ne zahteva nikakvu intervenciju van teritorije Belgije “.
- *Yahoo! Inc.*, „kao pružalac usluge besplatnog vebmejla, jeste prisutan na belgijskoj teritoriji i dobrovoljno se pridržava zakona Belgije pošto aktivno učestvuje u belgijskom privrednom životu, konkretno koristeći naziv domena 'www.yahoo.be', koristeći lokalni jezik, prikazujući reklame zasnovane na lokaciji korisnika njegovih usluga i njegove dostupnosti tim korisnicima u Belgiji time što je instalirao pretnac za žalbe i pult za često postavljena pitanja.“
- „Javni tužilac ne traži ništa u Sjedinjenim Državama od američkog subjekta, već traži nešto u Belgiji od američkog subjekta koji pruža usluge na belgijskoj teritoriji“.
- Stoga, nije bilo vršenja eksteritorijalne nadležnosti.

Direktna saradnja sa multinacionalnim pružaocima usluga

⁸⁴ Odluka Vrhovnog suda Belgije u predmetu *Yahoo!* od 1. decembra 2015; belgijski Vrhovni sud je doneo konačnu presudu da je *Yahoo! Inc.* registrovan u Kaliforniji, SAD, dužan da preda podatke o pretplatnicima i da to podleže prinudnim merama iz člana 46bis belgijskih Pravila krivičnog postupka Dostupno na holandskom na: http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1

Saradnja sa SAD je od naročite važnosti pošto mnogi multinacionalni pružaoci usluga tamo imaju svoje sedišta i broj zahteva za međunarodnu pravnu pomoć je sve veći. U konačnom izveštaju CEG o pristupu krivičnog pravosuđa elektronskim dokazima koji se drže u kladu ističe da američki pružaoci usluga mogu otkriti podatke o pretplatnicima i podatke o saobraćaju stranim vlastima na osnovu pravnog zahteva i da je to u skladu sa intencijom člana 18, stav 1, tačka b) Budimpeštanske konvencije. Međutim, u njemu se napominje da nestalnost politika provajdera⁸⁵ i nepredvidljivost otkrivanja podataka dovodi do nepredvidljivosti kod organa za sprovođenje zakona kao i kod korisnika i pokreće pitanja povezana sa vladavinom prava.

U slučaju evropskih provajdera takva saradnja nije moguća zbog pravila o zaštiti privatnosti podataka te se mora dostaviti zahtev za MPP.

Američki pružaoci usluga prihvataju zahteve za zaštitu bilo kakvih sačuvanih podataka koji su direktno primljeni od stranih vlasti očekujući da će za njima uslediti zahtev za otkrivanje preko međunarodne pravne pomoći. Evropski provajderi ne prihvataju zahteve za zaštitu podataka koje prime direktno od organa reda u drugim jurisdikcijama.

Hitni postupci

U preporuci 8 iz Izveštaja o proceni međunarodne pravne pomoći T-CY navodi se da se strane ugovornice podstiču da uspostave hitne procedure za zahteve koji su povezani sa rizikom po život i sličnim vanrednim okolnostima. Istraživanje koje je sprovedla CEG⁸⁶ 2016. godine, u kome su učestvovala 33 države, pokazuje sledeće:

- Većina strana ugovornica nema zakone i propise koji dozvoljavaju otkrivanje podataka domaćim organima krivičnog pravosuđa u hitnim situacijama;
- Manje od 20% imaju uspostavljene procedure koje dozvoljavaju domaćim nadležnim organima da hitno otkriju podatke stranim organima;
- Samo dve strane ugovornice su dozvolile pružiocima usluga na svojoj teritoriji da otkriju podatke stranim nadležnim organima u hitnim situacijama.

CEG je predložila da se pitanja iz Preporuke 8 takođe rešavaju putem Protokola uz Budimpeštansku konvenciju.

Dodatni protokol uz Budimpeštansku konvenciju

CEG je preporučila da se započne pregovori o dodatnom Protokolu uz Budimpeštansku konvenciju o visokotehnološkom kriminalu kako bi se omogućila delotvornija međunarodna pravna pomoć, olakšala direktna saradnja sa pružiocima usluga u drugim jurisdikcijama kada je potrebna, kao i definisali i utvrdili uslovi i zaštitne mere u vezi sa postojećom praksom prekograničnog pristupa podacima i definisali zahtevi u pogledu zaštite podataka (o ličnosti).

Protokol uz Budimpeštansku konvenciju bi mogao da:

⁸⁵ Za pregled različitih politika provajdera vidi Criminal justice access to data in the cloud: cooperation with "foreign" service providers, (Pristup krivičnog pravosuđa podacima koji se drže u kladu: saradnja sa „inostranim“ pružiocima usluga), T-CY Cloud Evidence Group, maj 2016. Dostupno na: <https://rm.coe.int/168064b77d>

⁸⁶ Emergency requests for the immediate disclosure of data stored in another jurisdiction through mutual legal assistance channels or through direct requests to service providers, (Hitni zahtevi za neposredno otkrivanje podataka sačuvanih u drugoj jurisdikciji putem kanala međunarodne pravne pomoći ili direktnih zahteva pružiocima usluga), T-CY Cloud Evidence Group, maj 2016. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651a6f>

- pojasni procedure i uslove za direktnu saradnju sa pružaocima usluga u drugim jurisdikcijama, kao i prihvatljivost podataka primljenih u krivičnom postupku;
- uspostavi zakonski osnov za direktne zahteve za zaštitu prema stranim pružaocima usluga. To je već praksa koju prihvataju američki pružaoci usluga;
- predvidi hitne postupke u kojima se dozvoljava direktna saradnja sa pružaocima usluga u stranoj jurisdikciji u posebnim hitnim situacijama.

Mogući elementi Protokola:

- Odredbe za delotvorniju međunarodnu pravnu pomoć:
 - Pojednostavljeni režim za zahteve za međunarodnu pravnu pomoć koji se odnose na podatke o pretplatnicima;
 - međunarodni nalozi za predaju (podataka);
 - direktna saradnja između pravosudnih organa u zahtevima za međunarodnu pravnu pomoć;
 - zajedničke istrage i zajednički istražni timovi;
 - zahtevi na engleskom jeziku;
 - audio/video saslušavanje svedoka, oštećenih i veštaka;
 - hitni postupci međunarodne pravne pomoći.
- Odredbe koje omogućavaju direktnu saradnju sa pružaocima usluga u drugoj jurisdikciji kod zahteva za podatke o pretplatnicima, zahteva za zaštitu (sačuvanih podataka) kao i hitnih zahteva.
- Jasniji okvir i snažnije zaštitne mere za postojeću praksu prekograničnog pristupa podacima.
- Zaštitne mere, uključujući zahteve za zaštitu podataka (o ličnosti).

Projektni zadatak za izradu nacrtu II Dodatnog protokola uz Budimpeštansku konvenciju o visokotehnološkom kriminalu je usvojen na 17. plenarnoj sednici T-CY u junu 2017. godine.⁸⁷

4.3 Korišćenje modeli i obrazaca za međunarodnu pravnu pomoć

Zahtevi za međunarodnu pravnu pomoć se razlikuju, čak i ako su zasnovani na međunarodnim pravnim instrumentima, pošto zavise od nacionalnog zakonodavstva države koja ih upućuje kao i od zakonodavstva i praktičnih očekivanja države koja ih prima. Obrasci zahteva za MPP bi mogli pomoći državama u izvesnoj meri i stoga su uloženi određeni napor da se izrade modeli obrazaca.

PC-OC komitet Saveta Evrope je 2016 godine izradio Model obrasca zahteva za međunarodnu pravnu pomoć u krivičnim stvarima⁸⁸.

⁸⁷ T-CY(2017)3 Terms of Reference for the preparation of a draft 2nd Additional Protocol to the Budapest Convention on Cybercrime (T-CY(2017)3 Projektni zadatak za izradu nacrtu 2. Dodatnog protokola uz Budimpeštansku konvenciju o visokotehnološkom kriminalu), jun 2017. Dostupno na: <https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-protocol/168072362b>

T-CY u svom Izveštaju o proceni godine odredbi o međunarodnoj pravnoj pomoći Budimpeštanske konvencije o visokotehnološkom kriminalu iz 2014. u Preporuci 17 navodi da Savet Evrope treba – u okviru projekata za izgradnju kapaciteta – da izradi ili obezbedi link sa standardizovanim višejezičnim obrascima za zahteve na osnovu člana 31⁸⁹.

Zaključci Saveta EU o unapređenju krivično-pravnog sistema u sajber prostoru (jun 2016.g.) su, između ostalog, pozvali Komisiju da, zajedno sa državama članicama, Eurojust-om i trećim zemljama, da razmotre i sačine preporuke o tome kako da se postojeći standardizovani obrasci i postupci prilagode, gde je to primereno, za zahteve za obezbeđivanje i pribavljanje elektronskih dokaza.

Primer obrasca naloga za trajno oduzimanje može se naći u Okvirnoj odluci Saveta 2006/783/JHA od 6. oktobra 2006. godine o primerni načela međusobnog priznavanja naloga za oduzimanje imovine⁹⁰.

Još jedan primer predstavlja Direktiva 2014/41/EU Evropskog parlamenta i Saveta od 3. aprila 2014. godine u vezi sa evropskim nalogom za istragu u krivičnim stvarima⁹¹.

Konačno, UNODC je izradio Alat za sastavljače zahteva za međunarodnu pravnu pomoć⁹².

Očigledno je da tradicionalni pristupi međunarodnoj pravnoj pomoći više nisu adekvatni u globalnom svetu sa internet kriminalom. Svest o mogućnostima i izazovima u okviru oba instrumenta Saveta Evrope: Budimpeštanska konvencija (npr. pristup podacima u kladu) i Varšavska konvencija (izvršenje naloga za zabranu raspolaganja i oduzimanje imovine) će doprineti boljim rezultatima kada se istraga visokotehnološkog kriminala kombinuje sa paralelnom finansijskom istragom.

⁸⁸ Vidi dokumenta sa 69. sastanka (maj 2016.): Draft model request form on MLA and practical guidelines for practitioners (Nacrt modela obrasca zahteva za MPP i praktične smernice za praktičare) : <http://www.coe.int/en/web/transnational-criminal-justice-pcoc/pc-oc-69th-meeting>
<http://www.coe.int/en/web/transnational-criminal-justice-pcoc/model-request-form-for-mutual-assistance-in-criminal-matters>

⁸⁹ The mutual legal assistance provisions of the Budapest Convention on Cybercrime (Odredbe Budimpeštanske konvencije o međunarodnoj pravnoj pomoći), 3.12.2014. (T-CY(2013)17rev). (<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>)

⁹⁰ <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006F0783&from=EN>

⁹¹ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041>

⁹² <https://www.unodc.org/mla/en/index.html>

5 Virtuelne valute

Kriptovalute, posebno bitcoin, su i dalje valuta izbora u većini dela visokotehnološkog kriminala, bez obzira da li se koriste za plaćanje kriminalnih usluga ili za primanje uplata od žrtava iznude. Ipak, ključni članovi bitcoin zajednice, kao što su menjači, sve više se nalaze u poziciji žrtve sajberkriminalaca⁹³. Posle uvida u virtuelne valute koji je dat na osnovnom kursu, napredni kurs pruža nešto detaljnije informacije o funkcionisanju virtuelnih valuta (naročito bitcoina) i diskusiju o rizicima povezanim sa korišćenjem ovih virtuelnih valuta. Ovaj deo u zaključku predstavlja neke izazove koji se javljaju u istrazi i ograničavanju raspolaganja/oduzimanju imovinske koristi iz iskustava sa virtuelnim valutama.

5.1 Rekapitulacija osnovnog kursa

Na osnovu FATF-ovih definicija⁹⁴, osnovni kurs je definisao sledeće pojmove i kategorije koje se odnose na virtuelne valute:

- Virtuelna valuta
- Elektronski novac/e-novac
- Digitalna valuta
- Konvertibilna u odnosu na nekonvertibilnu virtuelnu valutu
- Centralizovana u odnosu na decentralizovanu virtuelnu valutu

Ovi pojmovi su rekapitulirani u tabeli ispod.

Virtuelna valuta	"Virtuelna valuta je digitalni prikaz vrednosti kojom se može trgovati na internetu i funkcioniše kao (1) sredstvo razmene; i/ili (2) obračunska jedinica; i/ili (3) sredstvo čuvanja vrednosti, ali nema status zakonskog sredstva plaćanja ni u jednoj jurisdikciji"
Elektronski novac/e-novac	"Virtuelna valuta se takođe razlikuje od elektronskog novca, koji je digitalni prikaz dekretne (<i>fiat</i>) valute koji se koristi za elektronski prenos vrednosti denominovane u dekretnoj valuti."
Digitalna valuta	"Digitalna valuta može značiti digitalni prikaz ili virtuelne valute (ne-dekretne) ili elektronskog novca (dekretnog) i stoga se često koristi kao zamena za pojam virtuelna valuta."
Konvertibilna u odnosu na nekonvertibilnu virtuelnu valutu	Konvertibilna (ili otvorena) virtuelna valuta ima ekvivalentnu vrednost u realnoj valuti i može se zameniti za realnu valutu i obratno. Nekonvertibilna (ili zatvorena) virtuelna valuta je namenjena da bude specifična za posebni virtuelni domen ili svet, i prema pravilima kojima se uređuje njeno korišćenje, ne može biti zamenjena za dekretnu valutu.
Centralizovana u odnosu na decentralizovanu virtuelnu valutu	Centralizovane virtuelne valute imaju jedan administrativni organ (administratora) – tj. treće lice koje kontroliše sistem. Administrator izdaje valutu, uspostavlja pravila njenog korišćenja, održava centralnu glavnu knjigu plaćanja i ima ovlašćenje da otkupi valutu (povuče je iz optica). Decentralizovane virtuelne

⁹³ The Internet Organised Crime Threat Assessment (IOCTA) 2016, (Procena pretnji od organizovanog kriminala na internetu) Europol. Dostupno na: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016>

⁹⁴ Izveštaj FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks, (Glavne definicije virtuelnih valuta i potencijalni rizici od pranja novca i finansiranja terorizma), jun 2014. Dostupno na: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

valute su distribuirane, otvorenog izvora na matematički zasnovane *peer-to-peer* (bez posrednika) virtualne valute koje nemaju nikakav centralni administrativni organ i nikakvo centralno praćenje i nadzor.

5.2 Uvod u virtualne valute

5.2.1 Dodatna terminologija o virtualnim valutama⁹⁵

Kriptovaluta	Odnosi se na matematički zasnovanu decentralizovanu virtualnu valutu koja je zaštićena kriptografijom – tj. ona ima ugrađene principe kriptografije radi realizacije distribuirane, decentralizovane bezbedne informacione ekonomije. Kriptovaluta se oslanja na javne i privatne ključeve za vršenje prenosa vrednosti od jednog lica (fizičkog ili pravnog) drugom i mora biti kriptografski potpisana svaki put kada se prenosi. Sigurnost, integritet i bilans u glavnim knjigama kriptovaluta se obezbeđuje pomoću mreže međusobno nepoverljivih strana (kod bitcoina oni se nazivaju rudari) koji štite mrežu u zamenu za priliku da pribave nasumično distribuiranu naknadu (kod bitcoina, jedan mali broj novostvorenih bitcoina, koji se nazivaju „nagrada za blok” i u nekim slučajevima naknade za transakciju koje plaćaju korisnici kao podsticaj rudarima da uključe njihove transakcije u sledeći blok). Definisano je na stotine kriptovaluta, uglavnom izvedenih iz bitcoina, koji koristi sistem dokaza rada (<i>proof of work</i>) za validaciju transakcija i održavanje lanca blokova (<i>blockchain</i>). Dok je bitcoin doneo prvi kompletno implementirani protokol kriptovalute, sve je veće interesovanje za razvoj alternativnih, potencijalno efikasnijih metoda dokaza, kao što su sistemi bazirani na „dokazu uloga” (<i>proof of stake</i>).
Bitcoin	Pokrenut 2009. godine, bio je prva decentralizovana konvertibilna virtualna valuta, kao i prva kriptovaluta. Bitcoini su obračunske jedinice koje se sastoje od jedinstvenih nizova brojeva i slova koji čine jedinice valute i imaju vrednost samo zato što su korisnici spremni da plate za njih. Bitkoinima korisnici digitalno trguju uz visok stepen anonimnosti a mogu se zameniti (kupiti ili unovčiti) za/u američke dolare, evre i druge dekretno i virtualne valute.
Itirijum (Ethereum)	Jedina kriptovaluta (uz izuzetak njegovog 'fork'-a Ethereum Classic) koja obuhvata kompletan programski jezik. To se može koristiti za stvaranje pametnih ugovora – samoizvršnih skriptova, gde se uplata šalje pošto se ispune unapred definisani uslovi.
Altkoin	Odnosi se na matematički zasnovanu decentralizovanu konvertibilnu virtualnu valutu osim bitcoina, koji je prvobitna takva valuta. Primeri obuhvataju <i>Ripple</i> , <i>PeerCoin</i> , <i>Lite-Coin</i> , <i>zerocoin</i> , <i>anoncoin</i> i <i>dogecoin</i> .

⁹⁵ FATF Report, Virtual Currencies Key Definitions and Potential AML/CFT Risks, June 2014. Dostupno na: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

Monero	Stvoren u aprilu 2014.g., je kriptovaluta otvorenog izvora koja navodno obezbeđuje najviši nivo privatnosti pomoću nekoliko tehnologija koje čine tradicionalno praćenje i pronalaženje nedelotvornim pošto su adrese slanja i prijema maskirane. Iznos transakcije je skriven. Karakteristike privatnosti transakcija su obezbeđene kao unapred zadate.
Čvor	Klijent koji upućuje transakcija širom bitcoin mreže ka drugim čvorovima (<i>node</i>).
Privatni ključ	Tajni ključ koji omogućava da se vrše transakcije sa bitcoinom i koristi se za kreiranje potpisa za transakciju koji ne može da se falsifikuje. Vlasnik privatnog ključa kontroliše bitcoine.
Javni ključ	Javno poznat ključ izveden iz privatnog ključa.
Transakcija sa bitcoinom	Bitkoini se premeštaju sa jedne adrese na drugu. Kada vrši transakciju korisnik koristi bitcoin novčanik instaliran na kompjuteru ili na onlajn servisu koji nudi relevantne funkcionalnosti. Transakcija sa bitcoinom je jednokratna transakcija koja se ne može poništiti. Transakcije sa bitcoinom su transparentne i mogu se videti na internetu na razne načine. Podaci koji se mogu videti su bitcoin adresa pošiljaoca, bitcoin adresa primaoca i iznos bitcoina koji je predmet transakcije.
Oduzimanje	Premeštanje bitcoina sa adresa osumnjičenog na adresu koju kontrolišu organi reda.
Anonimizator (alat za anonimizaciju)	Odnosi se na alate i usluge koje su koncipirane tako da prikriju izvor transakcije sa bitcoinom i olakšaju anonimnost.
Mikser (perionica, mešalica)	Je ime za jednu vrstu anonimizatora koji prikriva niz transakcija u lancu blokova povezivanjem svih transakcija na istoj bitcoin adresi i njihovog zajedničkog slanja na način da izgleda da su poslali sa neke druge adrese. Mikser ili mešalica (<i>mixer, tumbler</i>) šalje transakcije preko kompleksne, polu-nasumične serije fiktivnih transakcija koje izuzetno otežavaju povezivanje konkretnih virtuelnih novčića (adresa) sa konkretnom transakcijom. Mikser servisi rade tako što primaju instrukcije od korisnika da pošalju sredstva na određenu bitcoin adresu. Mikser servis zatim „pomeša“ ovu transakciju sa transakcijama drugih korisnika tako da postaje nejasno kome je korisnik nameravao da usmeri sredstva.
Tor (The Onion Router)	Ime dato podzemnoj distribuiranoj mreži kompjutera na Internetu koja prikriva pravu IP adresu i stoga identitete korisnika mreže preusmeravajući komunikaciju preko više kompjutera širom sveta i njihovog 'obmotavanja' u brojne slojeve enkripcije.
Dark novčanik	Ime dato novčaniku zasnovanom na pretraživaču čiji je cilj obezbeđivanja anonimnosti transakcija sa bitcoinom inkorporiranjem sledećih karakteristika: autoanonimizator (mikser), decentralizovana trgovina, platforme za grupno finansiranje (<i>crowd funding</i>) koje se ne mogu cenzurisati, berzanske platforme i crna tržišta informacija i decentralizovane berze slične platformi Silk Road.
Hladno spremište	Odnosi se na oflajn novčanik za bitcoin – tj. novčanik za bitcoin koji nije povezan na Internet. Namena hladnog spremišta (<i>cold storage</i>) je da se pomogne u zaštiti sačuvane virtuelne valute od hakovanja i krađe.
Vruće spremište	Odnosi se na onlajn novčanik za bitcoin, za razliku od hladnog spremišta.

Lokalni sistem za trgovinsku razmenu	jeste lokalno organizovana ekonomska organizacija koja omogućava članovima da razmenjuju robu i usluge sa drugima u toj grupi. LETS (<i>Local Exchange Trading Systems</i>) koriste lokalno kreiranu valutu za denominiranje jedinica vrednosti kojima se može trgovati ili koje se mogu razmeniti za robu i usluge. Teoretski bitkoini bi mogli biti usvojeni kao lokalna valuta koja se koristi u LETS sistemu.
---	---

5.2.2 Učesnici u sistemu virtuelne valute

Menjač (takođe poznat kao berza virtuelnih valuta)	Fizičko ili pravno lice čija je delatnost zamena virtuelne valute za realnu valutu, sredstva ili druge forme virtuelnih valuta, kao i plemenite metale i obratno uz naknadu (proviziju). Menjači generalno prihvataju širok spektar načina plaćanja, uključujući gotovinu, elektronski transfer, kreditne kartice i druge virtuelne valute i mogu biti povezani ili nepovezani sa administratorom ili mogu biti treće lice-provajder. Menjači mogu nastupati kao berza ili menjačnica. Pojedinci tipično koriste menjače za deponovanje i podizanje novca sa računa virtuelnih valuta.
Administrator	Fizičko ili pravno lice čija je delatnost izdavanje (stavljanje u promet) centralizovane virtuelne valute, uspostavljanje pravila za njeno korišćenje, vođenje centralne glavne knjige plaćanja, a koji ima i ovlašćenje da iskupi (povuče iz prometa) virtuelnu valutu.
Korisnik	Fizičko ili pravno lice koje pribavlja virtuelnu valutu i koristi je za kupovinu realne ili virtuelne robe ili usluga ili šalje transfere u ličnom svojstvu drugom licu (za ličnu upotrebu), ili koji drži virtuelnu valutu kao (ličnu) investiciju.
Rudar	Fizičko ili pravno lice koje učestvuje u decentralizovanoj mreži virtuelne valute korišćenjem posebnog softvera za rešavanje kompleksnih algoritama u distribuiranom sistemu dokaza rada (<i>proof-of-work</i>) ili drugom distribuiranom sistemu dokaza koji se koristi da se validiraju transakcije u sistemu virtuelne valute. Rudari mogu biti korisnici ako samostalno generišu konvertibilnu virtuelnu valutu samo za svoje sopstvene potrebe. Rudari mogu takođe učestvovati u sistemu virtuelne valute kao menjači, koji kreiraju virtuelnu valutu kao posao da bi je prodali za dekretnu valutu ili drugu virtuelnu valutu.
Novčanik virtuelne valute (klijent)	Sredstvo (softverska aplikacija ili drugo) za držanje, čuvanje i prenos bitkoina ili druge virtuelne valute.
Pružalac usluge novčanika	Subjekt koji obezbeđuje novčanik za virtuelnu valutu za držanje, čuvanje i prenos bitkoina ili druge virtuelne valute. Novčanik sadrži privatne ključeve korisnika, koji omogućavaju korisniku da potroši virtuelnu valutu koja je raspoređena na adresu virtuelne valute u lancu blokova. Pružalac usluge novčanika olakšava učešće u sistemu virtuelne valute omogućavajući korisnicima, menjačima i trgovcima da lakše obavljaju transakcije sa virtuelnom valutom. Pružalac usluge novčanika vodi bilans virtuelne valute klijenta i generalno takođe pruža bezbednost čuvanja i transakcije.

Mnogi drugi subjekti mogu takođe učestvovati u sistemu virtuelne valute i mogu biti povezani sa menjačima i/ili administratorima ili nezavisni od njih. Oni obuhvataju, između

ostalog, pružaoci usluga administriranja veba (tj. veb administratori), procesori plaćanja-treća lica (koji olakšavaju prihvatanje od strane trgovca), oni koji razvijaju softver ili pružaju aplikacije.

5.2.3 Bitcoin

Bitcoin je decentralizovana, *peer-to-peer* platna mreža koju pokreću njeni korisnici bez centralnog organa ili posrednika. Satoshi Nakamoto je objavio prvu specifikaciju i dokaz koncepta bitcoina na mejling listi za kriptografiju 2009. godine⁹⁶. U osnovi, svrha i funkcionisanje bitcoin mreže su povezani sa upravljanjem i zajedničkim korišćenjem glavne knjige, koja je poznata pod imenom „lanac blokova”. Ova glavna knjiga sadrži svaku transakciju koja je ikad izvršena i koristi se za verifikaciju validnosti svake transakcije⁹⁷. Integritet i hronološki redosled transakcija u glavnoj knjizi se obezbeđuje kriptografijom. Bitkoini su konvertibilna, decentralizovana virtuelna valuta, koja se često naziva i kriptovaluta.

U ovom delu se opisuje kako funkcioniše virtuelna valuta bitcoin.

5.2.3.1 Prenos vrednosti

Najočiglednije pitanje o virtuelnoj valuti je kako korisnici valute vrše prenos vrednosti među sobom. U slučaju bitcoina, svaki korisnik ima jednu ili više bitcoin adresa. Korisnik može da kreira koliko god želi bitcoin adresa, čak i posebnu adresu za svaku pojedinačnu transakciju ako to želi. U praksi, bitcoin softver i servisi predstavljaju bitcoine korisnika onako kako su sačuvani u „novčaniku”. Novčanik može da predstavlja samo jednu bitcoin adresu ili više adresa zavisno od konkretnih karakteristika tog softvera ili servisa. Ta adresa služi kao jedinstvena identifikaciona vrednost koja se koristi da prikaže vlasništvo nad konkretnim bitcoinom⁹⁸. Kad Osoba A želi da pošalje novac Osobi B, ona objavi poruku bitcoin mreži koja sadrži identifikaciju adrese pošiljaoca, identifikaciju adrese primaoca („prijemna adresa”) i iznos transfera u bitcoinima. Svaki čvor u bitcoin mreži koji primi ovu poruku će ažurirati svoju kopiju glavne knjige a zatim proslediti poruku o transakciji drugim čvorovima.

Da bi se napadač, Osoba C, sprečio da objavi poruku kojom bi pokušao da prenese bitcoine iz novčanika Osobe A u novčanik Osobe C, verodostojnost transakcije se obezbeđuje prisustvom digitalnog potpisa Osobe A. da bi se kreirala validna poruka o transakciji kojom se bitkoini prenose iz novčanika Osobe A, osoba koje generiše poruku mora imati lozinku povezanu sa privatnim ključem tog novčanika.

5.2.3.2 Dokazivanje vlasništva

Kako primalac, Osoba B u gornjem primeru, zna da su bitkoini koje prima stvarno pripadali Osobi A? Da bi se konstruisala validna poruka za prenos bitcoina, pošiljalac bitcoina mora da dokaže da je on trenutni vlasnik tih bitcoina.

Pretpostavimo da Osoba A šalje pet bitcoina Osobi B. Osoba A mora u transakciju da uključi reference na prethodne transakcije gde je primalac u transakciji bila Osoba A i ukupnu vrednost prethodnih transakcija koja ja bila veća od pet bitcoina. Ovo se naziva „inputima” transakcije.

⁹⁶ <https://bitcoin.org/en/faq>

⁹⁷ <https://bitcoin.org/en/how-it-works>

⁹⁸ Strogo uzev, svaka adresa je par javnog/privatnog ključa. Javni ključ je „adresa”. Privatni ključ se čuva u tajnosti i koristi za digitalno potpisivanje transakcija koje uključuju tu adresu i tako verifikuje verodostojnost transakcije.

Svi korisnici bitcoin mreže vode primerak glavne knjige („lanac blokova“) koji sadrži istorijat svih prethodnih transakcija. Osoba B onda može da verifikuje da bitcoini iz reference u inputima za transakciju Osobe A zaista pripadaju Osobi A. Da bi se proces pojednostavio, postoji pravilo da transakcije moraju da budu izbalansirane. Drugim rečima, broj bitcoina na „ulazu“ transakcije mora biti jednak broju bitcoina na „izlazu“ transakcije. Ako postoji debalans, Osoba A onda može preostali saldo inputa da prenese sebi.

5.2.3.3 Dvostruko trošenje

U *peer-to-peer* mreži kao što je bitcoin mreža, nema garancije da redosled kojim transakcije prima bilo koji pojedinačni čvor predstavlja isti redosled po kome su kreirane. To praktično uvodi mogućnost da Osoba A kreira poruku o transakciji kojom se bitcoini šalju Osobi B i onda istovremeno da kreira drugu poruku o transakciji da šalje bitcoine nekom drugom. To je poznato pod nazivom dvostruko trošenje. Sasvim je moguće da će neki čvorovi u bitcoin mreži prvo primiti drugu transakciju. Kada bi prva transakcija nešto kasnije stigla do tih čvorova, smatrala bi se nevažećom jer koristi inpute koji su već iskorišćeni, iz njihove perspektive, u nekoj drugoj transakciji. Ključni tehnološki napredak bitcoinovog protokola je mehanizam kojim je ovaj problem rešen.

Transakcije se sklapaju u grupe koje se zovu blokovi, a blokovi se povezuju kako bi formirali lanac blokova. Smatra se da su se transakcije u okviru bloka dogodile u isto vreme. Blokovi se ređaju na osnovu činjenice da svaki blok ima referencu na prethodni blok u lancu. Transakcije koje nisu već u bloku se zovu „nepotvrđene“. Svaki čvor u mreži može prikupiti skup nepotvrđenih transakcija, sklopiti ih u blok i predložiti ih kao sledeći blok u lancu. Predloženi blok mora sadržati rešenje kompleksnog matematičkog problema koji je teško kompjuterski izračunati⁹⁹. Bitcoin mreža dinamički prilagođava težinu matematičkog problema tako da se novi blok dodaje lancu blokova prosečno svakih deset minuta¹⁰⁰.

Iako je to malo verovatno, može se dogoditi da više čvorova u bitcoin mreži predloži blokove otprilike u isto vreme. U tom slučaju, lanac blokova se privremeno grana kako različiti čvorovi pripajaju različite blokove lancu blokova. Situacija se razrešava kada se sledeći blok doda lancu. Kao što je već pomenuto, novi blok će sadržati referencu na prethodni blok u lancu. On će stoga biti dodat jednom od dva moguća ogranka lanca blokova, i time učiniti da jedan ogranak bude duži od drugog. Pravilo bitcoin mreže je da čvorovi moraju da se prebace na najduži raspoloživi ogranak a rezultat toga je da se lanac blokova vrlo brzo stabilizuje. Osim toga, svi čvorovi će se složiti oko svih blokova koji su udaljeni nekoliko blokova od kraja lanca. Stoga se smatra sigurnijim da se sačeka neko vreme pre nego što se, na primer, otpremi roba koja je zasnovana na transferu bitcoina. S obzirom da svakom bloku treba otprilike deset minuta da bude dodat na lanac, čekanje na šest blokova znači čekanje u trajanju od jedan sat.

5.2.3.4 Rudarenje

Prethodno opisani proces izgradnje blokova i njihovo dodavanje lancu blokova se zove rudarenje. Ko god reši blok i doda ga lancu blokova dobija nagradu od 25 bitcoina. Svake

⁹⁹ Čvor koji kreira blok mora da nađe numeričku vrednost koja, kada se iskombinuje sa drugim podacima tog bloka, kao rezultat kombinovanih podataka daje kriptografski heš sa vrednošću manjom od određenog praga.

¹⁰⁰ To se postiže smanjenjem vrednosti praga u izračunavanju heša, što znači da postoji manji broj prihvatljivih odgovora i time je identifikacija validne vrednosti teža.

četiri godine nagrada za blok se prepolovi dok na kraju više neće biti izdat nijedan bitcoin. Biće stvoreno ukupno 21 milion bitcoina.

Pored nagrade za bitcoin, rudari takođe primaju i naknadu za transakciju koja opcionalno može biti obuhvaćena transakcijom. Trenutno je glavna naknada za rudarenje nagrada za blok ali vremenom će naknade za transakcije postati podsticaj za rudarenje.

Najveći deo rudarenja ne obavljaju pojedinci već organizovane grupe rudara, poznate pod nazivom pulovi rudara. Nagradu za izračunavanje blokova dele članovi pula u srazmeri sa količinom napora koji je svaki član pula uložio u izračunavanje.

5.3 Rizici povezani sa virtuelnim valutama

Konvertibilne virtuelne valute koje se mogu zameniti za realni novac ili druge virtuelne valute su potencijalno podložne zloupotrebi radi pranja novca i finansiranja terorizma iz mnogo razloga. U ovom delu se opisuju rizici koji su pobrojani u vezi sa obe ove pretnje finansijskom integritetu¹⁰¹.

Prvo, one mogu omogućiti veću anonimnost od tradicionalnih bezgotovinskih načina plaćanja. Sisteme virtuelnih valuta kojima se može trgovati na Internetu generalno karakterišu odnosi sa klijentima koji nisu direktni i mogu omogućiti anonimno finansiranje (gotovinsko finansiranje ili finansiranje od strane trećih lica preko virtuelnih menjača koji ne identifikuju izvor finansiranja kako treba). Oni takođe mogu dozvoljavati anonimne transfere ako pošiljalac i primalac nemaju adekvatnu identifikaciju. Decentralizovani sistemi su naročito podložni rizicima anonimnosti. Na primer, bitcoin adrese, koje funkcionišu kao računi, namerno nemaju sa njima povezana imena ili drugu identifikaciju klijenta, a sistem nema centralni server ili provajdera. Bitcoin protokol ne zahteva niti pruža identifikaciju i verifikaciju učesnika niti generiše istorijsku evidenciju transakcija koje su nužno povezane sa identitetom u realnom svetu.

Nema centralnog nadzornog tela i niti softvera za sprečavanje pranja novca koji je trenutno na raspolaganju za praćenje i identifikovanje obrazaca sumnjivih transakcija. Organi koji su zaduženi za sprovođenje zakona ne mogu da se fokusiraju na jednu centralnu lokaciju ili subjekta (administratora) za potrebe istrage ili oduzimanja imovine (iako vlasti mogu da ciljaju pojedinačne menjače radi pribavljanja informacija o klijentima koje menjač može da prikuplja). Time se nudi nivo potencijalne anonimnosti koji je nemoguć kod tradicionalnih kreditnih i debitnih kartica ili već etabliranih platnih sistema, kao što je PayPal. Isto tako, globalni domašaj virtuelnih valuta povećava njihov potencijalni rizik od pranja novca/finansiranja terorizma.

Sistemima virtuelnih valuta se može pristupiti preko Interneta (uključujući preko mobilnih telefona) i mogu se koristiti za prekogranična plaćanja i prenos sredstava. Osim toga, virtuelne valute se obično oslanjaju na kompleksne infrastrukture koje obuhvataju nekoliko subjekata, često raštrkanih u nekoliko zemalja, za transfer sredstava ili izvršenje plaćanja. Ova segmentiranost servisa znači da odgovornost za poštovanje propisa koji regulišu pranje novca/finansiranje terorizma i nadležnost za nadzor/sprovođenje zakona mogu biti nejasni. Pored toga, evidencija o klijentima i transakcijama se može držati kod nekoliko subjekata, obično u različitim jurisdikcijama, što otežava pristup organima reda i

¹⁰¹ Evropsko bankarsko regulatorno telo (EBA) je sačinilo odličan dokument u kome su pobrojani rizici koje virtuelne valute predstavljaju za finansijski. Dostupno na: <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>

regulatornim organima. Ovaj problem je uvećan zbog prirode tehnologije i poslovnog modela virtuelnih valuta, uključujući i promjenljivi broj i tipove/uloge učesnika koji pružaju usluge platnim sistemima virtuelnih valuta, koji brzo evoluiraju. Bitno je imati na umu da se komponente nekog sistema virtuelne valute mogu nalaziti u jurisdikciji koja nema adekvatne kontrole pranja novca/finansiranja terorizma. Centralizovani sistemi virtuelnih valuta bi mogli biti umešani u pranje novca i mogu namerno tražiti jurisdikcije sa slabim režimima za sprečavanje pranja novca/finansiranja terorizma. Može se činiti da decentralizovane konvertibilne virtuelne valute koje omogućavaju anonimne transakcije između dva lica direktno egzistiraju u nekom digitalnom univerzumu u potpunosti van domašaja bilo koje pojedinačne zemlje.

Procena rizika od virtuelnih valuta FATF-a¹⁰² ukazuje da barem na kratki rok, jedino konvertibilne virtuelne valute, koje mogu da se koriste da se vrednost premešta ka i od dekretnih valuta i regulisanih finansijskih sistema verovatno predstavljaju rizik od pranja novca/finansiranja terorizma. Shodno tome, prema pristupu zasnovanom na riziku opisanom u navedenom izveštaju, zemlje treba da svoje napore u borbi protiv pranja novca/finansiranja usmere na rizičnije konvertibilne virtuelne valute.

Procena rizika takođe sugeriše da kontrolni mehanizmi protiv pranja novca/finansiranja terorizma treba da ciljaju čvorove konvertibilnih virtuelnih valuta — tj. tačke preseka koji predstavljaju kapiju ka regulisanom finansijskom sistemu — a ne da nastoje da regulišu korisnike koji pribavljaju virtuelnu valutu radi kupovine roba ili usluga. Ovi čvorovi, između ostalog, obuhvataju treća lica-menjače konvertibilnih virtuelnih valuta. Gde je to slučaj, oni treba da budu regulisani prema Preporukama FATF¹⁰³. Tako, zemlje treba da razmotre primenu relevantnih uslova za sprečavanje pranja novca/finansiranja terorizma definisanih u međunarodnim standardima na menjače konvertibilnih virtuelnih valuta, kao i na sve druge vrste institucija koje služe kao čvorovi gde se aktivnosti vezane za konvertibilne virtuelne valute ukrštaju sa finansijskim sistemima regulisanih dekretnih valuta.

Prema FATF-ovom pristupu baziranom na riziku, zemlje bi takođe mogle da razmotre regulisanje finansijskih institucija ili drugih subjekata koji primaju, šalju i čuvaju virtuelnu valutu, ali ne pružaju usluge menjača ili usluge pretvaranja virtuelne u dekretnu valutu ili obratno.

Izmene i dopune V Direktive za borbu protiv pranja novca¹⁰⁴ će uključiti platforme za razmenu/berze virtuelnih valuta i pružaoce usluga novčanika u područje primene propisa za sprečavanje pranja novca koje uvodi Direktiva tako što će ih definisati kao „obveznike“

PITANJA ZA RAZMIŠLJANJE

¹⁰² Virtual Currencies – Guidance for a risk-based approach, Financial Action Task Force, (Virtuelne valute – Uputstvo za pristup baziran na riziku, Radna grupa za finansijske mere u borbi protiv pranja novca), jun 2015. Dostupno na: <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>

¹⁰³ Radi otklanjanja nedoumice, Preporuke FATF – International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, Financial Action Task Force (Međunarodni standardi u borbi protiv pranja novca i finansiranja terorizma i širenja oružja za masovno uništenje, Radna grupa za finansijske mere u borbi protiv pranja novca), februar 2012. Dostupno na: <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>

¹⁰⁴ http://www.consilium.europa.eu/register/en/content/out?typ=SET&i=ADV&RESULTSET=1&DOC_TITL=&CONTENTS=&DOC_ID=15849%2F17&DOS_INTERINST=&DOC_SUBJECT=&DOC_SUBTYPE=&DOC_DATE=&document_date_from_date=&document_date_to_date=&document_date_submit=&document_date_to_date=&document_date_submit=&MEET_DATE=&meeting_date_from_date=&meeting_date_to_date=&meeting_date_submit=&DOC_LANCD=EN&ROW_SPP=25&NRROWS=500&ORDERBY=DOC_DATE+DESC

1. Gde se odvija zamena virtuelne valute za realnu valutu?
2. Kako se identifikuju strane u transakciji u bitcoin sistemu virtuelne valute?
3. Koje osnovne karakteristike decentralizovanih virtuelnih valuta ih čine teškim za regulisanje?
4. Kako se naziva javna glavna knjiga transakcija sa bitcoinom?

5.4 Izazovi u istrazi¹⁰⁵

5.4.1 Znanje o tome da su korišćene virtuelne valute

Prvi izazov sa kojim se susreću istrage koje obuhvataju virtuelne valute su identifikovanje upotrebe virtuelne valute i/ili da li se imovina proistekla iz izvršenja krivičnog dela drži u formi virtuelne valute. Kod virtuelnih valuta, prikaz vrednosti je skoro uvek u potpunosti u elektronskoj formi¹⁰⁶.

Stoga, kod istražitelja mora postojati svest o mogućnosti da imovinska korist pribavljena krivičnim delom može biti pretvorena u virtuelnu valutu. Digitalni forenzički analitičari moraju takođe imati tehničke kapacitete i sposobnosti da razumeju gde/kako da traže da li je korišćena virtuelna valuta na zaplenjenim medijumima za čuvanje elektronskih podataka.

5.4.2 Anonimnost transakcije

Od nastanka distribuirane virtuelne valute, jedna često pominjana karakteristika njihovog funkcionisanja je navodna anonimnost transakcija. Stoga je možda ključni izazov u istrazi koja obuhvata bitcoine povezivanje aktivnosti određenog novčanika za bitcoin sa individuum u realnom svetu.

Bez obzira na činjenicu da su sve transakcije sa bitcoinom i sadržaj novčanika vidljivi svima u lancu blokova, osim ako nemate privatni ključ ne možete da prenesete bitcoin drugom vlasniku računa¹⁰⁷. Međutim, osoba koja je u posedu konkretnog privatnog ključa ne biva otkrivena kroz vršenje transakcije sa bitcoinom.

Identifikovane su tehnike koje omogućavaju da se, u određenim okolnostima, IP adrese povežu sa konkretnom transakcijom¹⁰⁸. Jedna od prvih identifikacionih tehnika je opisana u akademskom radu koji su objavili Filip i Dajana Koši (Philip and Diana Koshy) 2014 godine¹⁰⁹. Oni su napravili svoju sopstvenu verziju bitcoin softvera koji je preuzeo kopiju svakog pojedinačnog paketa podataka koji je preneo svaki kompjuter u bitcoin mreži. Analizom ovih podataka, Košijevi su bili u stanju da utvrde određene obrasce podataka koji su omogućili identifikaciju IP adrese iza konkretnih transakcija sa bitcoinom. Međutim,

¹⁰⁵ Napominjemo da se u narednim razmatranjima bitcoin pominje kao primer decentralizovane virtuelne valute. Ovde opisani izazovi su relevantni za veliku većinu virtuelnih valuta, naročito za decentralizovane virtuelne valute.

¹⁰⁶ Postoje neke organizacije koje prodaju fizičke prikaze vrednosti virtuelne valute, ali oni su ekstremno retki i nisu u širokoj upotrebi. Vidi, na primer <http://www.coindesk.com/10-physical-bitcoins-good-bad-ugly/>

¹⁰⁷ Vidi prethodno navedenu studiju za opis toga kako bitcoin funkcioniše.

¹⁰⁸ <http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin>

¹⁰⁹ An Analysis of Anonymity in Bitcoin Using P2P Network Traffic, Koshy et al http://fc14.ifca.ai/papers/fc14_submission_71.pdf

trenutno nije verovatno da će takve tehnike biti na raspolaganju većini krivičnih istraga zbog računskih izazova koje predstavljaju.

5.4.3 Identifikacija izvora sredstava

U istragama gde je utvrđeno da su korišćene virtuelne valute, može biti neophodno u nekim slučajevima da se utvrdi da su sredstva pribavljena na nezakonit način. Osumnjičeni može biti saslušan po ovom pitanju ali u slučajevima kada osumnjičeni ne sarađuje i/ili kada osumnjičeni još uvek nije svestan da je pod istragom, može biti teško da se ustanovi kako su virtuelne valute kupljene.

U tom kontekstu, pomoć privatnog sektora je ključna. Menjači virtuelnih valuta koji su obveznici¹¹⁰ bi mogli da pruže informacije o pojedinačnim klijentima, tako što će čuvati imena, verifikovane podatke za kontakt, IP evidencije, dnevnik aktivnosti, sve adrese virtuelne valute koje korisnik koristi na berzi, lične poruke, podatke o uplatama, dokaz identiteta i dokaz kućne adrese.

Korišćenje procesnih pravila koje predviđa Budimpeštanska konvencija o visokotehnološkom kriminalu bi takođe omogućilo pristup podacima koje drže menjači i drugi učesnici u ekosistemu virtuelnih valuta (npr. putem naloga za zaštitu sačuvanih podataka, prikupljanje podataka o saobraćaju u realnom vremenu, itd.)

Izazov identifikovanja izvora sredstava u transakciji sa bitkoinom je još veći zbog korišćenja mikser-servisa. Ovi servisi rade tako što prihvataju transakcije više ljudi, dele preneti sredstva na manje iznose i pomešaju sredstva sa sredstvima koje prenose drugi korisnici tog servisa. To znači da, s tačke gledišta primaoca sredstava, prvobitni izvor sredstava je u najmanju ruku dobro prikriiven a potencijalno postao potpuno anoniman¹¹¹.

5.4.4 Unovčavanje/realizacija i konverzija imovinske koristi

Tačka u kojoj se vrednost prikazana u virtuelnoj valuti konvertuje u dekretnu valutu, predstavlja priliku za snage reda. Ova konverzija se obično odvija na berzi virtuelnih valuta, te otud se preporuke FATF-a u vezi sa virtuelnim valutama, o kojima je kratko bilo reči u delu 5.3, fokusiraju na regulisanje čvorova virtuelnih valuta. „Čvorovi“ u ovom kontekstu se odnose na tačke gde je svet virtuelnih valuta u dodiru sa svetom tradicionalnih finansija, i obuhvataju, između ostalog, berze virtuelnih valuta.

Kada su berze virtuelnih valuta regulisane, one moraju da preduzmu mere poznavanja i praćenja stranke kako bi identifikovale svoje klijente. U konkretnom slučaju bitkoina, sve transakcije su javno dostupne u lancu blokova. To znači da, u slučajevima kada organi za sprovođenje zakona saznaju za konkretnu adresu virtuelne valute koja je pod kontrolom osumnjičenog, analiziranjem transakcija koje je izvršio osumnjičeni može biti moguće da se identifikuje korišćenje određene berze virtuelnih valuta. U tim slučajevima, organi zaduženi za sprovođenje zakona mogu onda uručiti sudski nalog relevantnoj berzi virtuelnih valuta da otkrije podatke o korisniku kao što su ID, kućna adresa, IP adrese, email adrese, broj telefona, istorija transakcija, adrese deponovanja i podizanja sredstava, ima banke, broj računa u banci i informacije o transakciji.

U januaru 2016. godine, na primer, deset ljudi je uhapšeno u Holandiji u sklopu međunarodne akcije protiv onlajn tržišta nelegalnih droga. Ti ljudi su bili uhvaćeni kako

¹¹⁰ Obveznici po zakonima o sprečavanju pranja novca/ finansiranja terorizma nisu ograničeni na menjače virtuelnih valuta, agente za obradu plaćanja, onlajn novčanike, priređivače onlajn igara; i drugi onlajn servisi takođe mogu pomoći u istrazi.

¹¹¹ https://en.bitcoin.it/wiki/Mixing_service

konvertuju svoje bitcoine u evre na bankarskim računima pomoću komercijalnih bitcoin servisa, a onda podižu milione u gotovini sa bankomata. Trag bitcoin adrese koja je navodno povezivala novac sa onlajn prodajom droge su pratili FBI i Interpol. FATF, u svom izveštaju o virtuelnim valutama iz 2014. godine („Virtuelne valute: Glavne definicije i potencijalni rizici od pranja novca i finansiranja terorizma”), daje primere nekoliko drugih dobro poznatih akcija organa reda koje su obuhvatale virtuelne valute.¹¹² Zainteresovani čitalac se podstiče da prouči ove studije slučaja radi dodatnog uvida u red veličine i kompleksnost prethodnih istraga koje su uključivale virtuelne valute.

Međutim, kako je rečeno na drugom mestu u ovom priručniku, izazovi i dalje postoje zbog globalnog karaktera virtuelnih valuta. Ovi izazovi se kreću u rasponu od činjenice da regulisanje berzi virtuelnih valuta u svetu nije konzistentno do praktičnih teškoća povezanih sa međunarodnim istragama.

5.5 Izazovi ograničenja raspolaganja /oduzimanja

5.5.1 Virtuelna valuta kao imovinska korist stečena krivičnim delom

Mnoge zemlje ne moraju da definišu karakter protivpravne imovinske koristi. U tim slučajevima, sredstvo čuvanja vrednosti kao što je bitcoin treba da se smatra imovinskom korišću stečenu krivičnim delom ako je imovinska korist proistekla iz kriminalne aktivnosti. Međutim, to mora da bude utvrđeno u vašoj konkretnoj jurisdikciji.

5.5.2 Utvrđivanje postojanja virtuelne valute

Prvi izazov je da se utvrdi postojanje virtuelne valute i da se utvrdi da je ona pod kontrolom osumnjičenog. Neki od problema koji se pritom pojavljuju su već razmatrani u delu 5.4. Postojanje i kontrola virtuelnih valuta može, na primer, postati očigledna iz nadzora, posebnih dokaznih radnji ili čak priznanja.

5.5.3 Ograničavanje raspolaganja/preuzimanje kontrole nad virtuelnom valutom

Po identifikovanju imovinske koristi stečene krivičnim delom koja se drži u obliku virtuelne valute, sledeće pitanje je imobilizacija virtuelne valute i sprečavanje njenog rasipanja. Deo izazova kod zabrane raspolaganja virtuelnim valutama predstavlja njihov virtuelni karakter, što znači da mogu postojati mnoge kopije novčanika virtuelne valute. Čak i u slučajevima gde je onlajn novčanik ili novčanik koji se drži na ličnom računaru osumnjičenog privremeno oduzet, nema osnova da se veruje da je virtuelna valuta izmeštena van kontrole osumnjičenog. Nije neuobičajeno da osumnjičeni ima rezervne ključeve/novčanik koji se drži na nekom drugom mestu u klauđu (prostoru za čuvanje na internetu). Stoga, pokušaji da se preuzme kontrola nad novčanikom virtuelne valute osumnjičenog ne mogu izvesno značiti da je imovina izmeštena van kontrole osumnjičenog.

Mora da se naglasi da se virtuelne valute ne čuvaju na nekom uređaju kao takvom. U slučaju bitcoina, privatni ključ je taj koji omogućava nekome da ih potroši. Postoje dva glavna načina za privremeno oduzimanje bitcoina, naime obezbeđivanje pristupa privatnom ključu osumnjičenog ili saradnja sa privatnim sektorom (tj. menjačima) koji

¹¹² FATF Report, Virtual Currencies Key Definitions and Potential AML/CFT Risks, June 2014. Dostupno na: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

kontrolišu privatni ključ osumnjičenog. Onog trenutka kad istražitelji budu u posedu privatnog ključa osumnjičenog, da bi se oduzimanje izvršilo, potrebno je da se izvrši transfer sredstava pošto osumnjičeni ili neko drugo lice koje kontrolise privatni ključ može da premesti sredstva na neku drugu adresu. Sredstva treba preneti na bitkoin adresu koju kontrolišu organi reda (istražitelji ili javno tužilaštvo). Napominjemo da će postupak zavisiti od nacionalnog zakonodavstva.

Tužilac može pribaviti sudski nalog ili poseban nalog za zabranu raspolaganja koji bi sprečio osumnjičenog ili njegove zastupnike da troše virtuelnu valutu. To neće sprečiti agente koji se nalaze u inostranstvu, gde nalog možda nema nikakvo dejstvo, da učine nešto da se virtuelna valute premesti ili potroši.

Ako je moguće, tužilaštvo treba da se postara da likvidira saldo virtuelne valute što pre (vidi deo 5.5.4). To zahteva blagovremeno izvršenje procesa preuzimanja kontrole nad imovinom, u slučaju da osumnjičeni ima pristup rezervnoj kopiji ciljnog novčanika virtuelne valute. Osim toga, vrednost virtuelnih valuta je često nestabilna i likvidiranjem i prenošenjem salda na državni račun možete biti sigurni da ste sačuvali vrednost prikazanu virtuelnom valutom u trenutku istrage i da ste je stavili na raspolaganje radi konačnog trajnog oduzimanja u slučaju osuđujuće presude.

5.5.4 Upravljanje imovinom

Preporučena najbolja praksa je da se sredstvo čuvanja vrednosti u vidu virtuelne valute likvidira. To je zasnovano na potrebi da se održi vrednost oduzete robe (npr. kao sa privremeno oduzetim hartijama od vrednosti i stranom valutom u gotovini). Time se čuva i vrednost imovine i štiti se od nestabilnosti na tržištu. Tako se takođe obezbeđuje da virtuelna valuta ne može da se premesti, prenese ili stavi van domašaja sudova. Većina jurisdikcija u svojim zakonima i propisima predviđa likvidiranje imovine kako bi se sačuvala vrednost radi konačnog trajnog oduzimanja, ali to bi trebalo da bude tako utvrđeno u vašoj konkretnoj jurisdikciji.

Direktiva EU o oduzimanju imovine¹¹³ preporučuje da se osnuje kancelarija za upravljanje privremeno i trajnom oduzetom imovinom¹¹⁴. Ako je takva kancelarija osnovana u vašoj jurisdikciji, vredi upoznati sa mogućnostima te kancelarije da likvidira vrednost koja je sačuvana u virtuelnoj valuti. Alternativno, ako takva kancelarija ne postoji, mogućnost da se likvidira vrednost virtuelne valute će zavisiti od kapaciteta mehanizma za upravljanje imovinom pre njenog trajnog oduzimanja, kakav god on bio.

PITANJA ZA RAZMIŠLJANJE

1. Zašto je najbolja praksa da se virtuelna valuta likvidira što pre?
2. Da li je neophodno u vašoj jurisdikciji da se utvrdi nezakoniti izvor konkretne imovinske koristi pribavljene krivičnim delom? Ako je tako, kako bi to moglo da se uradi u slučaju virtuelne valute?
3. Koji uslovi moraju biti zadovoljeni pre nego što može da se pribavi nalog za privremeno oduzimanje virtuelne valute?
4. Koje mere se mogu koristiti za utvrđivanje postojanja ili korišćenja virtuelne valute? Koje zaštitne mere postoje za zaštitu interesa nedužnih

¹¹³ Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union.

¹¹⁴ *Ibid* Preambula stav 32.

trećih lica?

6 Praktičan rad/Studije slučaja

6.1 Pretraga literature

Molimo vas da uputite na relevantne članove vaših nacionalnih zakona i propisa i relevantne sudske prakse, uz kratak opis, u vezi sa sledećim pitanjima:

1. Trajno oduzimanje imovinske koristi pribavljene krivičnim delom kao obaveza po Krivičnom zakoniku ili Zakoniku o krivičnom postupku/posebnom zakonu.
2. Definicija finansijske istrage, kada treba da se vodi finansijska istraga, ko sprovodi finansijsku istragu?
3. Pristup podacima u banci i nadzor nad bankarskim računom.
4. Definicija i korišćenje posebnih dokaznih radnji.
5. Pristup drugim bazama podataka o vlasništvu (zemljišnim knjigama, registru automobila, itd.)
6. Nalog za zabranu raspolaganja.
7. Odluka o trajnom oduzimanju.
8. Režim trajnog oduzimanja (krivični postupak, trajno oduzimanje bazirano na vrednosti, prošireno oduzimanje, pretpostavka neravnoteže, trajno oduzimanje koje nije zasnovano na osuđujućoj presudi (in-rem)).
9. Međunarodna pravna pomoć.
10. Specijalizovane institucije.
11. Formiranje Udarne grupe (tužilaštvo, policija, FOS, poreska služba, carina).
12. Pristup podacima o pretplatnicima (IP adresi, internet stranici, nalogu elektronske pošte).
13. Pristup podacima o saobraćaju i podacima iz sadržaja.
14. Zahtev za zaštitu (sačuvanih podataka).
15. Privremeno oduzimanje elektronskih dokaza.

6.2 Studija slučaja 1: Razmatranje zakonskog osnova za radnje

Vaša nacionalna policija je pokrenula istragu protiv osumnjičenih A, B i C, koji formiraju organizovanu kriminalnu grupu da bi prodavali velike količine marihuane kupcima, D i E.

Pomoću tajnih mera (tajno praćenje i nadzor komunikacija) je utvrđeno da je dana 15. oktobra 2016. godine Osoba A isporučila 1kg marihuana Osobi D, koja je platila 1.000 EUR u gotovini u koferu. Odobreni su odlaganje zaplene i hapšenje. Istog dana, Osoba A je dostavila kofer s novcem Osobi B. Dalje je utvrđeno da se Osoba A dogovorila telefonom sa Osobom E da mu proda 2kg marihuane, za šta će 2.000 EUR biti preneto na račun u banci broj 11.

Odlučujete da vam je potreban pristup podacima o vlasniku računa u banci broj 11, uključujući vlasnika računa i podatke o transakcijama a poslednjih X meseci. Takođe odlučujete da vam je potrebno da započnete nadzor nad transakcijama za račune osoba A, B i E.

PITANJE: Opišite pravni osnov u vašem nacionalnom zakonodavstvu, pozivajući se na konkretne članove i uslove za pristup bankarskim podacima, podacima o transakcijama i nadzor nad računima.

Ovom merom utvrđujete da A, B i E svi imaju račune u bankama u vašoj zemlji. Takođe identifikujete račun u banci u vlasništvu Osobe B u Austriji.

Odlučite da zatražite sudski nalog za bankarske podatke, podatke o transakcijama i nadzor nad računom B u Austriji i zatražite međunarodnu pravnu pomoć u ovoj stvari.

PITANJE: Navedite pravni osnov u vašem nacionalnom zakonodavstvu, pozivajući se na konkretne članove i uslove za međunarodnu pravnu pomoć.

Kroz analizu bankarskih računa A, B i E postaje jasno da postoje česte transakcije između A i B, česte transakcije od E prema B i takođe transakcije od B ka inostranstvu (u jednu drugu zemlju u regionu i u Luksemburgu). Poredite i pravite korelaciju dinamike transakcija sa nalazima krivične istrage.

Nadzor na telefonskim komunikacijama otkriva da B pregovara sa C, koji boravi u vašoj zemlji i u jednoj drugoj zemlji u regionu, o isporuci veće količine marihuane za mesec dana, 15. decembra 2016. godine. C traži avans pre 1. decembra 2016. u iznosu polovine cene (100.000 EUR) na račun u banci 22 (koji drži pravno lice DOO); preostalih 100.000 EUR mora da se plati na račun u banci 33, koji je u banci u Luksemburgu.

Odlučite da nađete podatke o bankarskim računima osobe C u vašoj zemlji i u toj drugoj zemlji u regionu i da obezbedite nalog za nadzor nad računima. Takođe odlučujete da utvrdite vlasništvo na pravnim licem DOO i njegove račune u bankama i da naložite davanje podataka o transakcijama za poslednjih X meseci i nadzor nad računima DOO.

PITANJE: Navedite pravni osnov u vašem nacionalnom zakonodavstvu, pozivajući se na konkretne članove i uslove za pristup podacima o pravnim licima, podacima o banci i transakcijama pravnih lica i poreskoj evidenciji pravnih lica.

UZ pomoć poreske službe, odlučite da utvrdite kako DOO posluje i ko su mu poslovni partneri. Otkrijete da DOO takođe trguje industrijskim kanabisom.

Tražite evidenciju za račun u banci 33 u Luksemburgu i otkrivete da pripada pravnom licu u vašoj zemlji, u vlasništvu osobe C.

PITANJE: Da li postoji sumnja na pranje novca? U kom trenutku se javlja ta sumnja? Treba li da uključite FOS u udarnu grupu za ovu istragu? Oko čega FOS može da vam pomogne? Koje moguće tipologije pranja novca se ovde koriste? Navedite pravni, elemente i uslove za pranje novca u vašem nacionalnom zakonodavstvu. Navedite pravni osnov i uslove u vašem nacionalnom zakonodavstvu za angažovanje FOS.

Nadzorom nad telefonskom komunikacijom utvrđeno je da se Osoba B poziva na imejl komunikaciju sa Osobom A koja sadrži informacije o transakcijama sa drogom i plaćanju u bitkoinima.

Odlučite da je potrebno da identifikujete imejl adrese koje koriste Osoba A i Osoba B i sadržaj elektronske pošte. Utvrdite da Osoba A koristi imejl adresu koju pruža lokalni internet provajder.

PITANJE: Navedite pravni osnov u vašem nacionalnom zakonodavstvu, pozivajući se na konkretne članove i uslove za saradnju sa provajderom internet usluga i pristup sadržaju imejl poruka.

Iz sadržaja imejla Osobe A identifikujete transakciju sa drogom prema D i E i drugima i takođe transfere gotovine na bankarske račune kao i transfer vrednosti u bitkoinima.

Odlučili ste da zatražite pomoć od FOS za analizu bankarskih transakcija i traženje veza i podataka o vlasnicima relevantnih računa u inostranstvu (u Austriji i Luksemburgu kao i u drugim zemljama u vašem regionu).

PITANJE: Navedite pravni osnov u vašem nacionalnom zakonodavstvu, pozivajući se na konkretne članove i uslove za pristup bankarskim podacima od strane FOS i međunarodnu saradnju FOS.

Kroz istragu utvrdite da dospeva uplata u bitkoinima od Osobe C prema Osobi B dana 15. decembra 2016. godine. Utvrdite da novčanik sa bitkoinima Osobe B drži berza bitkoina u Luksemburgu.

PITANJE: Navedite pravni osnov u vašem nacionalnom zakonodavstvu, pozivajući se na konkretne članove i uslove za traženje podataka o pretplatnicima od berze bitkoina. Da li bi berza bitkoina u vašoj zemlji bila dužna da drži podatke i sarađuje?

PITANJA:

- Koje mere biste preduzeli u vezi sa planiranom uplatom 1. decembra 2016. g. na račun 22 pravnog lica DOO?
- Da li biste naložili unapred zamrzli transakciju? Kada se otkriva nalog za zabranu raspolaganja? Da li bi zamrzavanje transakcije na računu DOO ugrozilo zaplenu velike količine droge čija isporuka je planirana za 15. decembar 2016.g?
- Pošto osumnjičeni budu uhapšeni, koje mere bi bile preduzete u vezi sa gotovinskom isplatom od 15. decembra 2016.g?
- Imajući u vidu da je grupa A, B i C već dugo u poslu s drogom, koliko i koje imovine bi bilo trajno oduzeto? Navedite pravni osnov u vašem nacionalnom zakonodavstvu za svoj odgovor.
- Da li pravno lice DOO može da bude optuženo za nedozvoljenu trgovinu drogom i/ili pranje novca? Ako je tako, navedite pravni osnov u vašem nacionalnom zakonodavstvu i uslove za izricanje kazne pravnom licu. Dajte primer odluke i obrazloženja u vezi sa trajnim oduzimanjem imovine od pravnog lica.

Analiziranjem komunikacije elektronskom poštom između B i A, otkrijete da grupa takođe prodaje drogu preko posebne internet stranice na *darkwebu*. To potvrđuje jedan od njihovih kupaca koji tokom saslušanja otkriva kako funkcioniše naručivanje i otprema droge preko *darkweba* i kako se plaćanje traži ili na račun u banci ili u bitkoinima¹¹⁵.

PITANJE: Koje bi bile vaše radnje u vezi sa dokazima o aktivnostima na *darkwebu*? Da li biste mogli da se upustite u prikrivenu istragu kao kupac i kupite drogu, otkrijete relevantne bankarske račune i bitkoin novčanike i zamrznete novac i imovinu (zabranite raspolaganje)?

¹¹⁵ Vidi primer na: <https://www.bitstamp.net/help/what-is-bitcoin/>

6.3 Studija slučaja 2: Razmatranje interakcije između FOS i organa reda

Finansijsko-obaveštajna služba (FOS) u vašoj zemlji primi prijavu iz jedne banke koja ukazuje na sumnju u pogledu nekih transakcija koje se odvijaju preko onlajn bankarstva. Ta institucija je utvrdila da su velike sume novca bile prenete na nekoliko računa klijenata, s tim da takvi iznosi novca nisu bili tipični za klijente o kojima je reč. Osim toga, finansijska institucija je primetila da su se klijenti naizgled prijavljivali (logovali) na svoj nalog za onlajn bankarstvo sa IP adrese u Rumuniji, zemlji iz koje se ni jedan od tih klijenata nikad nije prijavljivao ranije na svoj nalog. Ovakvo ponašanje je uočeno na ukupno 20 računa klijenata a ukupna vrednost koja je ušla na tih 20 računa je 750.000 EUR.

FOS vrši analizu i utvrđuje druge izveštaje o sumnjivim transakcijama koji pokazuju da je bilo sumnjivih transakcija koje su prolazile preko računa klijenata drugih banaka. FOS priprema izveštaj i predaje ga policiji.

Pregledom operativnih policijskih podataka utvrđeno je da postoji policijska istraga rumunskih državljana (zapravo Moldavaca sa boravkom u vašoj zemlji) u vezi sa lažnim ličnim dokumentima.

Policija hapsi ta lica i vrši pretres njihovih prostorija i pritom oduzima neke laptop kompjutere. Forenzičkim ispitivanjem laptopova otkriva se da su korišćeni za kontrolu preko 200 bankarskih računa koji se koriste za prijem i pranje novca poteklog sa bankarskih računa fizičkih lica čiji kompjuteri su zaraženi trojancem 'Dridex'¹¹⁶ koji je pokupio njihove podatke za identifikaciju za onlajn račune u banci. Ukupan iznos opran preko ovih računa je preko 3 miliona evra.

Osumnjičeni se krivično gone i izriče im se kazna zatvora od po 8 i 5 godina. Nije došlo do povraćaja bilo kakve imovinske koristi.

PITANJE: Šta predstavlja zakonski osnov za FOS da prijavi ovaj slučaj policiji?

Možda postoji zakonodavni osnov za ovakvu interakciju, ali u mnogim slučajevima, policija i FOS (i druge organizacije kao što su poreska i carinska uprava, itd.) potpisuju Memorandum o razumevanju koji omogućava razmenu informacija. Osnov može zavisiti od karaktera izveštaja koji je dostavljen policiji. Na primer, informacije koje se dostavljaju policiji mogu se smatrati (od strane policije) za obaveštajne podatke ili se mogu smatrati prijavom krivičnog dela.

Molimo vas da ispitajte situaciju u svojoj zemlji.

PITANJE: Koje odredbe zakonika o krivičnom postupku su relevantne za policijsku istragu?

U vezi sa oblašću visokotehnološkog kriminala, finansijskih istraga i pranja novca postoji nekoliko radnji koje policija preduzima u scenariju ovog slučaja; pretres lica i prostorija,

¹¹⁶ Dridex je agresivan Trojanac koji se koristi uglavnom za krađu bankarskih podataka o identitetu. Taj maliciozni softver (malver) je konfigurisan da cilja na klijente skoro 300 raznih organizacija u preko 40 regiona. Dridex je vrlo fokusiran na klijente finansijskih institucija u bogatim zemljama u kojima se govori engleski, i većina ciljanih organizacija se nalaze u ovim zemljama. Napadači su takođe svrstali druge evropske nacije u prioritete zajedno sa nizom azijsko-pacifičkih regiona.

privremeno oduzimanje laptopova i forenzičko ispitivanje, prikupljanje dokaza sa kompromitovanih bankarskih računa.

Vrha ovog pitanja je razmatranje pravnog osnova u vašem zakoniku o krivičnom postupku za ove radnje.

PITANJE: Kojim odredbama vašeg krivičnog zakonika se inkriminiše inficiranje ličnog računara klijenata virusom?

Ako je vaša zemlja ratifikovala Budimpeštansku konvenciju, onda će inficiranje ličnog računara virusom biti inkriminisano. Koja je odredba vašeg Krivičnog zakonika kojom se transponuje relevantni član iz Budimpeštanske konvencije?

Ako vaša zemlja nije ratifikovala Budimpeštansku konvenciju, da li imate ekvivalentne odredbe? Kako se inkriminišu kompjuterska krivična dela?

PITANJE: Kako biste povezali aktivnost Dridex Trojanca sa okrivljenima?

Osumnjičeni su koristili maliciozni softver (malver) da pokupe podatke o identitetu za onlajn bankarstvo. Međutim, ovi podaci su pokupljeni sa ličnih računara žrtava, ne sa ličnih računara osumnjičenih. Kako, dakle, možete da povežete aktivnost Trojanca sa osumnjičenima? Da li možete da napravite uzročno-posledičnu vezu između posedovanja podataka o kompromitovanom bankarskim računima (što se može utvrditi njihovim prisustvom na laptopovima osumnjičenih), sa radnjom kompromitovanja tih podataka o računima Trojancem? Ako možete, kako biste tome pristupili? Ako ne možete, kakve implikacije, ako postoje, to ima na tačke optužnice koja može da se podigne protiv osumnjičenih?

PITANJE: Kako biste utvrdili veze između Rumuna/Moldavaca i kontrolora računa u bankama gde je novac prenet i lica koje je izvršilo diseminaciju virusa. Kako biste mogli da utvrdite da li postoji imovina osumnjičenih (u vašoj zemlji ili inostranstvu)?

Nadovezujući se na prethodno pitanje, prisustvo podataka o bankarskim računima na laptopovima osumnjičenih može, ili ne mora, da demonstrira da su osumnjičeni imali kontrolu nad bankarskim računima u trenutku kada je predmetni novac bio transferisan. Da li to mora odvojeno da se utvrdi ili se može izvesti iz posedovanja bankarskih računa? Ako ne, šta još je potrebno utvrditi?

PITANJE: Da li možete da krivično gonite kompjuterski omogućenu krađu?

Kompjuteri su se u ovom slučaju koristili kao fundamentalna komponenta krađe. Da li postoji odredba u vašem nacionalnom zakonodavstvu kojom se inkriminiše korišćenje računara kao instrumenta u slučajevima krađe/prevare?

PITANJE: Koje procesne odredbe u vašem nacionalnom zakonodavstvu regulišu prikupljanje i korišćenje elektronskih dokaza?

U slučajevima kao što je ovaj, dokazi sa laptopova osumnjičenih mogu biti od ključne važnosti. Koje su, stoga, odredbe vašeg nacionalnog zakonodavstva koje omogućavaju prikupljanje i korišćenje elektronskih dokaza?

PITANJE: Da li vaša zemlja ima kapacitete za kompjutersku forenziku? Kako se koriste kapaciteti za kompjutersku forenziku?

U praksi prikupljanje elektronskih dokaza i upravljanje istima zahteva specijalističke alate i veštine. Kako je to organizovano u vašoj zemlji?

PITANJE: Da li finansijska istraga treba da se vodi u ovom slučaju? U kom trenutku treba da se pokrene finansijska istraga?

Kako je opisano u scenariju, postoje jasno značajne finansijske implikacije povezane sa aktivnošću osumnjičenih. Da li bi u vašoj zemlji finansijska istraga bila sprovedena u ovom slučaju (i da li bi trebalo)? Ako da, u kom trenutku treba finansijsku istragu?

PITANJE: Kojim odredbama vašeg nacionalnog zakonodavstva je regulisan pretres, privremeno i trajno oduzimanje imovine u ovom slučaju? Kako biste povratili ukradeni novac? Da li možete da ga zamrznete/zabranite raspolaganje istim (FOS ili policija/tužilac)?

U ovom scenariju se navodi da su osumnjičeni dobili zatvorske kazne. Da li vaše nacionalne odredbe zahtevaju da se komponenta postupka koja se odnosi na trajno oduzimanje imovine sprovodi posle krivičnog postupka ili se to događa u okviru jednog postupka?

Da li oštećeni koji su bili prevareni imaju ikakvu priliku da povrate svoja ukradena sredstva? Da li možete da izvršite nadoknadu oštećenima ako povratite neki deo novca/sav novac? Koje odredbe u vašem nacionalnom zakonodavstvu to omogućavaju?

PITANJE: Koje odredbe vašeg nacionalnog zakonodavstva opisuju delo pranja novca? Da li je izvršeno delo pranja novca?

Kako je delo pranja novca definisano u vašem nacionalnom zakonodavstvu? Uzimajući u obzir činjenice slučaja kako je opisan u scenariju, da li je izvršeno delo pranja novca?

PITANJE: Da li biste krivično gonili za delo pranja novca pored krađe/prevare? Zašto/zašto ne?

Tokom razmatranja ovog slučaja, da li biste krivično gonili za delo pranja novca kao i za krađu/prevaru? Ako da, zašto? Ako ne, zašto ne?

PITANJE: Oštećeni su rasprostranjeni širom mnogih zemlja, kako biste koordinirali vašu istragu sa tim zemljama?

Zbog prirode interneta koji ne poznaje granice, praktično svi predmeti sa komponentom visokotehnološkog kriminala takođe imaju i međunarodni element. U ovom slučaju, ako ima oštećenih iz mnogo zemalja, da li biste koordinirali svoje aktivnosti sa drugim zemljama? Šta ako tokom vaše istrage utvrdite postojanje još oštećenih za koje niste ranije znali?

PITANJE: Da li imate rokove za podnošenje dokaza i da li bi upiti preko međunarodne pravne pomoći prekoračili te rokove? Kako biste mogli da smanjite kašnjenje vezano za zahteve za međunarodnu pravnu pomoć?

Ako postoji i međunarodna komponenta, može postojati potreba da se koristi postupak međunarodne pravne pomoći, koji može da dovede do značajnih odlaganja u istrazi. Da li rokovi u postupku međunarodne pravne pomoći donose izazove u istrage u vašoj zemlji? Kako se odlaganja mogu smanjiti? Da li možete da koristite zajedničke istražne timove, na primer? Da li možete da koristite neformalne kanale komunikacija da biste omogućili upite pre pokretanja postupka međunarodne pravne pomoći?

6.4 Studija slučaja 3: Razmatranje interakcije između visokotehnološkog kriminala i pranja novca I

Nekoliko građana vaše zemlje prijavljuje da su njihovi lični računari zaraženi malicioznim softverom (malverom) koji je izvršio enkripciju svih njihovih fotografija i dokumenata. Malver je tada zahtevao plaćanje bitcoinom pre nego što ukloni enkripciju sa fotografija i dokumenata. U nekoliko slučajeva su građani platili otkupninu.

Tokom istrage, policija je radila sa FOS koji je pomagao u traganju i pronalaženju bitcoina. FOS je uspeo da uđe u trag bitcoinu na berzi gde se bitcoini konvertuju u dekretnu valutu. Berza bitcoina se nalazi u Sjedinjenim Državama.

Zahtev za međunarodnu pravnu pomoć (MPP) je upućen Sjedinjenim Državama, u kome se traže podaci o nalogima sa kojih je izvršena transakcija. Kada stigne odgovor od Sjedinjenih Država otkriva se da je vrednost bitcoina preneti na bankarske račune u vašoj zemlji pomoću IP adresa u vašoj zemlji.

PITANJE: Kako biste identifikovali osumnjičene (IP adrese)? Kako možete da pribavite takve podatke – u zemlji ili inostranstvu? Šta da te IP adrese nisu bile u vašoj zemlji?

Povezanost između IP adrese i osobe u realnom svetu je jedan od najvažnijih aspekata svake onlajn istrage. Ako je IP adresa u vašoj zemlji, kako radite sa nacionalnim pružaocima internet usluga da biste dobili pristup tim podacima? Koje zakonske odredbe omogućavaju takav pristup? Koje obaveze su nametnute pružaocima internet sluga da da zadrže i stave te podatke na raspolaganje?

Razmotrite situaciju u kojoj IP adresa nije u vašoj zemlji? Šta je drugačije? Kako biste pristupili toj situaciji u ovom slučaju?

PITANJE: Kako možete da uspostavite vezu između vlasnika računa u banci (stav tri u scenariju) i vlasnika novčanika za bitcoin i lica koja su koristila maliciozni softver? Da li u ovom slučaju treba da se sprovede finansijska istraga?

U odgovoru na zahtev za međunarodnu pravnu pomoć navode se podaci o IP adresama i računima u banci koji su korišćeni da se bitcoin konvertuje u dekretnu valutu. Kako ćete (a) saznati kod koje finansijske institucije se drži račun, ako to već ne znate i (b) raditi sa finansijskom institucijom da pribavite informaciju o vlasniku računa u banci. Koje zakonske odredbe vam omogućavaju ovakav pristup? Koje obaveze se nameću finansijskim institucijama u pogledu zadržavanja i stavljanja tih podataka na raspolaganje?

Ponovo razmotrite situaciju u kojoj su bankarski računi u drugoj zemlji. Šta je drugačije i kako biste pristupili ovoj situaciji u tom slučaju?

PITANJE: Da li treba da se pokrene finansijska istraga, i ako da, u kom trenutku?

Kako je opisano u scenariju, jasno postoje značajne finansijske implikacije povezane sa aktivnošću osumnjičenih. Da li bi se u vašoj zemlji sprovela finansijska istraga u ovom slučaju (i da li treba da se sprovede)? Ako je tako, u kom trenutku treba da se započne finansijska istraga?

PITANJE: U kojim odredbama vašeg nacionalnog zakonodavstva je opisano delo pranja novca? Da li je izvršeno delo pranja novca?

Kako se delo pranja novca definiše u vašem nacionalnom zakonodavstvu. Uzimajući u obzir činjenice o slučaju kako su opisane u scenariju, da li je izvršeno delo pranja novca?

PITANJE: U scenariju se opisuje zajednička aktivnost policije i FOS u analizi i traganju i pronalaženju aktivnosti sa bitkoinom. Koji zakonski osnov postoji za tu saradnju?

Možda postoji zakonodavni osnov za ovakvu interakciju, ali u mnogim slučajevima, policija i FOS (i druge organizacije kao što su poreska i carinska uprava, itd.) potpisuju Memorandum o razumevanju koji omogućava razmenu informacija.

Molimo vas da ispitajte situaciju u svojoj zemlji.

PITANJE: Kako su virtuelne valute, naročito bitkoin, regulisane u vašoj zemlji?

Postoje razni regulatorni režimi uspostavljeni širom sveta u vezi sa bitkoinom. Kakva je situacija u vašoj zemlji?

PITANJE: Da li su virtuelne valute obveznici i da li se od njih zahteva da prijave sumnjive transakcije u vašoj zemlji?

Naročito, da li postoji obaveza subjekata virtuelne valute kao što su berze ili servisi novčanika da prijavljuju sumnjive aktivnosti?

7 Aneks: Spisak relevantne literature

7.1 Savet Evrope

- Convention on Cybercrime, ETS 185, 23.11.2001 (Konvencija o visokotehnološkom kriminalu, ETS 185, 23.11.2001):
<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
- Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS 189, 28.01.2003 (Dodatni protokol uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema, ETS 189, 28.01.2003):
<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189>
- Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, CETS 198, 16.05.2005 (Konvencija o pranju, traženju, zapleni i oduzimanju prihoda stečenih kriminalom i o finansiranju terorizma, CETS 198, 16.05.2005):
<http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/198>
- Convention on Laundering, Search, Seizure And Confiscation of the Proceeds From Crime, Strasbourg, ETS 141, 08.11.1990 (Konvencija o pranju, traženju, zapleni i konfiskaciji prihoda stečenih kriminalom, Strazbur, ETS 141, 08.11.1990): <https://rm.coe.int/168007bd23>
- MONEYVAL/Global Project on Cybercrime, Criminal money flows on the Internet - Typology research, March 2012 (MONEYVAL/Globalni projekat o sajber kriminalu, Tokovi prljavog novca na internetu – Tipološka studija, mart 2012):
[http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL\(2013\)6_Reptyp_flows_en.pdf](http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2013)6_Reptyp_flows_en.pdf)
- Council of Europe Study on filtering, blocking and take-down of Illegal Content on the Internet, June 2016 (Studija Saveta Evrope o filtriranju, blokiranju i obaranju nelegalnog sadržaja na internetu, jun 2016):
<https://www.coe.int/en/web/cybercrime/-/study-on-filtering-blocking-and-take-down-of-illegal-content-on-the-internet>
- Questionnaire on the use and efficiency of Council of Europe instruments as regards international co-operation in the field of seizure and confiscation of proceeds of crime, including the management of confiscated goods and asset sharing. PC-OC Mod (2015) 06Rev4, 19.05.2016 (Upitnik o korišćenju i efikasnosti instrumenata Saveta Evrope kada je reč o međunarodnoj saradnji na polju privremenog i trajnog oduzimanja imovinske koristi, uključujući upravljanje trajno oduzetom imovinom i podelu imovine, PC-OC Mod (2015) 06Rev4, 19.5.2016.):
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000001680666607>

- Cybercrime Legislation – Country profiles (Zakonodavstvo o visokotehnološkom kriminalu – profili zemalja):
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp
- The functioning of 24/7 points of contact for cybercrime (discussion paper prepared by the Project on Cybercrime), April 2009 (Funkcionisanje kontaktnih tačaka 24/7 za visokotehnološki kriminal (dokument za diskusiju koji je pripremio Projekat o visokotehnološkom kriminalu), april 2009.):
<https://rm.coe.int/16802fa3be>
- Electronic Evidence Guide - A basic guide for police officers, prosecutors and judges (March 2013). Available subject to request at (Vodič za elektronske dokaze – Osnovni vodič za policijske službenike, tužioce i sudije (mart 2013). Dostupno na upit na):
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp
- T-CY (2006)04 – Strengthening co-operation between law enforcement and the private sector – examples of how the private sector has blocked child pornographic sites, 20 February 2006 (T-CY(2006)04 Jačanje saradnje između organa zaduženih za sprovođenje zakona i privatnog sektora - primeri slučajeva kada je privatni sektor blokirao sajtove sa dečjom pornografijom), februar 2006):
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e6ed1>
- T-CY(2013)17rev - T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, 3 December 2014 (T-CY(2013)17rev - T-CY Izveštaj o proceni: Odredbe Budimpeštanske konvencije o visokotehnološkom kriminalu o međunarodnoj pravnoj pomoći, 3. decembar 2014.):
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>
- T-CY(2014)17 - Rules on obtaining subscriber information report, December 2014 (T-CY(2014)17 – Pravila za dobijanje izveštaja o podacima o pretplatniku, decembar 2014.):
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7ad1>
- T-CY(2015)10 - Criminal justice access to data in the cloud: challenges, discussion paper prepared by the T-CY Cloud Evidence Group, May 2015 (T-CY (2015)10 - Pristup krivičnog pravosuđa podacima koji se nalaze u kladu: izazovi, dokument za diskusiju koju je pripremila Radna grupa T-CY za pristup dokazima u kladu, maj 2015.):
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59>
- T-CY(2016)13 - Emergency requests for the immediate disclosure of data stored in another jurisdiction through mutual legal assistance channels or through direct requests to service providers, T-CY Cloud Evidence Group, May 2016 (T-CY(2016)13 – Hitni zahtevi za neposredno otkrivanje podataka

sačuvanih u drugoj jurisdikciji putem kanala međunarodne pravne pomoći ili direktnih zahteva pružaocima usluga), Radna grupa T-CY za pristup dokazima u kladu):

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651a6f>

- T-CY (2016)2 – Criminal justice access to data in the cloud: cooperation with “foreign” service providers. Background paper prepared by the T-CY Cloud Evidence Group, May 2016 (T-CY (2016)2 – Pristup krivičnog pravosuđa podacima koji se drže u kladu: saradnja sa „inostranim“ pružaocima usluga, Osnovni dokument koji je pripremila Radna grupa T-CY za pristup dokazima u kladu, maj 2016.):
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d>
- T-CY(2016)7 - Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, final report of the T-CY Cloud Evidence Group, September 2016 (T-CY(2016)7 – Pristup krivičnog pravosuđa elektronskim dokazima u kladu: Preporuke za razmatranje T-CY, finalni izveštaj Radne grupe T-CY za pristup dokazima u kladu, septembar 2016.):
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>
- T-CY(2015)16 Adopted Guidance Note on Production Orders (Article 18) - Version 01 March 2017 (adopted by written procedure on 28 February 2017) (T-CY(2015)16 Usvojene smernice o nalogima za predaju [podataka] (član 18) – verzija od 01. marta 2017. (usvojene pisanim postupkom 28. februara 2017.)): <https://rm.coe.int/16806f943e>

7.2 Evropska unija

- Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union OJ L 127/39, 29.4.2014 (Direktiva 2014/42/EU o zabrani raspolaganja imovinom i trajnom oduzimanju predmeta krivičnih dela i imovinske koristi u Evropskoj uniji OJ L 127/39, 29.4.2014.) <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0042>
- Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Direktiva (EU) 2015/849 Evropskog Parlamenta i Saveta od 20. maja 2015. godine o sprečavanju korišćenja finansijskog sistema u svrhu pranja novca ili finansiranja terorizma, o izmeni Uredbe (EU) br. 648/2012 Evropskog parlamenta i Saveta kao i stavljanju van snage Direktive 2005/60/EZ Evropskog parlamenta i Saveta i Direktive Komisije 2006/70/EZ):
<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849>

- Joint Action 98/699/JHA of 3 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds from crime (OJ L 333, 9.12.1998, p. 1) (Zajednička akcija 98/699/JHA od 3. decembra 1998. koju je usvojio Savet na osnovu člana K.3 Ugovora o Evropskoj uniji, o pranju novca, identifikaciji, pronalaženju, zabrani raspolaganja, privremenom i trajnom oduzimanju predmeta i imovinske koristi stečene krivičnim delom (OJ L 333, 9.12.1998, str. 1)):
<http://eur-lex.europa.eu/legal-content/NLN/TXT/?uri=celex:31998F0699>
- Council Framework Decision 2001/500/JHA of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (OJ L 182, 5.7.2001, p. 1) (Okvirna odluka 2001/500/JHA od 26. juna 2001. o pranju novca, identifikaciji, ulaženju u trag, zabrani raspolaganja imovinom, privremenom i trajnom oduzimanju predmeta krivičnog dela i imovinske koristi, OJ L 182, 5.7.2001, str. 1):
<http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001F0500>
- Council Framework Decision 2005/212/JHA of 24 February 2005 on confiscation of crime-related proceeds, instrumentalities and property (OJ L 68, 15.3.2005, p. 49) (Okvirna odluka 2005/212/JHA od 24. februara 2005. o oduzimanju imovinske koristi, predmeta krivičnog dela i imovine proistekle iz izvršenja krivičnog dela, OJ L 68, 15.3.2005, str. 49):
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:068:0049:0051:en:PDF>
- Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence (OJ L 196, 2.8.2003) (Okvirna odluka 2003/577/JHA od 22. jula 2003. o izvršavanju naloga za zamrzavanje imovine ili dokaza u Evropskoj uniji (OJ L 196, 2.8.2003)):
<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003F0577>
- Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders (OJ L 328, 24.11.2006) (Okvirna odluka Saveta 2006/783/JHA od 6. oktobra 2006. godine o primerni načela međusobnog priznavanja naloga za oduzimanje imovine):
<http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32006F0783>
- Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime (L 332/103, 18.12.2007) (Odluka Saveta 2007/845/JHA od 6. decembra 2007. koja se odnosi na saradnju između kancelarija država članica za oduzimanje imovine na polju ulaženja u trag i identifikacije imovinske koristi ili druge imovine proistekle iz izvršenja krivičnog dela (L 332/103, 18.12.2007)):
<http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007D0845>
- Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council

Framework Decision 2005/222/JHA (Direktiva 2013/40/EU Evropskog parlamenta i Saveta od 12. avgusta 2013. o napadima na informacione sisteme i o zameni Okvirne odluke Saveta 2005/222/JHA):

<http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040>

- European Union Directive 2016/1148 on the security of network and information systems ("NIS Directive") of 6 July 2016 (Direktiva 2016/1148 Evropskog parlamenta i Saveta od jula 2016. godine o bezbednosti mrežnih i informacionih sistema ("NIS" direktiva) od 6. jula 2016.):

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG

- EU GENVAL 2012 Final report on fifth round of mutual evaluation – "Financial crime and financial investigations" (Konačni izveštaj EU GENVAL o petoj rundi uzajamne evaluacije - "Finansijski kriminal i finansijske istrage" iz 2012. godine):

<http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012657%202012%20REV%202>

- Draft Final report of the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime", June 2017 (Nacrt konačnog izveštaja o sedmoj rundi uzajamne evaluacije o "Praktičnoj primeni i radu evropskih politika o prevenciji i borbi protiv visokotehnološkog kriminala", jun 2007.):

<http://data.consilium.europa.eu/doc/document/ST-9986-2017-INIT/en/pdf>

7.3 Ujedinjene nacije

- United Nations Convention Against Illicit Traffic In Narcotic Drugs And Psychotropic Substances, Vienna, 19.12.1988 (Konvencija Ujedinjenih nacija protiv nezakonitog prometa opojnih droga i psihotropnih supstanci, Beč, 19.12.1988):

<https://www.unodc.org/unodc/en/treaties/illicit-trafficking.html>

- United Nations Convention Against Transnational Organized Crime, New York, 15.11.2000 (Konvencija Ujedinjenih nacija protiv transnacionalnog organizovanog kriminala, Njujork, 15.11.2000):

<https://www.unodc.org/unodc/en/treaties/CTOC/>

- United Nations Convention Against Corruption, New York, 31.10.2003 (Konvencija Ujedinjenih nacija protiv korupcije, Njujork, 31.10.2003):

<http://legal.un.org/avl/ha/uncc/uncc.html>

7.4 Radna grupa za finansijske mere u borbi protiv pranja novca

- International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, the FATF Recommendations, 2012 (Međunarodni standardi u borbi protiv pranja novca i finansiranja terorizma i širenja oružja za masovno uništenje, Preporuke FATF-a, 2012):

<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>

- Money Laundering Using New Payment Methods, October 2010 (Pranje novca korišćenjem novih metoda plaćanja, oktobar 2010.):
<http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf>
- Virtual Currency Key Definitions and Potential AML/CFT Risks, June 2014 (Glavne definicije virtuelnih valuta i potencijalni rizici od pranja novca i finansiranja terorizma, jun 2014.):
<http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>
- Virtual Currency – Guidance for a risk-based approach, Financial Action Task Force, June 2015 (Virtuelne valute – Uputstvo za pristup baziran na riziku, Radna grupa za finansijske mere u borbi protiv pranja novca, jun 2015.):
<http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>

7.5 Sudska praksa

- - European Court of Human Rights (ECtHR) Judgement in K.U. v. Finland, 2 December 2008, on the obligation of Governments to protect individuals against crime, including through criminal law (Presuda Evropskog suda za ljudska prava (ESLJP) u predmetu K.U. protiv Finske, 2. decembar 2008, o obavezi država da zaštite fizička lica od kriminala, uključujući kroz krivično pravo):
[http://hudoc.echr.coe.int/eng#{%22fulltext%22:\[%22K.U.%20v.%20Finland%22\],%22documentcollectionid%22:\[%22GRANDCHAMBER%22,%22CHAMBER%22\],%22itemid%22:\[%22001-89964%22\]}](http://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22K.U.%20v.%20Finland%22],%22documentcollectionid%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-89964%22]})
- ECtHR case law on Personal Data Protection (Sudska praksa ESLJP o zaštiti ličnih podataka):
http://www.echr.coe.int/Documents/FS_Data_ENG.pdf
- ECtHR case law on New Technologies (Sudska praksa ESLJP o novim tehnologijama):
http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf
- ECtHR case law on Mass Surveillance (Sudska praksa ESLJP o masovnom nadzoru):
http://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf
- Court of Justice of the European Union Judgement in Joined Cases C-293/12 and C-594/12. Digital Rights Ireland and Seitlinger and Others (Presuda Suda pravde Evropske unije u spojenim predmetima C-293/12 i C-594/12. *Digital Rights* Irska i Seitlinger i drugi):
<http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>
- EU Court of Justice of the European Union Judgement in Case C-582/14, 19 October 2016, dynamic IP addresses may qualify as 'personal data' under

EU privacy law (Presuda Suda pravde Evropske unije u predmetu C-582/14, 19. oktobar 2016, dinamičke IP adrese mogu se smatrati 'podacima o ličnosti' na osnovu zakona EU o privatnosti):

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1034974>

- Court of Justice of the European Union Judgement in Case C-264/14, 22 October 2015, "'bitcoin' virtual currency has no other purpose than to be a means of payment and that it is accepted for that purpose by certain operators" (Presuda Suda pravde Evropske unije u predmetu C-264/14 od 22. oktobra 2015, Virtuelna valuta 'bitkoin' nema drugu svrhu osim da bude sredstvo plaćanja i da je za tu svrhu prihvataju određeni operateri):
<http://curia.europa.eu/juris/document/document.jsf?text=&docid=170305&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=160800>
- Supreme Court of Belgium ruling in the case of Belgium vs. Yahoo! (Odluka Vrhovnog suda Belgije u predmetu Belgija protiv Yahoo!):
http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1
- US Court of Appeals ruling in the case of Microsoft vs. United States (Presuda Apelacionog suda SAD u predmetu *Microsoft* protiv SAD):
<http://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412>

7.6 Druga literatura

- Data Retention after the Judgement of the Court of Justice of the European Union, Prof. Dr. Franziska Boehm et al., Munster/Luxembourg, 30. June 2014 (Zadržavanje podataka posle presude Suda pravde Evropske unije), Prof. Dr. Franziska Boehm et al., Munster/Luksemburg, 30. juna 2014.):
http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf
- Encryption a Matter of Human Rights, Amnesty International Report, March 2016 (Šifrovanje kao pitanje ljudskih prava, izveštaj *Amnesty Internationala*, mart 2016.):
http://www.amnestyusa.org/sites/default/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf
- "Brochure: The 6 need-to-knows about Financial Investigation", February 2016 (Brošura: Šest stvari koje treba znati o finansijskoj istrazi, februar 2016.):
<https://english.eu2016.nl/documents/publications/2016/02/10/brochure-the-6-need-to-knows-about-financial-investigation>
- "Needs assessment on tools and methods of financial investigation in the European Union", ECORYS, December 2015 (Procena potreba o sredstvima i metodama finansijskih istraga u Evropskoj uniji, ECORYS, decembar 2015.):
https://www.wodc.nl/binaries/2612-summary_tcm28-74130.pdf
- European Banking Authority Opinion on 'virtual currencies', EBA/Op/2014/08, July 2014 (Mišljenje Evropskog nadzornog tela za bankarstvo o 'virtuelnim valutama', EBA/Op/2014/08, jul 2014.):

<https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>

- An Analysis of Anonymity in Bitcoin Using P2P Network Traffic, Koshy *et al*, Pennsylvania State University (Analiza anonimnosti kod bitcoina kod koga se koristi P2P mrežni saobraćaj, Koshy i dr., Državni univerzitet Pensilvanija): http://fc14.ifca.ai/papers/fc14_submission_71.pdf
- The Internet Organised Crime Threat Assessment (IOCTA) 2016, Europol (Procena pretnji od organizovanog kriminala na internetu (IOCTA) 2016. Europol),: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016>
- The Internet Organised Crime Threat Assessment (IOCTA) 2017 (Procena pretnji od organizovanog kriminala na internetu), Europol: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>