



iPROCEEDS

Project on targeting crime proceeds on the Internet in
South-eastern Europe and Turkey

www.coe.int/cybercrime

Верзија од 21-ви декември, 2017

Курс за обука за судии и обвинители

Напреден курс за претрес, заплена и конфискување приходи од кривични дела на Интернет

Прирачник за самостојна обука

Funded
by the European Union
and the Council of Europe



Implemented
by the Council of Europe

Контакт:

Александер Сегер
Сектор за компјутерски криминал
Генерален директорат за човекови права
и владеење на правото
Совет на Европа,
Стразбур, Франција

Тел: +33-3-9021-4506

Факс: +33-3-9021-5650

е-пошта: alexander.seger@coe.int

Ограничување од одговорност:

Овој технички извештај не ги одразува нужно официјалните ставови на Советот на Европа или донаторот што го финансира овој проект.

Содржина

1 Вовед.....	6
1.1 Цел на курсот.....	8
1.2 Целна група слушатели.....	8
1.3 Резиме на содржината	9
1.3.1 Предизвици на истрагите на Интернет	9
1.3.2 Прекугранични истраги	9
1.3.3 Виртуелни валути.....	9
1.3.4 Практична работа/Примери.....	10
2 Предизвици на истрагите на Интернет	11
2.1 Типологии и перење пари на Интернет	11
2.1.1 Користење Интернет банкарство	11
2.1.2 Користење други финансиски услуги на Интернет	12
2.1.3 Користење Интернет комуникациски услуги.....	14
2.1.4 Непробојно хостирање.....	16
2.1.5 Подземна економија	17
2.2 Откривање на сторителот.....	18
2.2.1 Збирна мрежна адреса (<i>NAT - Network Address Translation</i>)	18
2.2.2 Збирни мрежни адреси кај операторот (<i>CGN - Carrier Grade Network Address Translation</i>)	20
2.2.3 Употреба на анонимизатори	21
2.2.4 Ботнет/малвер/контролирање компјутер од далечина.....	24
2.2.5 Користење отворен, јавен или украден безжичен Интернет	25
2.2.6 Откривање на сопственикот на <i>IP</i> адреса.....	26
2.3 Работа со интернет провајдери.....	27
2.3.1 Вид податоци што се бараат.....	27
2.3.2 Директивата на ЕУ за чување податоци е поништена со одлука на Судот на правдата на ЕУ	28
2.3.3 Домашни интернет провајдери	31
2.4 Меѓународни даватели на услуги	32
2.4.1 Јурисдикција.....	33
2.4.2 Општ став.....	33
2.4.3 Барања за сочувување	33
2.4.4 Итни барања	34
2.4.5 Опсег на барањето	34
2.4.6 Известување на лицето што е предмет на барањето	34
3 Финансиски истраги	36
3.1 Вовед.....	36
3.2 Финансиски истраги и приходи од криминал на Интернет.....	36

3.2.1	Елементи на финансиската истрага	37
3.2.2	Аспекти на компјутерски криминал во финансиската истрага	37
3.2.3	Финансиски истраги во Европската унија	38
4	Прекугранична соработка	41
4.1	Резиме	41
4.1.1	Релевантни мрежи и организации за размена на информации и заемна правна помош	42
4.1.2	Меѓународни правни инструменти	43
4.1.3	Одредби за меѓународна соработка	46
4.2	Оценка на примената на одредбите за меѓународна соработка	48
4.2.1	Оценка за гонењето приходи од криминал	48
4.2.2	Оценка за компјутерски криминал	51
4.3	Користење шаблони и обрасци за заемна правна помош	59
5	Виртуелни валути	61
5.1	Резиме од основниот курс	61
5.2	Вовед во виртуелни валути	62
5.2.1	Повеќе терминологија за виртуелните валути	62
5.2.2	Учесници во виртуелната валута	64
5.2.3	<i>Bitcoin</i>	65
5.3	Ризици од виртуелни валути	67
5.4	Предизвици на истрагите	69
5.4.1	Сознание дека се користеле виртуелни валути	69
5.4.2	Анонимност на трансакцијата	70
5.4.3	Откривање на изворот на средства	70
5.4.4	Повлекување/реализација и конверзија на приходите	71
5.5	Предизвици за замрзнување/заплена	72
5.5.1	Виртуелни валути како приходи од криминал	72
5.5.2	Откривање на постоењето на виртуелна валута	72
5.5.3	Замрзнување/преземање контрола на виртуелна валута	72
5.5.4	Управување со средства	73
6	Практична работа/Примери	74
6.1	Пребарување литература	74
6.2	Пример 1: Разгледување на правната основа за дејство	74
6.3	Пример 2: Разгледување на интеракцијата меѓу УФР и органите на прогонот	77
6.4	Пример 3: Интеракција во случај на компјутерски криминал/перење пари	80
7	Прилог: Список за релевантна литература	82
7.1	Совет на Европа	82
7.2	Европска Унија	83

7.3	Обединети нации.....	85
7.4	Работна група за финансиска акција - <i>FATF</i>	85
7.5	Судска пракса	85
7.6	Други референци.....	86

1 Вовед

Прашањата за компјутерски криминал, електронски докази, приходи од криминал и перење пари засегаат разни институции, а особено, службите за компјутерски криминал, службите за финансиско истражување, управите за финансиско разузнавање (УФР) и обвинителството. Сепак, истрагите за компјутерски криминал ретко ги придружува финансиска истрага и обратно, истрагите за други кривични дела ретко ги придружува истрага за компјутерски криминал. Затоа има потреба од поделотворна меѓуагенциска соработка меѓу сите тие институции, којашто се очекува да има особено силно влијание врз претресот, заплена и конфискувањето на приходи од криминал на Интернет.

Компјутерскиот криминал и тековите на пари од криминал на Интернет не сопираат на географските граници. Затоа, за да работат на овие појави сеопфатно, истражните активности треба да ги минуваат границите и да делуваат во разни јурисдикции. Делотворната меѓународна соработка е клучна и за претрес, заплена и конфискување на приходи од криминал на Интернет. Поврзувањето на следењето приходи од криминал, мерките за спречување перење пари и спречување финансирање тероризам со истрагите за компјутерски криминал и компјутерската форензика нуди дополнителни можности. На пример, привремените мерки за замрзнување имот треба да ги придружуваат барања за итно сочувување електронски докази.¹ Ова е една од причините што Препораката 36 од Работната група за финансиски активности (*Financial Action Task Force - FATF*) предлага спроведување на Конвенцијата од Будимпешта за компјутерски криминал и Варшавската конвенција на Советот на Европа.

Употребата и потпирањето на информатичка технологија се сè поприсутни во општеството, па и нападите и користењето компјутерски системи станаа сè почести. Делата со компјутерски елемент брзо пораснаа, како по бројност, така и по сложеност, но има временски расчекор со изготвувањето делотворни противмерки. Изведувањето на сторителите пред правдата бара доказ за вина вон разумен сомнеж, но доказите изведени од електронски уреди се нестабилни, често нематеријални, и веројатно во друга јурисдикција. Тоа значи дека е од витална важност да има делотворни, правно усогласени и јаки процедури за идентификување, прибирање и сочувување електронски докази. Кривичните постапки сè повеќе вклучуваат компјутерски криминал или електронски докази што се наоѓаат на компјутерски системи или уреди за чување. Тоа важи слично и за приходите од криминал.

Со оглед на тоа што општествата во сиот свет се потпираат на информатичка и комуникациска технологија, судиите и обвинителите треба да се подготвени да работат со компјутерски криминал и електронски докази. Во многу земји, органите на прогонот успеаја да ги зајакнат капацитетите за истражување компјутерски криминал и обезбедување електронски докази, но нема таков акцент на потребите на судиите и обвинителите. Искуството укажува дека судиите и обвинителите најчесто се соочуваат со потешкотии при справувањето со новата реалност на компјутерскиот свет. Затоа се потребни особени заложби за да им се овозможи на судиите и обвинителите да гонат и судат компјутерски криминал и да користат електронски докази, и тоа преку обука, вмрежување и специјализација.

¹ Види став 317, Криминални парични текови на Интернет: методи, трендови и противдејство со повеќе чинители, од истражувачкиот извештај на *MONEYVAL*, март 2012. Достапен на: [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)

Во 2009-та година, Советот на Европа во рамки на Проектот за компјутерски криминал, во соработка со лисабонската мрежа на институции за судска обука и во соработка со повеќе члената работна група, изготви концепт за поддршка на тие заложби.

Целта на концептот е да им помогне на институциите за судска обука да изготват програми за обука за компјутерски криминал и електронски докази за судии и обвинители, и да ја вгради таа обука во редовната почетна и обука на работното место.

Целите на концептот за обука за судии и обвинители се следните:

- Да им се овозможи на институциите за обука да спроведат почетна и обука на работното место за компјутерски криминал според меѓународни стандарди
- Да подготви колку што може повеќе идни и постојни судии и обвинители со основни познавања за компјутерски криминал и електронски докази
- Да обезбеди напредна обука за критичен број судии и обвинители
- Да ги поддржи континуираната специјализација и техничка обука на судиите и обвинителите
- Да придонесе за зајакнати знаења преку вмрежување на судиите и обвинителите
- Да го олесни пристапот до разни иницијативи за обука и мрежи.

Во овој контекст, преку Заедничкиот регионален проект на Европската унија и Советот на Европа *CyberCrime@IPA* (Регионална соработка во кривичното право: Зајакнување на капацитетите за борба против компјутерскиот криминал) се изготвија материјали за обука за компјутерски криминал и електронски докази за употреба од страна на институциите за обука.

Со оглед на успехот и прикажаната вредност на основната и напредна обука за судии и обвинители за компјутерски криминал и електронски докази, преку Заедничкиот проект *iPROCEEDS*² на Европската Унија и Советот на Европа, се изготвија уште два други модули за обука: основен и напреден модул за истражување, претрес, заплена и конфискување приходи од криминал на Интернет.

Општо земено, активностите на криминалците и криминалните организации се наменети да донесат добивка. Според проценките на Обединетите нации, вкупниот износ на приходи од криминал во 2009-та изнесувал приближно 2,1 трилијарда американски долари, или 3,6% од светскиот БДП, но само мал дел од тие средства биле вратени³. Гонењето приходи од криминал преку спроведување финансиска истрага заедно со кривична истрага може да открие и докази за делото перење пари. Перењето пари им овозможува на организациите да извлечат корист од своите нелегални активности и да продолжат со работа.

² Заедничкиот проект на Европската унија и Советот на Европа „Гонење приходи од криминал на Интернет во Југоисточна Европа и Турција“ - *iPROCEEDS* има за цел да го зајакне капацитетот на властите во регионот на *IPA* да претрес, заплена и конфискување приходи од компјутерски криминал и спречување перење пари на Интернет.
<http://www.coe.int/en/web/cybercrime/iproceeds>

³ Меморандум за објаснување на Предлогот за директива на ЕУ за сузбивање перење пари преку кривично право (22.12.2016). Достапно на: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0826>

Без сигурни податоци и истражување, тешко е да се каже колкави се финансиското влијание на компјутерскиот криминал и обемот на поврзаните приходи, но има случаи што покажуваат дека приходите од компјутерски криминал се перат преку сложени шеми што вклучуваат и традиционални и нови начини за плаќање⁴. Сепак, истрагите за компјутерски криминал ретко ги придружува финансиска истрага и обратно, истрагите за други кривични дела ретко ги придружува истрага за компјутерски криминал.

Организираните криминални групи ги кријат и реинвестираат средствата надвор од земјата каде што било сторено кривичното дело од коешто потекнува имотот. Тоа ја усложнува борбата на надлежните органи против прекуграничниот сериозен и организиран криминал. Така, компјутерскиот криминал и тековите на пари од криминал на Интернет не сопираат на географските граници. За да работат на оваа појава сеопфатно, истражните активности треба да ги минуваат границите и да делуваат во разни јурисдикции. Затоа, делотворната меѓународна соработка е клучна и за претрес, заплена и конфискување на приходи од криминал на Интернет.

Концептот за гонење приходи од криминал на Интернет што е изложен во оваа обука ги спојува пристапите на истрагите за компјутерски криминал, финансиските и истрагите за перење пари, сè со цел да се зголемат ефикасноста и успехот на кривичните истраги и кривичните постапки, како од аспект на гонењето на криминалецот, така и од аспект на гонењето на приходите од криминал.

1.1 Цел на курсот

Овој курс е наменет да го олесни континуираното образование на заинтересиран судија или обвинител којшто го има завршено основниот курс за истражување, претрес, заплена и конфискување приходи од криминал на Интернет и сака да го продолжи образованието во оваа област. Целта е да се подобри знаењето на заинтересираниот судија или обвинител во однос на правниот и технички контекст релевантен за приходи од криминал на Интернет. Тоа се постигнува преку детално проучување на одбрани теми од интерес во оваа област.

Курсот покрива подетално одбрани теми од следните области:

- Правните и технички предизвици на истрагите што вклучуваат текови на пари од криминал на Интернет.
- Практични моменти во прекуграничните истраги.
- Криминално користење виртуелни валути и ризиците поврзани со нив.

Тоа е проследено со практична работа, и тоа пребарување литература и примери за слушателот.

1.2 Целна група слушатели

Овој курс е наменет за судии и обвинители што веќе имаат завршено основен курс за претрес, заплена и конфискување приходи од криминал на Интернет. Се очекува корисниците на овој прирачник веќе да ги имаат следните предзнаења:

⁴ Криминални парични текови на Интернет: методи, трендови и противдејство со повеќе чинители, истражувачки извештај на *MONEYVAL*, март 2012.

- Значење на компјутерски криминал и природа на истрагата за компјутерски криминал
- Природа на финансиските истраги
- Делото перење пари и улогата на управата за финансиско разузнавање (УФР)
- Основно техничко знаење, како на пример, природата на *IP* адресата.
- Основно познавање на спецификите на електронските докази.

Сите овие предуслови се исполнуваат со завршување Основниот курс на Советот на Европа за претрес, заплена и конфискување приходи од криминал на Интернет.

1.3 Резиме на содржината

1.3.1 Предизвици на истрагите на Интернет

Во основниот курс имаше вовед во повеќе типологии на текови на пари од криминал на Интернет и перење пари. Во овој дел ќе дискутираме подетално за некои предизвици на истрагите со коишто може да се соочиме кај дел од претходно опишаните типологии. Тоа вклучува дискусија за предизвиците поврзани со идентификување сторител на Интернет, идентификување приходи од криминал на Интернет, како и за предизвиците во работата со домашни, меѓународни и мултинационални интернет провајдери (internet service providers - ISP).

1.3.2 Прекугранични истраги

Концептот за гонење приходи од криминал на Интернет ги спојува пристапите на истрагите за компјутерски криминал, финансиските и истрагите за перење пари, сè со цел да се зголемат ефикасноста и успехот на кривичните истраги и кривичните постапки, како од аспект на гонењето на криминалецот, така и од аспект на гонењето и конфискувањето на приходите од криминал.

Заемната правна помош сè уште се смета за главно средство за извршување судски наредби и прибирање докази во странство, но траењето на постапката претставува значителна пречка. Сепак, користењето заеднички истраги и заеднички истражни тимови може да ја подобри ефикасноста. Соработката и размената на информации меѓу органите на прогонот (полицијата и обвинителите) се неопходни во прекуграничните случаи. Овде важна улога играат релевантните мрежи.

За овој напреден курс, корисно е да се нагласат некои нови наоди за пречките што ги имаат утврдено меѓународните организации при примена на меѓународните стандарди во домашното законодавство и пракса, како и релевантните препораки што може да се употребат за инспирација.

1.3.3 Виртуелни валути

Овој курс се надоврзува на основната терминологија за виртуелни валути за којашто стана збор во воведниот курс, и се работи повеќе на учесниците во екосистемот на виртуелните валути, вклучително и берзи за виртуелни валути, сервиси за паричници и слично. Се опишува како функционира виртуелната валута *Bitcoin* и тоа е проследено со објаснување на ризиците и предизвиците во истрагите со виртуелни валути, како и претресот, заплenuвањето и управувањето со средства.

1.3.4 Практична работа/Примери

За да им помогнеме на слушателите да ги организираат информациите од овој курс во контекст на нивното домашно законодавство, има насочено пребарување литература и неколку примери за да им се овозможи на слушателите во своето слободно време дополнително да истражуваат за темите што се начнати тука.

2 Предизвици на истрагите на Интернет

2.1 Типологии и перење пари на Интернет

Во основниот курс имаше вовед во повеќе типологии на текови на пари од криминал на Интернет и перење пари. Целта на овој дел е да дискутираме подетално за некои предизвици на истрагите со коишто може да се соочиме кај дел од претходно опишаните типологии. Има две крупни и чести прашања за коишто ќе дискутираме поодделно во посебни делови од курсот; предизвиците на истрагата за идентификување сторител на Интернет (в. Дел 2.2.) и мноштвото предизвици сврзани со употребата на виртуелни валути (в. Дел 5).

2.1.1 Користење Интернет банкарство

Неколку типологии обработени во основниот курс претпоставуваат дека криминалецот има пристап до сметка во банка. Тоа особено важи за типологиите електронски трансакции, преземање банкарски сметки и меѓународни преноси. Регулаторните услови за финансиските институции во однос на проверка на клиенти, водење документација и сл. се добро разбрани⁵. Сепак, криминалците се потпираат на опкружувањето на Интернет банкарството, коешто не подразбира контакт лице в лице, да се обидат да ги заобиколат овие контроли⁶. Ако нема потреба од непосреден контакт со клиентот, криминалецот може, на пример, да се претстави како легитимен клиент на банката (на пр. ако украде или користи податоци за најава за Интернет банкарство) на начин што финансиската институција многу потешко може да го препознае.

Има три главни траги што треба да се следат во истрагата за такви случаи:

- Начинот на којшто била компрометирана сметката (на пр. фишинг, заразување со малвер). Докази за тоа може да се обезбедат од сопственикот на сметката, којшто е најверојатно и жртвата.
- Податоци за најава за компрометираната сметка. Овие информации може да ги обезбеди финансиската институција.
- Сметка/и што биле употребени за префрлување на парите од компрометираната сметка. Информациите ги имаат финансиските институции и тие може да помогнат да се откријат инволвираните поединци (мулиња) и да се следат парите за понатамошна заплена.

Понатаму во овој дел ќе дискутираме за некои прашања во истрагата што се усложнуваат преку користење банкарски услуги на Интернет.

Прво, потешко е да се утврди природата на односот, ако тоа воопшто и постои, меѓу сопственикот на сметката и осомничениот. На пример:

1. Дали сопственикот на сметката е свесен за активноста на осомничениот?

⁵ Меѓународни стандарди за сузбивање перење пари и финансирање тероризам и ширење, Препораки на Работната група за финансиска акција (FATF), 2012. Достапни на: <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>

⁶ Извештај на FATF, Перење пари со нови начини на плаќање, октомври 2010. Достапен на: <http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf>

2. Дали осомничениот има директна контрола врз сметката или осомничениот ги диригира активностите на сопственикот на сметката?
3. Дали е можно да се открие лицето кое извршило дадена трансакција на сметката?

Преку овие и многу други прашања, треба да е јасно дека Интернет банкарството, коешто не подразбира контакт лице в лице, го отежнува утврдувањето на фактите во истрагата.

Второ, користењето банкарски услуги на Интернет носи предизвици и за откривање на самата сомнителна активност. Ако осомничениот дојде во некоја експозитура и се обиде да изврши трансакција, барем има можност службеникот да утврди дали активната што се врши е очигледно сомнителна. На Интернет, обработката на трансакциите е главно автоматизирана. Во комбинација со структурирањето на средствата за да се избегнат праговите за пријавување, тоа може да доведе до зголемен ризик да се пропуштат сомнителни трансакции. За да се борат против ова, финансиските институции често користат автоматизиран софтвер за следење трансакции, чијашто функција е да открие трансакции што застрануваат од профилот на трансакции што вообичаено се вршат на дадена сметка.

Некои, но не сите, софтвери за следење измами ја проверуваат и *IP* адресата од којашто наводно се пристапува до дадена сметка на Интернет. На пример, ако од некоја *IP* адреса првпат се пристапува до сметката, тоа може да се употреби да се постави сомнеж дека сметката на Интернет е можеби компрометирана. Сепак, од практичен аспект, финансиските институции имаат тешка задача да одржуваат рамнотежа меѓу откривање и спречување измама од една страна, и немешање во легитимните банкарски активности на глобално мобилните клиенти од друга страна.

Освен тоа, дури и да е компрометирана Интернет сметката на некој клиент, тоа не е секогаш очигледно од *IP* адресата од којашто е извршена најавата. Тоа е така затоа што кога компјутерот на клиентот е заразен со малвер, можно е криминалецот да има контрола врз компјутерот на клиентот. Тоа му овозможува на криминалецот да се најави во сметката на клиентот од *IP* адресата на компјутерот на клиентот, и така да избегне тревога поради најава од невообичаена *IP* адреса.

Трето, се поставува прашањето кои дополнителни докази се потребни за да се покажат активностите на осомничениот и дали тие докази се достапни. *IP* адресите од коишто се пристапило до дадена сметка најверојатно се документирани кај финансиските институции, но не се секогаш непосредно достапни. Може да требаат значителни напори за да се утврди кои *IP* адреси се користени за која најава на која сметка. Тоа се должи на сложеноста на инфраструктурата на Интернет банкарството и особено на тоа што записите може да не се чувани или организирани на начин што овозможува лесен пристап до потребните информации. Згора на тоа, ако и кога ќе се открие употребената *IP* адреса, поврзувањето на осомничениот со таа *IP* адреса е посебен предизвик.

2.1.2 Користење други финансиски услуги на Интернет

Другите (небанкарски) финансиски услуги на Интернет играат улога во неколку типологии од основниот курс. Тоа особено важи за системите за плаќање преку Интернет, купување на Интернет и користењето Интернет платформи за коцкање/тргување. Повторно, природата на односот меѓу услугата и корисникот без лично присуство отвора можност криминалците да ги искористат овие видови услуги.

Во даден момент, на овие услуги ќе им треба некаков контакт со традиционалниот сектор за финансиски услуги. Тоа вообичаено се прави со платежни картички што се користат да се наполни сметка кај давателот на финансиски услуги на Интернет. Кога ќе се префрлат средствата од платежната картичка кај давателот на услуги, природата на интеракцијата меѓу корисникот и давателот на финансиски услуги на Интернет се невидливи за традиционалниот финансиски систем. Затоа се препорачува услугите за плаќање на Интернет да подлежат на регулаторни обврски и надзор⁷. Природата на таа регулатива може да варира во разни јурисдикции.

Да го земеме, на пример, концептот на микро-плаќања⁸. Нема финансиска логика сервисот за плаќање преку Интернет веднаш да го реализира секое микроплаќање од кредитната картичка на корисникот затоа што провизиите би ја изеле добивката што ја има сервисот за плаќање во таа трансакција. Наместо тоа, сервисите за плаќање вообичаено собираат повеќе плаќања наеднаш и поднесуваат еден налог за сета активност на корисникот во даден временски период. Така, сервисите за плаќање прифаќаат извесен ризик за измама, но бидејќи износите во поединечните плаќања се вообичаено многу ниски, вкупните загуби загуби се исто така ниски.

И мобилните оператори некогаш нудат модел за микроплаќања. Во тие случаи, корисникот врши микроплаќања преку телефонот или телефонскиот број, а износите се појавуваат на следната сметка за мобилен на корисникот.

Во овие случаи, за истражителот најважно е да ги расветли природата на нелегалната активност (измами, неовластен пристап), типовите податоци што може да се соберат и од каде, за да се докаже криминалната активност и да се следи паричниот тек.

Во повеќето случаи жртвите дознаваат во подоцнежна фаза за измамите со нивните сметки или кредитни картички. Сепак, давателите на платежни услуги можат да откријат нелегални активности и да ги сочуваат податоците коишто подоцна може да им се предадат на истражителите.

Главните предизвици што произлегуваат од користењето услуги за плаќање преку Интернет се поради тоа што потребните записи вообичаено се наоѓаат во друга јурисдикција. Вклучувањето меѓународни даватели на услуги и постапката за заемна правна помош може значително да ја забават и усложнат истрагата.

Слични проблеми произлегуваат и од користењето платформи што овозможуваат купување преку Интернет. Како што видовме во основниот курс, купувањето стоки или услуги преку Интернет, коишто потоа му се испраќаат на криминалецот или на некое муле, се добар начин да се претворат украдените податоци за плаќање во реална вредност. Во тие случаи, истрагите во целост се потпираат на записите кај платформата за купување и нејзината можност да открие сомнителна активност. Повторно, за повеќето истраги, големите платформи за купување преку Интернет се со седиште во друга јурисдикција. За да се приберат докази од овие организации, треба да се поднесе барање за заемна правна помош до соодветната јурисдикција.

Платформите за коцкање на Интернет исто така претставуваат специфични предизвици коишто главно произлегуваат од разновидната регулатива за овие

⁷ Извештај на FATF, Перење пари со нови начини на плаќање, октомври 2010. Достапен на: <http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf>

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

субјекти низ светот. На пример, во некои јурисдикции коцкањето на Интернет е нелегално, па соработката со операторот на фирма за коцкање на Интернет во тие случаи може да доведе до откривање на субјектите и да донесе правни потешкотии. Во рамките на ЕУ, на пример, 20 земји-членки на ЕУ дозволуваат коцкање на Интернет, а седум не. Некои земји со нова регулатива имаат решено да дозволат или забранат коцкање на Интернет, а други го дозволуваат или забрануваат „пасивно“ со тоа што продолжуваат да применуваат регулатива за конвенционално коцкање, којашто е често многу постара. Од дваесетте земји-членки коишто дозволуваат коцкање на Интернет, тринаесет земји имаат либерализиран пазар, шест земји имаат државен монопол, а една земја има лиценцирано приватен монопол⁹.

2.1.3 Користење Интернет комуникациски услуги

Интернетот е во суштина платформа за комуникација и криминалците користат комуникациски услуги да ја помогнат својата активност. Во контекст на криминалните парични текови на Интернет, комуникациските услуги на Интернет овозможуваат врбување мулиња, комуникација и управување. Криминалците може да користат сервиси како електронска пошта, групен разговор на Интернет, инстант пораки и Интернет телефонија за да си ги организираат активностите.

Може да има технички потешкотии како со откривање на страните во комуникацијата, така и со откривање на суштината на комуникацијата. Со прашањето за откривање осомничени на Интернет ќе се занимаваме поподробно во Дел 2.2.

Последниве неколку години има тренд меѓу давателите на услуги на Интернет да ја гарантираат приватноста на корисниците. Во многу случаи тоа значи зголемена употреба на енкрипција. Генерално земено, енкрипцијата се користи на три начини¹⁰:

- **Енкрипција на цел диск или уред:** Во случај на лаптоп или десктоп, одамна постои технологија за енкриптирање на целата содржина на хард дискот. Исто така, веќе извесно време постои можност на ист начин да се енкриптира меморијата на мобилен уред како смартфон. Околу 2014-та година, технолошките фирми како *Apple* и *Google* почнаа фабрички да ја вклучуваат енкрипцијата на своите смартфони. За дешифрирање и пристап до уредот вообичаено треба лозинка или *PIN*. Законскиот услов за енкрипцијата е да се заштитат личните податоци на сопственикот од губење или кражба на уредот.
- **Енкрипција од точка до точка:** Овој израз се однесува на енкрипција на пораки што се праќаат преку платформа за пораки на начин да може да ги прочитаат единствено испраќачот и примачот на пораките. Многу сервиси за пораки, меѓу кои *iMessage*, *WhatsApp* и *Facebook Messenger* нудат разни варијанти на енкрипција од точка до точка. Во случајот на *iMessage*, на пример, примената на енкрипција од точка до точка значи дека дури ни *Apple*, давателите на услугата, немаат пристап до содржината на пораките.
- **Енкрипција на пренос:** Овој облик на енкрипција се однесува на податоци што се енкриптираат заради пренос меѓу две страни. Денес тоа

⁹ Студија на Европскиот Парламент од Секторот за политики, економска и научна политика, под наслов „Коцкање на интернет, акцент на интегритетот и кодекс на однесување за коцкање“. IP/A/IMCO/FWC/2006-186/C1/SC2. Достапна на: [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 Енкрипција, прашање на човекови права, извештај на Amnesty International, март 2016. Достапен на: <http://www.amnestyusa.org/sites/default/files/encryption-a-matter-of-human-rights-pol-40-3682-2016.pdf>

вообичаено значи енкрипција на Интернет сообраќај. Енкрипцијата на пренос е една од основните безбедносни контроли што ги користи современиот свет на е-трговија и е-банкарство, со тоа што спречува напаѓачот да ја пресретне комуникацијата меѓу клиентот и интернет страницата на банката или интернет страницата за е-трговија.

Во случаи каде што има енкрипција на пренос, сепак има техничка можност за посебни истражни мерки како пресретнување комуникации, со соработка на релевантните страни, како сопственикот на интернет страницата и/или интернет провајдерот. Пристапот до енкриптиран уред или комуникација што е енкриптирана од точка до точка е потежок и често претпоставува пристап до уредот или компјутерот на осомничениот.

ПРИМЕР: APPLE против FBI¹¹

FBI сакале да отклучат *iPhone 5C* што го користел еден од напаѓачите во напад во Сан Бернардино, Калифорнија, во декември 2015, во којшто загинале 14 лица.

На 16-ти февруари 2016, на барање на Министерството за правда на САД, сојузниот судија му наредил на *Apple* да изработи наменска верзија на својот оперативен систем *iOS* којшто ќе им овозможи на истражителите на случајот да ги минат безбедносните елементи на телефонот. Генералниот директор на *Apple*, Тим Кук, реагирал со отворено писмо во коешто стои дека барањето на владата претставува „прекршување на приватноста“ со „грозоморни“ последици. Кук напишал:

„Кога *FBI* го побараа она што го имаме, ние им го дадовме. *Apple* соработуваше со важечките наредби и налози за претрес, вклучително и за случајот Сан Бернардино. Исто така, *Apple* ги стави на располагање своите инженери за консултации со *FBI*, и ги понудивме нашите најдобри идеи за низа истражни алтернативи што им се на располагање... Меѓутоа сега владата на САД ни побара нешто што едноставно го немаме, нешто што сметаме дека е премногу опасно да се направи. Ни побара да направиме таен влез во ајфонот.“

Apple ја обжалил судската наредба и било закажано рочиште во сојузен суд на 22-ри март 2016. Голем број независни стручњаци за технологија, професори по право, технолошки фирми и организации за човекови права го поддржаа ставот на *Apple* по ова прашање. Општоприфатениот став меѓу оние што се противеа на барањето на *FBI*, меѓу кои и *Amnesty International*, е дека ако *Apple* се примора да го измени својот софтвер за да го отвори телефонот, тоа би поставило преседан што би можел да овозможи владата на САД, и потенцијално други влади, да ги принудат технолошките фирми да ја ослабат или на друг начин да ја заобиколат својата енкрипција со оставање таен влез за разузнавачките и другите безбедносни служби.

Во реакција на случајот, високиот комесар за човекови права на ОН рече: „Успешен случај против *Apple* во САД ќе постави преседан што ќе им оневозможи на *Apple* и која било друга меѓународна информатичка фирма да ја заштитат приватноста на клиентите каде било во светот. Тоа може да биде подарок за авторитарните режими, како и за криминалните хакери. Веќе имало низа организирани заложби од властите

¹¹ *Ibid.*

во други земји да ги принудат информатичките и комуникациските фирми како *Google* и *Blackberry* да ги изложат своите клиенти на масовно следење.”

На 28-ми март, *FBI* изјавиле дека го отвориле ајфонот со помош на трето лице и Министерството за правда го повлекло предметот.¹²

2.1.4 Непробојно хостирање

Условите за користење на повеќето сервиси за Интернет и хостирање интернет страници забрануваат незаконски активности на нивните мрежи или сервиси. Затоа тие вообичаено соработуваат со барања за информации од властите, како и барања за отстранување незаконски домени или интернет страници.

Непробојно хостирање е термин за сервисите за хостирање што не соработуваат со барања од властите за информации или бришење интернет страници. Тие сервиси географски се често во други земји (во однос на земјата каде што се одвива истрагата). Во повеќето случаи фирмите со непробојно хостирање се бранат со тоа што немаат правна одговорност за криминалните активности што ги вршат нивните клиенти преку нивната инфраструктура.

Тие сервиси често се користат за ширење нелегален материјал, за праќање спам, како командни и контролни сервери за малвер, и за други облици криминална инфраструктура^{13, 14, 15}.

Интернет страниците за фишинг чијашто мета се клиенти на сервиси за интернет банкарство (и други сервиси) често користат непробојно хостирање за да постават интернет страници што личат на легитимните сајтови. Тие често се бришат или блокираат поради неовластена употреба на трговската марка на финансиската институција. Интернет страниците што не ја користат трговската марка на легитимна организација потешко се бришат.

Законите во некои земји поддржуваат блокирање од страна на домашните провајдери, преку разни техники за филтрирање, на содржина што се знае дека е нелегална¹⁶.

Информациите за корисниците и услугите коишто фирмите со непробојно хостирање им ги даваат на властите не се многу корисни за истрагата затоа што деталите за тие лица се најчесто лажни. Сепак, начинот на плаќање за изнајмените услуги може да претставува важна трага што може да помогне во откривањето на изворот на криминална активност.

¹² *FBI* вели дека го пробила телефонот на терористот без помош од *Apple*, *CNN*, 29-ти март 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=

¹⁵ https://en.wikipedia.org/wiki/Bulletproof_hosting

¹⁶ *T-CY* (2006)04 - Зајакнување на соработката меѓу органите на прогонот и приватниот сектор, примери како приватниот сектор блокирал интернет страници со детска порнографија, февруари 2006. Достапно на: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e6ed1>

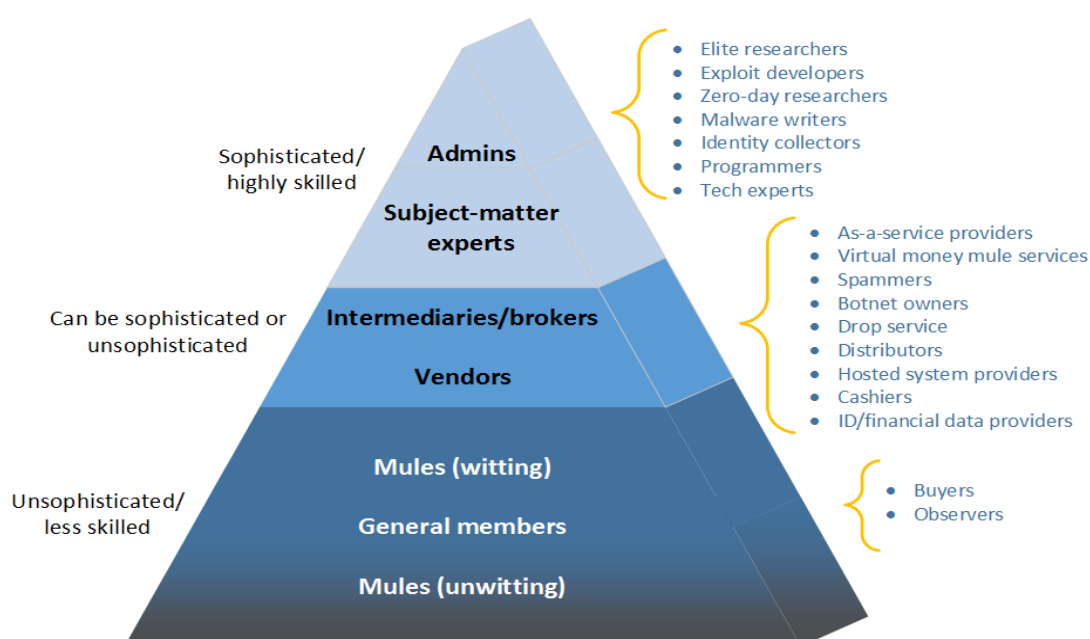
Законски гледано, има и потешкотии да се утврди јурисдикцијата за извршените незаконски активности бидејќи може да се вплеткани повеќе извори, одредишта и други места/субјекти за координација.

Во земјите каде што има непробојно хостирање, во текот на истрагата може да се користи пресретнување. Тоа помага да се приберат информации за изворот, одредиштето и природата на криминалната активност.

2.1.5 Подземна економија

Подземна економија се сервисите што ги користат криминалците за да тргуваат едни со други со услуги и информации. Има многу примери на подземни форуми, како *Silk Road* и *DarkMarket*.¹⁷

Подземната економија организациски е структурирана за вршење кривични дела. Тие често користат деловен модел по име *Crime-as-a-Service*.



Слика 1: Учесници во криминалниот деловен модел на Даркнетот

Слика Емракт обука

Подземните форуми специјализирани за измама со кредитни картички и продажба на украдени податоци од кредитни картички често се нарекуваат картични форуми.

Тие форуми најчесто се отворни само за ограничени „клиенти“ со лозинки или преку други безбедносни мерки.

Истрагите за овие форуми често се долги и сложени; агенции со прикриен идентитет често бавно се инфилтрираат во форумите и доаѓаат до водечки позиции од каде што добиваат пристап до информации што овозможуваат да се поднесе обвинение против администраторите и операторите на форумот. Тоа што се потребни толку сложени истраги значи дека за повеќето истраги не е можно да се инфилтрираат во подземен

¹⁷ За да најдете информации за пазарите на Даркнетот, видете: <https://www.deepdotweb.com/>

форум за да приберат докази за поединечно кривично дело на Интернет или поединечна истрага за перење пари.

Исто така, од перспектива на истрагата, важно е да има релевантни закони што ги инкриминираат овие незаконски активности, што дозволуваат спроведување активности со прикриен идентитет, и што овозможуваат прибраните докази да се допуштат на суд. Таквата истрага е мешавина од класични истражни техники и интернет техники.

Во случаи каде што сопствениците или операторите на познат подземан форум се присутни во домашната јурисдикција, или каде што подземниот форум се хостира во домашната јурисдикција, како основа за кривична постапка може да се искористат релевантните материјални одредби во домашното законодавство. Релевантните одредби зависат од спецификите на случајот, но може да одговарат, на пример, на член 6 од Конвенцијата од Будимпешта.

ПРАШАЊА ЗА РАЗМИСЛУВАЊЕ

1. **Кои услови треба да се исполнети за да се одобри следење сомнителна сметка?**
2. **Каква рамнотежа е потребна за да се заштитат интересите на потенцијално невинно трето лице чијашто сметка е компромитирана?**
3. **Кои одредби постојат во вашето домашно законодавство за да се принуди некој осомничен да декриптира енкриптиран уред или датотека?**
4. **Кои мерки се достапни во вашето домашно законодавство за да се принуди домашен провајдер да блокира или филтрира нелегална содржина?**

2.2 Откривање на сторителот

Потсетете се од основниот курс дека клучната карактеристика што се користи за откривање на осомничен на Интернет е неговата *IP* адреса.

Целта на овој дел е подетално да се опишат некои практични предизвици што се јавуваат при обидите да се поврзе дадена *IP* адреса со некој поединец. Со други зборови, во ситуации кога некоја криминална активност на Интернет може да се поврзе со дадена *IP* адреса и сакате да го откриете лицето коешто ја имало таа *IP* адреса во моментот кога се случил криминалот на Интернет.

Прашањето може да биде и обратно, кога имате вистински осомничен и сакате да ја откриете *IP* адресата што тоа лице ја користело на Интернет. Оваа ситуација во многу погледи е полесна за работа и може да се употребат традиционални истражни техники (на пр. посебни истражни мерки).

2.2.1 Збирна мрежна адреса (*NAT - Network Address Translation*)

За да се комуницира на Интернет, потребни се појдовна и целна *IP* адреса. Порано (пред воведувањето на *NAT*) на секој компјутер требаше да му се додели единствена

IP адреса. Проблемот е што *IP* адресите се доделуваа неефикасно и поради тоа ги нема доволно. Долгорочното решение на недостатокот од *IP* адреси е воведувањето нова верзија на *IP*, верзија 6, којашто има многу поголем број достапни *IP* адреса. Во меѓувреме, се користат неколку техники за да се продолжи времетраењето на *IP* верзија 4, меѓу кои и *NAT*.

Некои низи *IP* адреси се резервирани. Тие не се за користење на Интернет. Наместо тоа, тие се наменети за употреба во приватни мрежи, на пример во внатрешни деловни низи. Резервираните низи се следните:

1. 10.0.0.0 – 10.255.255.255
 - a. Сите *IP* адреси што почнуваат со „10.“
2. 192.168.0.0 – 192.168.255.255
 - a. Сите *IP* адреси што почнуваат со „192.168.“
3. 172.16.0.0 – 172.31.255.255
 - a. Сите *IP* адреси што почнуваат со „172.“ проследени со број меѓу „16“ и „31“.
 - b. Оваа резервирана низа се користи поретко од другите две.

Најчестата примена на *NAT* е кога една организација доделува *IP* адреси од некоја од овие низи на сите свои службени компјутери. Потоа, кога еден од компјутерите во мрежата сака да комуницира со *IP* адреса на Интернет, нивниот рутер ја заменува внатрешната *IP* адреса со адреса од помала низа вистински *IP* на Интернет. Во повеќето случаи, резултатот на оваа постапка е што сите *IP* податоци од сите компјутери во службената мрежа на фирмата на Интернет изгледаат како да доаѓаат од само една *IP* адреса.

Употребата на *NAT* е многу честа, па и сеприсутна, во домашните интернет мрежи. Тоа значи дека некој корисник во домот може да користи повеќе уреди на домашната мрежа, но интернет провајдерот треба да ѝ додели на конекцијата само една *IP* адреса.

На Интернет има повеќе одлични технички описи како функционира *NAT*^{18, 19, 20}. Ако некој е заинтересиран, по потреба, може да погледне некои од референците за повеќе информации.

Вреди да се размисли за импликациите од употребата на *NAT* во истрагите на Интернет. Можеби ќе се открие јавната *IP* адреса што се користела во текот на дадена криминална активност, но ако се употреби *NAT*, таа *IP* адреса може да ја претставува интернет активната на повеќе независни корисници. Затоа е потребен дополнителен истражен чекор да се утврди врската меѓу Интернет активната и компјутерот на поединечен корисник со употреба на резервирана *IP* адреса зад *NAT* рутерот.

Постои мала можност организацијата што користи *NAT* да има запис за дојдовниот и појдовниот сообраќај преку коишто може да се утврди која внатрешна *IP* адреса била одговорна за извесен сообраќај што е предмет на истрагата. Сепак, тоа е малку веројатно. Освен тоа, кај малите канцеларии или домашни корисници коишто користат стандардни опрема и услуги обезбедени од нивниот провајдер, такви записи не се достапни.

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

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

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

Затоа истрагата мора да се потпира на алтернативен механизам за да ги поврзе осомничената *IP* адреса со даден компјутер. Може да има извесни карактеристики на сообраќајот што ќе овозможат да се открие внатрешната *IP* адреса. На пример, некои апликации во самиот сообраќај ја вклучуваат внатрешната *IP* адреса на компјутерот што учествува во сообраќајот. А, може да има и други препознатливи карактеристики, освен *IP* адресата, коишто може да се употребат. Тоа се кориснички имиња, и-мејл адреси, технички информации за изворниот уред и слично. Преку темелна анализа од страна на вештак, можеби е можно на тој начин да се открие изворот на сообраќајот.

Ако криминалната активност се одвива во реално време, може да се применат посебни истражни мерки за да се пресретне појдовниот сообраќај и на тој начин да се открие внатрешниот компјутер. Во таков случај, потребна е соработка од организацијата за да се открие соодветната локација во нејзината мрежа и да се монтира уред за следење. Тоа вообичаено подразбира соработка со информатичкиот персонал, и мора да се има предвид дека нема начин да се знае однапред дали осомничениот е некој од информатичкиот персонал којшто тогаш би станал свесен за истрагата.

Севкупно земено, *NAT* претставува предизвик при повзуваето на извесна *IP* адреса со активната на вистинскиот корисник. За да се заврши истрагата и да се открие осомничениот вообичаено ќе требаат дополнителни информации (освен *IP* адреса) прибрани со анализа на интернет активната или, пак, со дополнителни истражни мерки.

2.2.2 Збирни мрежни адреси кај операторот (*CGN - Carrier Grade Network Address Translation*)

Со користењето збирни мрежни адреси кај операторот, т.е. *CGN*, се поставуваат дополнителни предизвици. *CGN* е техника преку којашто интернет провајдерот може да користи *NAT* да преведе голем број претплатнички *IP* адреси во помал број вистински *IP* адреси на Интернет.

Во овие случаи, *CGN* значи дека освен оној *NAT* што се случува кога сообраќајот оди од мала канцеларија или дом кон мрежата на интернет провајдерот, може да има уште еден *NAT* во мрежата на интернет провајдерот пред сообраќајот да се препрати на Интернет^{21, 22}.

CGN се разликува од обичниот *NAT* од претходната точка бидејќи не само што приватната (внатрешна) *IP* адреса е заменета со јавна (надворешна) *IP* адреса, туку и приватниот (внатрешен) број на *TCP/IP* порта е заменет со јавен (надворешен) број на порта. Во суштина, *CGN* ги мапира *TCP* или *UDP* сесиите од просторот на внатрешна адреса во просторот на надворешна адреса. Со оваа техника *CGN* решава некои од проблемите со обем кај обичниот *NAT*, но создава проблем од истражна гледна точка; имено, во најголем број случаи, организациите ја заведуваат *IP* адресата од која што добиваат конекција, но не и бројот на дојдовната порта. *CGN* овозможува илјадници корисници да бидат под иста *IP* адреса, самата *IP* адреса не е доволна да се поврзе активната со даден корисник.

Затоа, под претпоставка дека бројот на портата не е достапен, ќе бидат потребни други дополнителни информации (освен *IP* адресата) прибрани од анализата на интернет активната за да се открие осомничениот.

²¹ Дополнителни информации и линкови има на: https://en.wikipedia.org/wiki/Carrier-grade_NAT.

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

Europol во Оценката за закана од организиран криминал на Интернет од 2016-та, дава неколку препораки за справување со истражните предизвици што ги поставува *CGN*, и тоа²³:

- За да може да се поврзе поединечен краен корисник со *IP* адреса на мрежа што користи *CGN*, органите за спроведување на законот треба да побараат дополнителни информации од давателите на услуги преку правен процес:
- Појдовна и целна *IP* адреса
- Број на појдовна порта
- Точно време на конекција (до секунда).
- Сепак, нехармонизираните стандардни обврски за чување податоци во Европа значат дека давателите на услуги за содржини, Интернет и хостирање податоци немаат правна обврска да ги чуваат тие информации, што значи дека и темелно барање од некој орган на прогонот не би донел корисни информации од давателот на услуги.
- Потребни се регулаторни/законодавни промени за да се обезбеди давателите на услуги за содржина да можат системски да ги чуваат потребните дополнителни податоци (изворна порта) што им се потребни на органите за да ги откријат крајните корисници.
- Или, пак, може да се изготват практични решенија преку соработка меѓу електронските даватели на услуги и органите на прогонот. Некои електронски даватели на услуги во Европа ги чуваат релевантните информации (изворна порта). Еден пан-европски портал би можел да води ажуриран список на давателите на услуги и список со лица за контакт за обраќање во случај некоја истрага да затаи поради *CGN*.

2.2.3 Употреба на анонимизатори

Анонимизатор е инструмент што се обидува да ја направи активноста на Интернет невозможна за следење. Тој е посредник меѓу компјутерот и остатокот од Интернетот и пристапува до Интернет во име на корисникот, а ги крие идентификациските информации на корисникот.

Анонимизаторите се делат во две главни категории:

- **Анонимизатори за конкретен протокол:** Тие функционираат само за еден конкретен протокол. Пример за тоа е анонимен препраќач на мејлови или анонимизирачки прокси сервер.
- **Анонимизатори независни од протоколот:** Тие функционираат така што создаваат *IP* тунел преку којшто се пренасочува сиот кориснички сообраќај. Од аспект на примачот корисник, *IP* сообраќајот ќе изгледа како да доаѓа од некој друг, а не од оригиналниот испраќач. Еден таков пример е *Tor* (претходно познат како *The Onion Router*).

Подолу ќе разгледаме неколку примери.

²³ Оценка на заканата од организиран криминал на Интернет (*IOCTA*) 2016, *Europol*. Достапно на: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016> и 2017 на: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>

Во истрагите каде што има употреба на анонимизатор и давателот на услуги не сака или не може да даде поддршка за истрагата, може да требаат алтернативни (нетехнички) истражни мерки за да се напредува.

ПРИМЕР: АНОНИМЕН ПРЕПРАКАЧ НА МЕЈЛ

Анонимниот препраќач служи да прими пораки, да ги отстрани информациите за идентификација и да ги препрати на саканиот примач на начин што примачот не може да види од каде првично дошле пораките.

Има неколку начини да се направи тоа:

- **Псевдонимни препраќачи;** ја отстрануваат и-мејл адресата на испраќачот, му доделуваат псевдоним на испраќачот и ја испраќаат пораката до саканиот примач.
- Примачот ќе може да одговори со испраќање мејл до псевдонимот и препраќачот ќе го препрати тој мејл до првичниот испраќач.
- **Сајферпанк препраќачи (или Тип I):** Се испраќа пораката до примачот и се отстранува адресата на испраќачот. Примачот не може да одговори на мејлови испратени преку овој тип на препраќач. Испраќачот на пораката вообичаено ја поднесува пораката до препраќачот во енкриптиран облик. Препраќачот ја декриптира и ја испраќа до примачот. Овие типови препраќачи не водат записи за преносите.
- **Миксмастер препраќачи (или Тип II):** Испраќачот составува мејл и го испраќа до препраќачот. Пораката се препраќа повеќе пати преку *peer-to-peer* мрежа на препраќачи и на крај доаѓа до примачот. Примачот не може да одговори на овој мејл, освен ако во содржината на мејлот е дадена адреса за одговор. За да се користи миксмастер препраќач, на компјутерот на корисникот треба да се инсталира посебен софтвер.
- **Миксминион препраќачи (или Тип III):** Тие се слични на миксмастер препраќачите, но со решени извесни технички прашања. Главно е тоа што е можно примачот да одговори преку мрежата препраќачи без да знае кој бил испраќачот.

Можно е да се направи верига од повеќе препраќачи за ниту препраќачите да не знаат кој ја праќа пораката. Може и да се употреби интернет интерфејс кон препраќачот, наместо стандардна или наменска и-мејл апликација инсталирана на компјутерот на корисникот.

ПРИМЕР: АНОНИМИЗИРАЧКИ ПРОКСИ СЕРВЕР

Анонимизирачкиот прокси сервер се обидува да ја анонимизира пребарувачката активност на Интернет на корисникот. Анонимизирачкиот прокси сервер вообичаено прифаќа барања од корисниците и ги проследува. Од аспект на серверот што го добива барањето, барањето изгледа како да

доаѓа од анонимизирачки прокси сервер. Освен ако анонимизирачкиот прокси сервер има достапни записи да се поврзат појдовните барања со конкретни појдовни *IP* адреси, тоа нема да биде можно од анализата на *IP* податоците.

Користењето прокси сервер на Интернет е поддржано во речиси секој стандарден пребарувач затоа што има многу легитимни причини зошто корисниците би сакале да конфигурираат прокси сервер²⁴. Користењето на овие услуги вообичаено бара не повеќе од конфигурирање мал број опции во софтверот на еден стандарден пребарувач.

Сепак, содржината на самиот интернет сообраќај може сè уште да содржи детали што би можеле да помогнат да се открие осомничениот. На пример, ако осомничениот се најави на некоја интернет страница преку анонимизирачки прокси сервер, *IP* адресата од којашто се најавил може да не е достапна, ама анализата на интернет сообраќајот може да ги открие корисничкото име и/или лозинката што ги користел.

ПРИМЕР: *TOR* (ПРЕТХОДНО *THE ONION ROUTER*)

Tor е софтверска алатка што го насочува Интернет сообраќајот преку мрежа од компјутери во сопственост на доброволци што работи бесплатно, а се состои од неколку илјади релеи. Целта е да се отежни следењето на Интернет активноста до првичниот корисник.

Насочувањето се врши преку повеќе слоеви енкрипција, а потоа сообраќајот се препраќа преку повеќе безредно одбрани релеи. Секој релеј дешифрира слој од енкрипцијата и со тоа само се открива следниот слој од преносот и таму се праќаат преостанатите енкриптирани податоци. Во последниот релеј се дешифрираат највнатрешните енкриптирани податоци и тие се праќаат до целното одредиште без да се открие, ниту да се знае појдовната *IP* адреса. Така насочувањето на комуникацијата делумно се крие од секој скок во мрежата *Tor*, што значи дека нема ниту една точка во којашто партнерите во комуникацијата може се откријат на начин што ги идентификува или се потпира на изворот и одредиштето на комуникацијата.

Корисникот на мрежата *Tor* инсталира посебен софтвер на компјутерот што го пресретнува сиот или дел од излезниот мрежен сообраќај и го препраќа во мрежата *Tor* наместо директно кон саканото одредиште. Кога сообраќајот ќе влезе во мрежата *Tor*, тој се праќа од рутер до рутер сè додека дојде до последниот рутер во мрежата (каде што се одвива последната дешифриција и се открива првичниот сообраќај). Овој рутер се нарекува излезна точка. Од аспект на одредиштето, изгледа дека сообраќајот потекнува од излезната

²⁴ На пример, некоја организација може да сака да ги блокира вработените да посетуваат извесни интернет страници во текот на работното време. Во такви случаи, може да се конфигурира прокси сервер на компјутерот на вработениот и директниот пристап до Интернет е блокиран со *firewall* заштита. Така сите барања минуваат преку прокси серверот и тој е во положба да ги блокира или одобри според политиката на организацијата.

точка.

Од описот горе се чини дека мрежата *Tor* дозволува само анонимизација на комуникација започната од клиентот. Но *Tor* поддржува и водење сервери преку мрежата *Tor* на начин што *IP* адресата на серверот не е видлива за корисниците на тој сервер. За да се постигне тоа, на серверите им се доделуваат посебни адреси, познати како *onion*-адреси, и до нив може да се пристапи преку мрежата *Tor* на начин што не ја открива локацијата на серверот²⁵. Скриен сервис покажува дека постои и потоа мрежата *Tor* воспоставува спојни точки на децентрализиран начин за да овозможи конекции меѓу скриени сервиси и корисници без никој од нив да го знае идентитетот на другиот.

Иако непосредното идентификување на *IP* адресата на осомничен што ја користи мрежата *Tor* е речиси невозможно, има специјалистички техники за откривање други информации што може да помогнат во истрагата. На пример, можно е погрешна конфигурација на серверот да открие информации за вистинскиот извор на скриениот сервис. Страниците со грешки што ги даваат многу обични Интернет сервери (на пример, пораката за грешка што му се прикажува на корисникот кога неговото барање ќе предизвика грешка) ја вклучуваат *IP* адресата на серверот, што значи дека со појавување на грешка на серверот, може да се открие *IP* адресата.

2.2.4 Ботнет/малвер/контролирање компјутер од далечина

Кога компјутерот на некое лице е заразен со малвер, можно е на компјутерот да е инсталиран софтвер што му овозможува на некој осомничен да го контролира компјутерот и да го користи за криминална активност. Меѓу другото, осомничениот може да инсталира прокси сервер на компромитираниот компјутер и да го препраќа сиот свој сообраќај преку тој прокси сервер.

Во тие случаи, Интернет сообраќајот поврзан со криминалната активност ќе изгледа како да доаѓа од *IP* адресата на невиното лице. Сепак, има технички мерки со коишто можеби ќе се открие вистинскиот извор на сообраќајот. На пример, со следење на *IP* сообраќајот до и од компромитираниот компјутер, можно е да се открие *IP* адресата на осомничениот којшто го контролира компјутерот. Тоа е најверојатно во случаи кога криминалецот компромитирал мал број компјутери и комуницира со нив поединечно.

Сепак, не треба да се потцени сложеноста на командно-контролната (*C&C*) инфраструктура преку која криминалците управуваат со мрежи компромитирани компјутери. Операторите на ботнети користат многу техники за да си ја прикријат активност^{26, 27} и да му овозможат на својот контролен сообраќај да минува преку *firewall* заштита²⁸.

²⁵ Повеќе детали за работењето на скриени сервиси има на:
<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/>

Анализата на компјутерот на лицето може да открие присуство на малвер, со што би се потврдило дека компјутерот може да бил контролиран од далечина од страна на трето лице. Сепак, не е невозможно некој осомничен намерно да го зарази својот компјутер со малвер за да се потпира на одбрана дека не бил одговорен за дејствата извршени на компјутерот или со компјутерот. Затоа предизвикот „да се стави осомничениот пред тастатурата“ може да бара и други нетехнички мерки, како на пример набљудување, за да се утврди со сигурност кое лице извршило кои дејства, или пак да се исклучи можноста некое лице да ги извршило криминалните дела.

Истражителите се соочуваат со предизвици и во однос на начинот на известување на корисникот за заразувањето и соодветните инструменти за отстранување на малверот. Мигот кога сопствениците се известуваат за заразените компјутери е важен и за тоа се решава врз основа на статусот на истрагата. Отстранувањето на малверот од заразените машини се прави на начин да се избегне нелегален пристап или пресретнување на комуникацијата без соодветно одобрување/овластување.

2.2.5 Користење отворен, јавен или украден безжичен Интернет

Отворените безжични мрежи се поставени за да му овозможат секому да се поврзе на нив и да користи Интернет. Отворените безжични мрежи претставуваат ризик за криминална употреба на поврзаноста на Интернет на начин што нивната активност ќе може да се поврзе единствено со изворот на отворениот безжичен Интернет. Некои, но не и сите, отворени безжични мрежи бараат регистрација и/или водат записи.

Сличен проблем се јавува во случаи кога напаѓачот може да ја погоди или пробие лозинката за безжичен Интернет или затворената безжична мрежа. Најчестото сценарио со користењето хакиран пристап до безжичен Интернет и/или украден пристап до безжичен Интернет е напаѓачот да се паркира во кола пред некоја деловна просторија и да го користи нивниот безжичен Интернет за да врши криминална активност. Во такви случаи, тешко е веројатно дека ќе има достапни какви било идентификациски записи за поврзувањето на безжичната мрежа (особено за мали фирми) и ќе нема начин да се продолжи истрагата за да се најде осомничениот. Можно е осомничениот да ја користи истата локација во повеќе наврати и во тој случај набљудувањето на локацијата може да доведе до откривање на осомничениот.

Друг проблем се јавува затоа што има многу локации со релативно анонимен интернет пристап, како библиотеки, универзитети или интернет-кафулиња.

Главната карактеристика на овој проблем е можноста осомничениот да добие речиси анонимен пристап до Интернет преку интернет врска, а некогаш и компјутери што се во сопственост на трето лице.

Слично како и кај претходната точка, анализата на мрежата на лицето може да открие присуство на отворен безжичен Интернет, со што би се потврдило тврдењето дека безжичниот Интернет може да го користело трето лице. Сепак, не е невозможно некој осомничен намерно да го остави својот безжичен Интернет отворен за да се потпира на одбрана дека не бил одговорен за дејствата извршени преку безжичниот Интернет. Повторно, може да се потребни други нетехнички мерки, како на пример набљудување, за да се утврди со сигурност кое лице извршило кои дејства, или пак да се исклучи можноста некое лице да ги извршило криминалните дела.

Пресретнувањето Интернет е уште една техника што може да се употреби да се утврди вмешаноста на разни лица во криминалните активности.

2.2.6 Откривање на сопственикот на IP адреса

WHOIS е бесплатен сервис што дава информации за сопственикот на некој домен, вклучително и име, презиме и податоци за контакт.

Според *ICANN*²⁹, светскиот администратор на домени, „Сервисот на *WHOIS* е бесплатен и јавен именик со контактите и техничките информации за впишаните регистриранти на домените. Секој што сака да знае кој стои зад некој Интернет домен може да ги побара тие информации преку *WHOIS*.

Податоците се прибираат и се ставаат на располагање од страна на регистраторите според условите од нивните договори со *ICANN*. *WHOIS* не е единствена централна база на податоци. Регистрациските податоци се чуваат на разни локации и ги водат повеќе регистри и регистратори. Тие поставуваат свои правила за сервисот *WHOIS*, во согласност со минималните правила утврдени во нивните договори со *ICANN*.“

WHOIS се користи да се открие кому му е доделена конкретна IP адреса. проблемот е што базата на податоци на *WHOIS* не е секогаш точна. Регистраторите треба периодично да комуницираат со оние што се регистрирани кај нив, меѓутоа од нив не се бара да ја потврдат точноста на податоците што ги дава регистраторот. Тоа е проблем особено кога треба да се открие кој е сопственик на конкретен домен.

Во случајот на IP адреси, има уште еден системски проблем - под-доделување IP адреси³⁰. Се јавува проблем ако некој провајдер кому му е доделена низа IP адреси потоа дава дел од тие IP адреси на под-провајдер, но не води точни или ажурни информации за тоа кој користи кои IP адреси. Провајдерот може нередовно да го пријавува под-доделувањето во регистарот на базата на податоци на *WHOIS*, што значи дека базата на *WHOIS* нема да содржи точни информации за крајниот контролор на IP адресата што е во прашање.

Податоците од *WHOIS* може да се сметаат како конкретен облик податоци за претплатникот, коишто се јавно достапни на Интернет со неограничен пристап. Сепак, со оглед на стапувањето во сила на Општата регулатива на ЕУ за заштита на податоци (*GDPR*) на 25-ти мај 2018, пристапот до *WHOIS* ќе се смени за да се обезбеди усогласеност со *GDPR*.³¹

ПРАШАЊА ЗА РАЗМИСЛУВАЊЕ

1. Дали наредбата за следње IP адреса може да се формулира така што нема да влијае на правата на невини трети лица?
2. Како може да се утврди дали активната поврзана со дадена IP адреса била извршена од страна имателот на таа IP адреса или далечински бидејќи неговиот компјутер бил заразен со малвер?

²⁹ Интернет корпорација за зададени имиња и броеви, меѓународна организација одговорна за дефинирање на политиките поврзани договори со интернет регистри и регистратори.

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

³¹ За повеќе за пристап до *WHOIS* видете: <https://www.icann.org/news/blog/data-protection-privacy-update-seeking-input-on-proposed-interim-model-for-gdpr-compliance>

3. Кои услови треба се задоволат за да се добие налог со којшто ќе се овозможи да се открие IP адресата што ја користи вистинскиот осомничен?
4. Кои услови треба да се задоволат за да се добие налог со којшто ќе се овозможи да се открие вистинскиот имател на IP адресата што е употребена за криминална активност?

2.3 Работа со интернет провајдери

2.3.1 Вид податоци што се бараат

За целите на кривичната истрага може да требаат три вида податоци:

- Информации за претплатникот
- Податоци за сообраќајот
- Податоци за содржината.

Во многу јурисдикции условите за пристап до информации за претплатникот вообичаено се пониски од оние за податоци за сообраќајот, а најстрогите правила се однесуваат на податоците за содржината. Видот податоци што се бараат секако влијае на природата на барањето што треба да се поднесе до меѓународен давател на услуги за да се добие пристап до податоците. Некои, но не и сите, меѓународни даватели на услуги имаат облик на брза доброволна соработка преку која може да се дадат информации за претплатникот додека се чека формално-правниот процес.

2.3.1.1 Информации за претплатникот

Информациите за претплатникот се најчесто бараните информации во домашните и кривичните истраги и без тие информации често е невозможно да се продолжи со истрагата³². Поимот „информации за претплатникот“ е дефиниран во Член 18.3 од Конвенцијата од Будимпешта на следниот начин:

„За целите на овој член, поимот „информации за претплатникот“ ги означува сите информации во облик на компјутерски податоци или какви било други податоци што ги има давателот на услуги, во врска со претплатниците на неговите услуги, освен податоци за сообраќајот или содржината, преку кои може да се утврди:

- a. видот користена комуникациска услуга, техничките предуслови за неа и периодот на услугата;
- b. Идентитетот или географската адреса на претплатникот, телефонски или друг број за контакт, информации за испраќање сметки и плаќање, коишто се достапни според договорот или аранжманот за услуги;
- c. Секои други информации на местото каде што е монтирана комуникациската опрема коишто се достапни според договорот или аранжманот за услуги.“

Информациите за претплатникот веројатно се чуваат кај давателите на услуги, иако информациите може фактички да се зачувани на сервери во други јурисдикции. Затоа може да не е секогаш јасно кому да му се упати барањето за информации за претплатникот.

³² Извештај на T-CY за правилата за прибавување информации за претплатникот усвоен на 12-тата пленарна седница, 2-3-ти декември 2014. Достапен на: <https://rm.coe.int/16802e7ad1>

2.3.1.2 Податоци за сообраќајот

Датотеките со записи каде што се заведуваат активностите на оперативниот систем на компјутерот, или друг софтвер, или комуникацијата меѓу компјутери, се клучни за случаи со компјутерски криминал и може да бидат подеднакво важни во случаи со приходи од криминал на Интернет. „Податоци за сообраќај“ во член 1.г. од Конвенцијата од Будимпешта се дефинирани на следниот начин:

„Податоци за сообраќајот претставуваат сите компјутерски податоци во врска со комуникација по пат на компјутерски систем, изведени од компјутерски систем којшто претставува дел од синџирот на комуникација, и каде што се гледаат појдовната точка на комуникацијата, целта, патеката, времето, датумот, обемот, времетраењето или видот на дадената услуга.“

2.3.1.3 Податоци за содржината

И, на крај, податците за содржината честопати се потребни во кривичните истраги. Според став 209 од Толкувањето на Конвенцијата од Будимпешта:

„Податоците за содржината не се дефинирани во Конвенцијата, туку ја означуваат комуникациската содржина на комуникацијата; т.е. значењето или намената на комуникацијата, или пораката или информациите што се пренесуваат со комуникацијата (освен податоци за сообраќајот).“

Треба да се направи разлика и меѓу „зачувани“ податоци за содржината коишто се достапни на компјутерски систем и „идни“ податоци за содржината коишто сè уште не се достапни и треба да се прибават, на пример, преку пресретнување комуникации. Пресретнувањето може да го изврши по судски налог или полицијата или специјализирано тело, и тоа директно, или со помош на давателот на услуги. Нивната употреба често е ограничена на сериозни дела.

2.3.2 Директивата на ЕУ за чување податоци е поништена со одлука на Судот на правдата на ЕУ

Како што видовме погоре, откривањето на сторителите во компјутерскиот свет многу пати зависи од пристапот до податоци што ги чуваат приватни интернет провајдери. Врската меѓу една IP адреса со податоците на едно лице (претплатник на IP адреса, и-мејл, или профил на Facebook) и интеракцијата на осомничениот со други можни осомничени (податоци за сообраќај), па дури и содржината на таа интеракција се суштински дел во откривањето на сторителот, другите осомничени и обезбедувањето докази за делото.

Сето тоа е можно единствено ако приватната фирма ги чува потребните податоци (податоци за претплатникот, сообраќајот и/или содржината). Правната обврска за чување податоци за целите на спроведување на законот е оспорена пред Судот на правдата на Европската унија³³. Во одлуката во споените предмети C-93/12 и C-594/12 (*Digital Rights Ireland* и *Seitlinger* и други), Директивата 2006/24/EЗ за чување податоци е прогласена за неважечка³⁴. Оваа одлука доведе до поништување на

³³ 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*. Available at:

<http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>

³⁴ Директива 2006/24/EЗ од 15-ти март 2006 за чување податоци создадени или обработени во врска со давање јавно достапни електронски комуникациски услуги или јавни комуникациски мрежи, со којашто се изменув и дополнува Директивата 2002/58/EЗ. (Невалидна)

релевантното домашно законодавство во некои земји на ЕУ каде што имаше обврска за провајдерите да ги чуваат податоците за сообраќај извесен период што варираше од 6 месеци до 2 години.

Резултатот е дека интернет провајдерите не се веќе обврзани да ги чуваат податоците за сообраќај заради истраги за сериозен криминал во периодот што претходно се барал со домашното законодавство, и ги чуваат податоците единствено за периодот што е неопходен за изготвување сметки или друга комерцијална употреба. Во пракса, тоа значи 1-3 месеци. ЕУ сè уште нема усвоено нов правен инструмент и многу држави сè уште ги дефинираат соодветните правни решенија за решавање на правните ситуации. Се чини дека претставува посебен предизвик да се реши очекувањето на Судот да не се покријат, на општ начин, сите поединци, сите средства за електронска комуникација и сите податоци за сообраќај без никакво разликување, ограничување или исклучок за борбата против сериозен криминал.

Еден од можните пристапи може да биде да се регулира наредбата за прибавување за чување податоци (за сообраќај) откако ќе се издаде правното барање за ограничен временски период.

Бидејќи причините за дерогација се засноваат на ставот на судот дека директивата ги надминува границите на принципот на пропорционалност затоа што сериозно се меша во основните права на почитување на приватниот живот и заштита на лични податоци, одлуката може да им влијае и на земјите вон ЕУ, особено ако домашното законодавство се оспорува пред домашните уставни судови или во случај на поединечни тужби до Европскиот суд за човекови права поради прекршување на Член 8 од Конвенцијата за човекови права.

Затоа главните елементи од одлуката на Судот може да се релевантни за домашните законодавци. Судот се произнел дека директивата сериозно се меша во основните права на почитување на приватниот живот и заштита на личните податоци. Исто така, веројатно е дека кај засегнатите лица тоа ќе доведе до чувство дека приватниот живот им е предмет на постојано набљудување.

Судот забележал дека директивата не ја регулира содржината на комуникацијата и дека чувањето податоци заради нивно евентуално предавање на надлежните домашни власти вистински ја задоволува целта на општиот интерес, т.е. борбата против сериозниот криминал и, на крај, јавната безбедност. Сепак, законодавецот ги надминал границите што ги наметнува почитувањето на принципот на пропорционалност, и се забележува дека разгледувањето на дискрецијата на законодавецот треба да биде строго.

Иако чувањето податоци што го бара директивата може да се смета дека е соодветно за постигнување на нејзината цел, широкото и особено сериозно мешање на директивата во основните права на почитување на приватниот живот и заштита на личните податоци ги надминува границите што ги наметнува принципот на пропорционалност бидејќи:

- Не е доволно ограничена за да се обезбеди мешањето да е во рамките на она што е строго неопходно,

- Ги покрива, на општ начин, сите поединци, сите средства за електронска комуникација и сите податоци за сообраќај без никакво разликување, ограничување или исклучок за борбата против сериозен криминал,
- Нема објективен критериум за надлежните домашни власти да имаат пристап до податоците и да може да ги користат единствено за спречување, откривање или кривично гонење дела што може да се смета дека се доволно сериозни за да оправдаат такво мешање. Упатува просто на „сериозен криминал“,
- Пристапот до податоците не зависи од претходно разгледување од страна на суд или независно административно тело,
- Наметнува период за чување од најмалку шест месеци, без да направи каква било разлика меѓу категориите податоци врз основа на засегнатите лица или можната корисност на податоците,
- Периодот е поставен меѓу најмалку шест и најмногу 24 месеци, но нема објективни критериуми за периодот на чување да се ограничи на она што е строго неопходно,
- Нема доволно заштитни мерки за да се обезбеди делотворна заштита на податоците од ризикот од злоупотреба,
- Не се обезбедува неповратно уништување на податоците на крајот на нивниот период за чување.

За повеќе информации за влијанието на одлуката, Франциска Бем и Марк Д. Кол имаат укажано на некои од релевантните аспекти во нивната статија „Чување податоци по пресудата на Судот на правдата на Европската унија од 30-ти јуни 2014“³⁵. Тие нагласуваат дека изјавите на Судот не само што упатуваат на самиот случај на директивата, туку и воспоставуваат општи принципи за слични мерки за чување податоци. Тие принципи ги опфаќаат следните точки:

- Прибирањето, чувањето и преносот на податоци поодделно претставуваат прекршување на Член 7 и 8 и бараат строг тест за неопходност и пропорционалност.
- Судот јасно го одбива општото чување податоци за несомнителни лица, како и неодредениот, па дури и долгиот период за чување на податоците.
- Судот гледа чувствителен проблем дека податоците што првично биле прибрани за други цели може подоцна да се употребат од органите на прогонот. За таа цел е потребна врска меѓу заканата за јавната безбедност и сочуваните податоци.
- Потребната врска значително влијае на односот меѓу приватните и јавните актери. Органите на прогонот имаат право на пристап до податоци собрани за други цели единствено во конкретни случаи.
- Судот изрично бара делотворни процедурални правила како независен надзор и контрола на пристапот.
- Прибирањето и примената на податоци за целите на органите на прогонот вклучува ризик од стигматизација што произлегува од вклучувањето на податоците во бази на податоци на органите на прогонот. Овој ризик треба да се има предвид кога се разгледуваат други постојни или планирани

³⁵ Чување податоци по пресудата на Судот на правдата на Европската унија, проф. д-р Франциска Бем и други, Мунстер/Луксембург, 30-ти јуни 2014. Достапно на: http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf

мерки за чување податоци на ниво на органи на прогон и на ниво на земји-членки.

За да се справи со прашањата што ги покренува пресудата на Судот на правдата, на 29-ти ноември 2016, Обединетото Кралство го донесе Законот за истражни овластувања од 2016. Меѓу другите важни техники, тој им задава обврска на интернет провајдерите да ги чуваат „податоците за врската“ 12 месеци. Ова е послаб облик на мешање одошто да се чуваат сите податоци од пребарувањето и намената е да се испочитуваат ставовите на Судот за непропорционалното мешање. Се создаваат и нови овластувања што овозможуваат, преку овластување со налог, диригирано следење и чување на пребарувањата на осомничениот и слично.

2.3.3 Домашни интернет провајдери

Податоците што ги чуваат интернет провајдерите се важни за откривање на сторителот и неговите соучесници, нивната врска во време и простор, и за доказите за содржината на комуникацијата (содржина на и-мејл, објави на социјални мрежи како *Facebook*).

Обврските на интернет провајдерите се уредуваат со домашни одредби за чување податоци (за сообраќај) и условите за пристап и користење на тие податоци заради кривични истраги. Податоците може да се категоризираат како податоци за претплатникот, сообраќајот и содржината.

Податоците за претплатникот се смета дека се помалку чувствителни и нападни во однос на приватноста отколку податоците за сообраќај и содржина. Тие се најчесто бараните информации во домашните и меѓународните кривични истраги во врска со компјутерски криминал и електронски докази. Без овие информации често е невозможно да продолжи истрагата.

Податоците за претплатникот вообичаено ги чуваат приватни интернет провајдери и тие може да се добијат преку наредба за прибавување од полиција или обвинител. Но во случај на динамични *IP* адреси, многу земји бараат судски налог бидејќи станува збор и за некои податоци за сообраќај. Во повеќето земји се бара судска наредба за: пристап до податоци за сообраќај (за прашањето на чување податоци видете во претходната точка); наредба за зачувување (да се чуваат податоци за сообраќај и понатаму); следење податоци за сообраќај; и пристап до податоци за содржина и особено за пресретнување комуникации (ова последново се смета за најнападно и затоа подлежи на конкретни заштитни мерки, услови и на принципот на пропорционалност).

Освен правните услови, важни се и практичните и технички аранжмани за пренос на податоци меѓу интернет провајдерите и органите за спроведување на законот, особено во случај на следење и пренесување податоци во живо, што овозможува брза обработка на податоци.

Друга област на соработка меѓу органите за спроведување на законот и интернет провајдерите е прашањето на блокирање и отстранување интернет страници во случај на кривично дело или криминална содржина. Во овој контекст најчесто се спомнува материјал со детска порнографија, но може да бидат релевантни и други облици, како говор на омраза и јавно провоцирање на терористички чин или прекршување на права од интелектуална сопственост. Иако за таква мерка вообичаено е потребен судски налог, се поттикнува „доброволно“ дејство на сопственикот или уредникот на

интернет страницата поради прекршување на интерниот кодекс на однесување. Таквиот пристап е најефикасен, особено во случај на дело *prima facie* (како порнографски материјал), но може да доведе до загриженост за можно мешање во слободата на говор, како што стои во студијата на Советот на Европа за филтрирање, блокирање и отстранување нелегална содржина на Интернет од 2016-та година³⁶.

ПРАШАЊА ЗА РАЗМИСЛУВАЊЕ

1. Што значи поимот „информации за претплатникот“?
2. Што значи поимот „податоци за сообраќајот“?
3. Што значи поимот „податоци за содржината“?
4. Кои се импликациите од одлуката на Судот на правдата за чување податоци во однос на откривањето на вистинскиот осомничен од IP адреса поврзана со криминална активност?

2.4 Меѓународни даватели на услуги

Во случаи со приходи од криминал на Интернет, исто како и во многу кривични истраги за компјутерски криминал, клучните докази се наоѓаат кај организации од приватниот сектор како *Facebook, Google, Microsoft, Twitter, Yahoo!* и други. Затоа соработката меѓу надлежните власти и овие меѓународни даватели на услуги е суштинска за обезбедување електронски докази. Не е можно ваков прирачник да даде информации за сите различни меѓународни даватели на услуги со коишто ќе треба да работи читателот; на интернет страниците на давателот на услуги вообичаено стојат детали за постапката за барања од органите на прогонот. Затоа, направивме напор да ги категоризираме клучните аспекти на политиките за прогон кај меѓународните даватели на услуги.

Целта е да понудиме рамка во којашто може да се разгледува како во иднина да се работи со даден давател на услуги. Понатаму, тоа ќе помогне и да се појаснат факторите што меѓународните даватели на услуги ги земаат предвид кога разгледуваат нови барања за прогон, а со тоа и факторите што треба да се имаат предвид кога се поднесува барање до давателот на услуги за да се максимизира можноста за успешен исход.

Групата за докази во Облакот (*Cloud Evidence Group - CEG*) има подготвено опширен документ за пристапот на органите на прогонот до податоци во рацете на меѓународни даватели на услуги³⁷. Ќе се занимаваме подетално со повеќе интересни аспекти во главата **Error! Reference source not found.** Еве некои од нив:

- CEG заклучи дека заемната правна помош останува главно средство за прибавување електронски докази од странски јурисдикции за примена во

³⁶ Студија на Советот на Европа за филтрирање, блокирање и отстранување нелегална содржина на интернет, јуни 2016. Достапна на: <https://www.coe.int/en/web/cybercrime/-/study-on-filtering-blocking-and-take-down-of-illegal-content-on-the-internet>

³⁷ T-CY (2016)5 - Кривично-правен пристап до електронски докази во Облакот: Препораки за разгледување од T-CY, Конечен извештај, 16-ти септември 2016. Достапно на: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>

домашната кривична постапка. Тоа особено важи за податоци за содржината.

- Пристапот до податоци за претплатникот е помалку нападен и треба да се олесни. Член 18 за домашната наредба за прибавување треба да се користи и за меѓународни интернет провајдери што работат на територијата на една земја - подготвена е нацрт Насока бр. 10 за наредби за прибавување информации за претплатникот.
- Се уважува директната соработка на интернет провајдерите од САД со странски органи на прогонот, имајќи го предвид и зголемувањето на барањата за заемна правна помош.
- CEG предлага да се размисли за изготвување дополнителен протокол за да се решат некои постојни предизвици; имено, да се олесни режимот за пристап до податоци за претплатникот и да се овозможи директен пристап до интернет провајдерите под извесни услови.

2.4.1 Јурисдикција

За кривично-правните власти често не е очигледно во која јурисдикција се чуваат бараните податоци и/или кој правен режим важи за податоците³⁸. Давателот на услуги може да има седиште во една јурисдикција, да применува правен режим од втора јурисдикција, а податоците да се чуваат во трета јурисдикција. Ако јурисдикцијата се одредува со локацијата на податоците, можно е давателот на услуги да не ја знае веднаш локацијата на податоците. Дури и да е позната локацијата на податоците, не е јасно кои правила важат за законски пристап од страна на кривично-правните власти. Може да се каже дека јурисдикцијата може да ја одредат локацијата на седиштето на давателот на услуги, или на неговата подружница, или локацијата на податоците, или правото на земјата каде што осомничениот се претплатил на услугата, или локацијата или државјанството на осомничениот³⁹.

2.4.2 Општ став

Во сите случаи (освен итни барања, како што ќе видиме подолу), треба да се следи постапката за заемна правна помош за да се добие пристап до податоци за содржината.

Во врска со податоците за претплатникот, меѓународните интернет провајдери се делат во две категории; оние што одговараат на правни барања од јурисдикции вон САД и оние што бараат суд од САД да им достави барање врз основа на договор за заемна правна помош.

2.4.3 Барања за сочувување

Некои даватели на услуги прифаќаат барања за сочувување и ги сочувуваат податоците извесен период (вообичаено околу 90 дена) додека дојде формално-правната документација. Ако се бара зачувување подолго од 90 дена, на давателот на услуги треба да му се испрати писмо за продолжување на рокот пред истекот на 90-дневниот период.

³⁸ Дискусија изготвена од Групата за докази во Облак при T-CY, Кривично-правен пристап до податоци во Облакот: предизвици, мај 2015. Достапно на: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59>

³⁹ T-CY (2016)5 - Кривично-правен пристап до електронски докази во Облакот: Препораки за разгледување од T-CY, Конечен извештај, 16-ти септември 2016. Достапно на: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>

2.4.4 Итни барања

Во случаи со непосреден ризик од повреда, смрт или сериозни физички повреди, повеќето меѓународни даватели на услуги соработуваат со барања за информации од органите на прогонот кога може да се покаже дека давателот на услуги има информации што може да се неопходни да се спречи повредата, смртта или сериозната физичка повреда. Еден практичен предизвик овде, којшто го нагласуваме и понатаму во овој курс⁴⁰, е дека многу земји немаат законодавство што овозможува обелоденување податоци на домашните кривично-правни власти во итни ситуации. Важно е што САД имаат таква одредба, којашто им овозможува на меѓународните даватели на услуги со седиште во САД да одговорат на итни барања, но во случаи кога давателот на услуги нема седиште во САД, или мал број други земји, правната основа за обелоденувањето може да претставува дополнителен практичен предизвик.

2.4.5 Опсег на барањето

Повеќето меѓународни даватели на услуги ќе одбијат барања за информации со премногу широк опсег. Вообичаено не се дава дефиниција за прифатлив опсег, туку само се вели: „премногу широките или нејасни барања нема да се обработат“. Затоа, за да има најголема можност за успешен одговор, барањата треба да се срочат со што е можно потесен опсег и да упатуваат, кога е тоа можно, на профили со соодветниот уникатен идентификатор што се користи на дадената платформа.

Не е секогаш очигледно кој е уникатниот идентификатор што го користи некоја платформа. Во многу случаи, но не секогаш, доволни се корисничкото име и/или и-мејл адресата поврзана со даден профил.

2.4.6 Известување на лицето што е предмет на барањето

Во многу случаи, кога се добива барање од органите на прогонот во однос на корисник на меѓународен давател на услуги, политиката на давателот на услуги е да го информира лицето што е предмет на барањето за постоењето на барањето. Тоа се прави, освен ако известувањето е забрането со закон или судска наредба.

Затоа, ако известувањето на лицето може да ја загрози истрагата, наредбата што е основа за барањето за информации од давателот на услуги треба да вклучува и забрана да се информира лицето што е предмет на барањето.

Згора на тоа, некои даватели на услуги укажуваат дека ако некое барање од органите на прогонот им открие прекршување на нивните услови за користење, може да преземат дејство да се спречи понатамошното прекршување, вклучително и дејства што може да го известат корисникот дека давателот на услуги е свесен за таквото однесување.

ПРАШАЊА ЗА РАЗМИСЛУВАЊЕ

1. Зошто е важно засебно да му се нареди на давателот на услуги да ги зачува податоците што се бараат во кривична постапка, додека се чека формално-правната документација за обелоденување докази?

⁴⁰ Види Дел 4.2.2.2.2

2. Кои услови треба да се исполнети за наредбата до давателот на услуги што го принудува да обелодени информации во однос на негов корисник да може да вклучи и клаузула да се спречи давателот на услуги да го извести (директно или индиректно) лицето што е предмет на барањето?
3. Кои алтернативи се достапни во сценарио каде што се знае дека профил кај меѓународен давател на услуги е поврзан со криминална активност во вашата јурисдикција, но не е можно без да се добијат информации од давателот на услуги да се знае дали сопственикот на тој профил е присутен во вашата јурисдикција или не?
4. Имајќи го предвид траењето на постапката за заемна правна помош, дали и кои алтернативи се достапни за да се забрза пристапот до податоци за содржината што се кај меѓународен давател на услуги?

3 Финансиски истраги

3.1 Вовед

Концептот за гонење приходи од криминал на Интернет ги спојува пристапите на истрагите за компјутерски криминал, финансиските и истрагите за перење пари, сè со цел да се зголемат ефикасноста и успехот на кривичните истраги и кривичните постапки, како од аспект на гонењето на криминалецот, така и од аспект на гонењето и конфискувањето приходите од криминал.

Прирачникот за основниот курс содржи основни и детални објаснувања за финансиската истрага, вклучително и дефинирање на нејзините опсег и елементи. Накусо ќе продискутираме за дефиницијата за финансиска истрага, како и нејзините елементи и некои специфики поврзани со криминалот на Интернет, вклучително и истрагата за компјутерски криминал, а ќе се осврнеме подетално на најновите нешта во поимот за финансиска истрага во ЕУ.

3.2 Финансиски истраги и приходи од криминал на Интернет

„Финансиска истрага“ може да има неколку значења, од истрага за финансиски криминал до истрага за даночни цели, на пример. Меѓународните правни инструменти не даваат дефиниција за финансиска истрага, но во рамките на замрзнување и конфискување приходи од криминал, може да се употреби како пример описната дефиниција што ја дава Работната група за финансиски активности (*Financial Action Task Force - FATF*).

Треба да се забележи и дека поимот „финансиска истрага“ може да вклучува истрага за гонење приходи од криминал во рамки на кривичната постапка, но и во (одделна) граѓанска (*in rem*) постапка. Треба да се забележи и дека финансиската истрага може, но не мора нужно да се совпадне со истрага за перење пари.

Финансиската истрага е метод на истражување и треба да се спроведува паралелно со кривичната истрага за дело што донело приходи, па дури и во судската фаза, со главна (но не и единствена) намера да се најдат и замрзнат приходите од криминал со цел тие на крај да се конфискуваат.

FATF ја има дефинирано финансиската истрага како испитување на финансиските работи поврзани со криминална активност⁴¹, и тоа со следните цели:

- Да се открие обемот на криминалните мрежи или степенот на криминалитет
- Да се откријат и најдат приходите од криминал, терористичките средства или кои било други средства што се или може да станат предмет на конфискување
- Да се подготват докази што може да се употребат во кривичната постапка.

Бидејќи добивката од криминал најчесто е барем делумно легализирана и повторно употребена во легалната економија, финансиската истрага може да се поврзе и/или

⁴¹ *FATF* (2012), Толкување на Препорака 30, став 2.

Видете и: Извештај на *FATF* за оперативни прашања. Водич за финансиски истраги, 2012.

да доведе до истрага за перење пари. Финансиската истрага може да доведе до сомнежи за кривичното дело перење пари, или пак кога управата за финансиско разузнавање (УФР) анализира сомнителни трансакции или го истражува кривичното дело перење пари, приходите од предикатното дело може да станат предмет на конфискување (како предмет на делото перење пари).

3.2.1 Елементи на финансиската истрага

Финансиската истрага најдобро се дефинира преку дефинирање на нејзините елементи⁴² и утврдување на меѓународните и домашните правни одредби што треба да се применат во праксата.

Како што е дадено во основниот курс, елементите на финансиската истрага се:

1. Откривање на кривичното дело и сторителот (паралелно со кривичната истрага)
2. Утврдување на (вредноста на) приходите од криминал
3. Утврдување на имотот што може да се конфискува
4. Наредба за замрзнување - привремени мерки за обезбедување на конфискувањето.

Резултатот на финансиската истрага и евентуално на наредбата за замрзнување би бил конфискување на приходите од криминал.

3.2.2 Аспекти на компјутерски криминал во финансиската истрага

Како што дискутиравме во детали во основниот курс, четирите елементи на финансиската истрага може да се применат и во истраги за компјутерски криминал и/или истраги за криминал на Интернет, што вклучува и приходи од криминал на Интернет.

Треба да се имаат предвид некои специфики во врска со истрагата на криминал на Интернет:

- Кој е сторителот и каде се доказите за делото?
 - Ова се однесува на прашањето на откривање на осомничениот преку *IP* адреса, пристап до податоци за претплатникот, електронската комуникација или социјалните мрежи, и потенцијално податоци за сообраќајот и содржината; соработка со интернет провајдери, домашни и меѓународни; поднесување барања за зачувување податоци, и судски наредби за заплена и прибавување електронски докази.
- Што се тоа приходи од криминал?
 - Ова прашање е поврзано со средства и платни системи како е-пари, виртуелни валути (на пример, биткоиини) и банкарски плаќања преку Интернет; банкарски сметки во странство; повеќекратни трансакции од различен тип, можеби и структурирани за да се скријат изворите на средствата; типологии на перење пари.
- Што може да се конфискува/имотот на осомничениот?
 - Кога се разгледуваат паричните текови на Интернет, постои прашањето на јурисдикција. Жртвите и сторителите често не се во истата земја. Треба да се размисли за пристапот да се конфискуваат приходите од компјутерски криминал, и тоа преку финансиска или

⁴² За повеќе детали видете во прирачникот од основниот курс (1.1.3).

истрага за перење пари. Вниманието и целта треба во најмала мера да се насочат на непосредните приходи од криминал (платено изнудување или измамнички трансакции) и на замрзнувањето на средствата во откриените банкарски сметки користени за кривично дело (изнудување на Интернет, компјутерска измама).

- Важноста во истрагите за компјутерски криминал да се води и паралелна финансиска истрага за да се откријат приходите (банкарски сметки и паричен тек, преноси на виртуелни валути) и постојниот имот на сторителот.
- Наредба за замрзнување
 - Брзото дејствување е клучно во случаи со е-банкарство и општо со Интернет. Можно решение е да се бара делото перење пари и да се употребат овластувањата и меѓународните врски на управата за финансиско разузнавање. Брзо потоа треба да следат судската наредба и заемната правна помош. Треба да се размисли да се употреби каналот на *INTERPOL* за заемна правна помош, Варшавската конвенција и дополнителните можности на Конвенцијата од Будимпешта, билатералните договори и реципроцитетот.
- Конфискување
 - Во меѓународните предмети се појавуваат прашања за заемна правна помош во однос на разните разните режими за конфискување и делење средства.

3.2.3 Финансиски истраги во Европската унија

Холандското претседателство со ЕУ во 2016-та година го посочи гонењето приходи од криминал и финансиските истраги како еден од своите приоритети. Беше изложена анализа на потребите за инструменти и методи за финансиски истраги во Европската унија, како и „шесте главни елементи во финансиските истраги“⁴³.

Анализата на потребите⁴⁴ нагласи дека:

- **Финансиски истраги може да се применат за кое било дело што носи приходи:** тоа не е ограничено на борбата со финансискиот/стопански криминал, вклучително и перење пари, ниту на прибавување докази главно за враќање средства.
- **Финансиски истраги може да се водат во сите фази на кривичните истраги и судските постапки:** од откривање на криминалитет, разузнавачки активности, прибирање докази (градење случај), па сè до обвинение, осудување и конфискување средства.

„Шесте главни елементи во финансиските истраги“ нагласија и дека поради тоа што финансиската добивка е најчесто главниот мотив за извршување кривични дела, приходите се трошат на стоки и често се перат во стопанството преку легитимни фирми и помагачи. Финансиската истрага е дополнителен истражен инструмент што им е на располагање на органите на прогонот и таа може да се примени за главните

⁴³ „Брошура: Шест главни елементи за финансиската истрага“, февруари 2016. Достапно на: <https://english.eu2016.nl/documents/publications/2016/02/10/brochure-the-6-need-to-knows-about-financial-investigation>

⁴⁴ Оценка на потребите за инструменти и методи за финансиска истрага во Европската унија, ECORYS, декември 2015. Достапно на: https://www.wodc.nl/binaries/2612-summary_tcm28-74130.pdf

поединци од една криминална организација да се стават зад решетки и да им се одземат парите и средствата. Ако главните лица се лишат од финансии, тогаш им е многу тешко да продолжат со криминалните активности. Тоа ја прави финансиската истрага многу делотворен инструмент во сузбивањето организиран криминал и тероризам.

„Главните елементи“ го нагласуваат и следното:

- **Финансиската истрага може да се примени на секој вид криминал:** финансиската истрага може и треба да се примени на сите видови сериозен и организиран криминал, како на пример трговија и шверц со луѓе, измама, шверц со дрога и оружје, и тероризам. Честа е заблудата дека финансиската истрага е ограничена на борба против стопански криминал како измама, даночни дела, корупција или перење пари.
- **Финансиска истрага во текот на целата кривична постапка:** идеално, финансиските истраги се применуваат во сите фази од кривичната истрага и судската постапка. Од проактивно откривање кривично дело или криминални мрежи, до истражување случај и градење доказен материјал, па сè до обвинението и осудувањето на сторителите и конфискувањето на средствата. Сепак, во многу случаи, финансиските истражители се вклучуваат во кривичната истрага дури во крајната фаза за да ги најдат, откријат и конфискуваат приходите од криминал. Тоа е пропуштена можност. Финансиската истрага треба да почне што е можно порано.
- **Широката финансиска свесност е од клучна важност:** потребна е финансиска свесност на сите нивоа на системот за прогон - од основна финансиска свесност во полициската работа во заедницата, па сè до високо специјализирана форензичка и сметководствена стручност што е потребна да се разоткрие „корпоративната маска“ зад комплексните прекугранични структури за перење пари. Важно е кривичните истражители да бидат свесни за потребата да се приберат финансиски докази на местото на делото и да побараат специјалистичка финансиска стручност кога е тоа потребно. Освен тоа, финансиската стручност кај обвинителите и судиите е клучна за да се разберат и оценат документите што ги подготвуваат финансиските истражители.
- **Прекуграничната соработка е клучна за успехот на финансиските истраги:** истражителите треба да се запознаат и со начините за неформална размена на информации (*CARIN, Europol, INTERPOL*) при водењето истраги, и со формалните, како на пример барања за заемна правна помош.
- **Важноста на интердисциплинарната соработка:** кога јавните органи вклучени во финансиски истраги, како на пример органите на прогонот, јавните обвинители, управите за финансиско разузнавање и даночните власти ја спојуваат својата стручност, соработуваат и споделуваат информации, тогаш се добиваат најдобри резултати. Освен тоа, сè повеќе се зголемува свесноста и желбата дека приватните страни, како на пример банките, агенциите за недвижности и другите професионални даватели на услуги, можат и да треба да дадат значен придонес во финансиските истраги.

1. Дали има практични или правни пречки за финансиската истрага да се води паралелно со истрагата за компјутерски криминал?
2. Дали има практични или правни пречки да се откријат приходи од криминал што се чуваат на Интернет или виртуелно?
3. Во кој момент во кривичната постапка (истрага, судска итн.) може да се започне финансиска истрага?
4. Кои услови треба да се задоволат пред да се даде наредба за замрзнување имот?

4 Прекугранична соработка

4.1 Резиме

Интернетот, покрај позитивните аспекти, нуди и можности за злоупотреба од страна на криминалци коишто можат да делуваат на речиси невидливи начини, брзо и анонимно, да ги кријат идентитетот, доказите и трагите од добивката од криминал. Оваа карактеристика претставува предизвик за органите за прогон.

Важно е да се препознаат придобивките од разните можности за меѓународна соработка преку спојување на трите аспекти на истрагата за приходи од криминал на Интернет: истрага за компјутерски криминал, паралелна финансиска истрага и истрага за перење пари⁴⁵. Советот на Европа, Варшавската конвенција и Конвенцијата од Будимпешта се важни инструменти за справување со овие аспекти.

Основниот курс содржи презентација на главните аспекти на меѓународната соработка, како на пример предностите на комбинирање начини на меѓународна соработка во областа на компјутерскиот криминал и електронските докази, како и финансиските истраги и спречување и истражување перење пари, разликување меѓународна соработка за размена на (оперативни) информации од заемна правна помош заради докази, релевантни меѓународни мрежи и организации за размена на информации, релевантни одредби од Варшавската и Конвенцијата од Будимпешта итн.

Истовремено, треба да се имаат предвид низа предизвици во однос на меѓународната соработка и особено заемната правна помош.

Варшавската и Конвенцијата од Будимпешта воведуваат начини на меѓународна соработка што се применуваат при комбинирање паралелна кривична истрага (за компјутерски криминал) со финансиска истрага. Сепак, меѓународната соработка се соочува со конкретни правни и практични предизвици поврзани со секој од договорите, поради практични околности, како на пример природата на електронските докази, технологијата на Облак, но и откривање на приходи од криминал, заплена и конфискување имот во странство, имајќи ги предвид различните правила за конфискување и законските разлики меѓу страните. Овие предизвици се утврдени и со нив се справуваат релевантните тела на Советот на Европа, како на пример Советот на стручњаци за функционирањето на европските конвенции за соработка во кривични прашања (PC-OC) и Комитетот за Конвенцијата за компјутерски криминал (T-CY).

Кога се комбинираат аспектите на истрага за компјутерски криминал, финансиска истрага, и спречување и истрага за перење пари, корисно е да се биде свесен за сите тие различни аспекти, за придобивките и предизвиците што произлегуваат од начините за соработка што ги нудат Варшавската и Конвенцијата од Будимпешта.

Заемната правна помош сè уште се смета за главно средство за извршување судски наредби и прибирање докази во странство, но траењето на постапката претставува значителна пречка. Сепак, користењето заеднички истраги и заеднички истражни тимови може да ја подобри ефикасноста. Соработката и размената на информации меѓу органите на прогонот (полицијата и обвинителите) се неопходни во

⁴⁵ Но треба да се забележи дека и покрај можните ефикасни инструменти да се спречи и сузбие перењето пари во повеќе земји, гонењето перење пари е сепак предизвик.

прекуграничните случаи. Релевантните меѓународни мрежи и организации играат важна улога во овој поглед, а и помагаат да се изгради доверба. Каналите за соработка и инструментите што тие ги нудат се од суштинско значење за размена на информации и докази во кривични истраги.

4.1.1 Релевантни мрежи и организации за размена на информации и заемна правна помош

Меѓународна соработка - размена на (оперативни) информации Полиција до полиција, обвинител до обвинител	
Мрежата 24/7	Мрежа (контакт точки во полиција и/или обвинителство) Член 35 од Конвенцијата од Будимпешта
Групата EGMONT	Мрежа на УФР - спречување перење пари, одложување сомнителни трансакции. Член 46 од Варшавската конвенција
Мрежата CARIN	Камденска меѓуагенциска мрежа за враќање средства Мрежа стручњаци за конфискување приходи од криминал
INTERPOL	Канал за размена на информации и пренесување барања за заемна правна помош
Europol (EC3)	ЕУ и релевантни договори со земји вон ЕУ
Eurojust	Европска судска мрежа за компјутерски криминал (2016) ЕУ и релевантни договори со земји вон ЕУ
Меѓународна соработка - заемна правна помош Формална соработка - докази	
Заемна правна помош: формална соработка, резултатот од барање за заемна правна помош може да се употреби како доказ на суд. Вообичаените канали за комуникација се преку назначените централни власти, најчесто министерството за правда или надворешни работи.	
Директна соработка: судија со судија, обвинител со обвинител (ЕУ, билатерални договори) Варшавската (Член 34) и Конвенцијата од Будимпешта (Член 27/9) исто така предвидуваат директна соработка меѓу одговорните судски и обвинителски власти во итни предмети, каде што формалното барање исто така се пренесува преку централните власти.	
Други алтернативи	Заеднички истражни тимови Паралелна истрага Пренос на постапката.

Криминалците го кријат (или го чуваат) имотот во странство. При истрагата за криминал на Интернет извршен од страна на меѓународни криминални групи, треба да се провери дали сторителите имаат имот во странство. Во такви случаи **полициската и обвинителската соработка** се многу важни. Лицето за контакт во странската полиција може да информира кои податоци за имот може да се прибават од јавни извори, преку полициска соработка или со замолница. Тие информации може да го

направат добивањето податоци значително полесно и побрзо. Таквата соработка е оперативна и извршувањето судски наредби е исклучено.

Оперативните контакти и соработка може да доведат и до формирање заеднички истражни тимови, коишто во принцип исто така може да овозможат поделотворен пристап на заемна правна помош. Тоа може да доведе и до организирање паралелни истраги во прекугранички случаи со повеќе сторители и жртви.

Заемна правна помош е формална соработка и резултатот од барањето може да се употреби како доказ на суд. Вообичаените канали за комуникација се преку назначените централни власти, најчесто министерството за правда. Други можни канали може да бидат министерството за надворешни работи, или преку *INTERPOL*, *Europol* или *Eurojust* во итни случаи.

Во рамки на ЕУ, заемната правна помош оди директно меѓу одговорните власти (обвинител/суд). Варшавската (Член 34) и Конвенцијата од Будимпешта (Член 27/9) исто така предвидуваат таков пристап во итни предмети, каде што формалното барање исто така се пренесува преку централните власти.

4.1.2 Меѓународни правни инструменти

Компјутерски криминал	Финансиска истрага
Совет на Европа	
Конвенцијата од Будимпешта за компјутерски криминал и Проколот за ксенофобија и расизам ⁴⁶	Варшавската Конвенција за перење, претрес, заплена и конфискување приходи од криминал и за финансирање тероризам ⁴⁸
Насоки од T-CY ⁴⁷	Конвенцијата од Стразбур од 1990-та година за перење, претрес, заплена и конфискување приходи од криминал ⁴⁹
ЕУ	
Директива 2013/40/EУ на Европскиот парламент и на Советот од 12-ти август 2013 за напади на информатички системи што ја земнува Рамковната одлука на Советот 2005/222/ПВР ⁵⁰	Директива 2014/42/EУ за замрзнување и конфискување на инструментите за криминал во Европската Унија ⁵¹

⁴⁶ Конвенција за компјутерски криминал, ETS 185, 21.11.2001 и Дополнителен протокол на Конвенцијата за компјутерски криминал во врска со криминализацијата на чинови од расистичка и ксенофобична природа извршени преку компјутерски системи, ETS 189, 28.01.2003.

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

⁴⁸ Конвенција за перење, претрес, заплена и конфискување приходи од криминал и за финансирање тероризам, CETS 198, 16.05.2005.

⁴⁹ Конвенција за перење, претрес, заплена и конфискување приходи од криминал, Стразбур, ETS 141, 08.11.1990.

⁵⁰ Директивата воведува нови правила за хармонизирање на криминализацијата и санкциите за низа дела насочени против информатички системи. Таа исто така ги повикува земјите-членки на ЕУ да ги користат истите контакт точки што ги користат Советот на Европа и Г8 за брзо да се реагира на закани со напредна технологија. Достапно на: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040>

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

Директива 2016/1148 на Европскиот парламент и на Советот од јули 2016 за мерки за високо заедничко ниво на безбедност на мрежите и информатичките системи (Директива <i>NIS</i>) ⁵²	Заедничко дејство 98/699/ПВР за перење пари, откривање, наоѓање, замрзнување и конфискување инструменти на криминал и приходи од криминал ⁵³
Заклучоци на Советот на Европската Унија за подобрување на кривичната правда на Интернет и Заклучоците за Европската судска мрежа за компјутерски криминал ⁵⁴ , јуни 2016	Заедничко дејство 2001/500/ПВР за перење пари, откривање, наоѓање, замрзнување и конфискување инструменти на криминал и приходи од криминал ⁵⁵
	Директивата што ја заменува Директивата (ЕУ) 2015/849 за спречување на употребата на финансискиот систем за перење пари или финансирање тероризам и што ја заменува Директивата 2009/101/ЕЗ ⁵⁶
	Рамковна Одлука 2005/212/ПВР за конфискување на приходи, инструменти и имот поврзани со криминал ⁵⁷
	Рамковна одлука 2003/577/ПВР за извршувањето на налози за замрзнување имот или докази во Европската Унија ⁵⁸
	Рамковна одлука 2006/783/ПВР за примена на принципот на заемно признавање наредби за конфискување ⁵⁹

⁵² *NIS* директивата е достапна на: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L.2016.194.01.0001.01.ENG>

⁵³ За да се подобри соработката меѓу земјите од Европската унија во борбата против организираниот криминал, оваа заедничка акција овозможува подготовка, во рамките на работењето на Европската судска мрежа, на практични водичи за откривање, следење, замрзнување или заплена и конфискување инструменти и приходи од криминал. Достапно на: <http://eur-lex.europa.eu/legal-content/NLN/TXT/?uri=uriserv:l33073>

⁵⁴ Заклучоците се задржуваат на: соработка со даватели на услуги што овозможува брзо обелоденување податоци; може да се предвидат помалку ригорозни правни постапки за прибавување конкретни категории податоци, особено податоци за претплатникот. Постапките за заемна правна помош во врска со електронски податоци треба да се забрзаат и скратат; обемот на барања за заемна правна помош меѓу надлежните органи може да се намали единство преку зајакнување на соработката со давателите на услуги. Постапките за заемно признавање треба да се користат ефикасно за да се обезбеди делотворно обезбедување и прибавување електронски докази. Утврдување фактори на поврзување за да се спроведе јурисдикција во виртуелниот простор, вклучително и во случаи каде што локацијата на податоците е (сè уште) непозната или нестабилна. Достапно на: <http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace/>.

⁵⁵ Рамковна одлука на Советот 2001/500/ПВР од 26-ти јуни 2001 за перење пари, откривање, наоѓање, замрзнување и конфискување инструменти на криминал и приходи од криминал (ОЈ L 182, 5.7.2001, стр. 1). Достапно на: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001F0500>

⁵⁶ Има за цел и да ги регулира виртуелните валути преку обврзување на давателите на менувачки услуги и сервисите за паричници, меѓу другото, да соработуваат со својата домашна управа за финансиско разузнавање. Достапно на: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:0450:FIN%20>

⁵⁷ Рамковна одлука на Советот 2005/212/ПВР од 24-ти февруари 2005 за конфискување приходи, инструменти и имот поврзани со криминал (ОЈ L 68, 15.3.2005, стр. 49). Достапно на: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:068:0049:0051:en:PDF>

⁵⁸ Рамковна одлука 2003/755/ПВР од 22-ри јули 2003 за извршувањето на налози за замрзнување имот или докази во Европската унија (ОЈ L 196, 2.8.2003, стр.45). Достапно на: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003F0577>

⁵⁹ Рамковна одлука на Советот 2006/783/ПВР од 6-ти октомври 2006 за примена на принципот на заемно признавање наредби за конфискување (ОЈ L 328, 24.11.2006, стр. 59). Достапно на: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32006F0783>

	<p>Одлука на Советот 2007/845/ПВР за соработката меѓу службите за враќање средства на земјите-членки во областа на наоѓање и откривање приходи или друг имот поврзан со криминал (воведена обврска да се формираат служби за враќање средства)⁶⁰</p> <p>Директива 2014/41/ЕУ за европски налог за истрага за кривични прашања⁶¹</p>
ОН	
Резолуции за борба против кривична злоупотреба на информатички технологии (Резолуции 55/63 и 56/121) ⁶²	Конвенција на ОН од 1988 против незаконска трговија со наркотични дроги и психотропни супстанции ⁶³
Резолуција 64/211 на Генералното собрание на ОН (март 2010) за создавањето глобална култура на компјутерска безбедност ⁶⁴	<p>Конвенција на ОН од 2000 против меѓународен организиран криминал⁶⁵</p> <p>Конвенција на ОН од 2003 против корупција⁶⁶</p>
Други (регионални договори)	
Конвенција на Африканската унија за компјутерска безбедност и заштита на лични податоци ⁶⁷	
Арапска конвенција за спречување дела со информатичка технологија ⁶⁸	
Договор на Комонвелтот од независни држави за соработка во борбата против дела поврзани со компјутерски информации ⁶⁹	
Шангајски договор за соработка и организација во областа на меѓународна информатичка безбедност ⁷⁰	

⁶⁰ Одлуката ги утврдува условите за формирање домашни служби за враќање средства во земјите-членки на ЕУ. Достапно на: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007D0845>

⁶¹ Директивата за европски налог за истрага поставува нов сеопфатен систем што им овозможува на земјите-членки на ЕУ да прибават докази во други земји-членки за кривични случаи каде што се вклучени повеќе од една земја. Достапно на: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041>

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

⁶³ Конвенција на ОН против незаконска трговија со наркотични дроги и психотропни супстанции, Виена, 19.12.1988 (Член 5).

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

⁶⁵ Конвенција на Обединетите нации против меѓународен организиран криминал, Њујорк, 15.11.2000 (Членови 12-14).

⁶⁶ Конвенција на Обединетите нации против корупција, Њујорк, 31.10.2003 (Членови 31, 54-57).

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

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

⁶⁹ http://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>

Во рамките на ЕУ, принципот на заемно признавање, наспроти заемна помош, е воведен од 2003-та година за извршување наредби за замрзнување, и во 2006-та за наредби за конфискување. Исклучувањето на извршувањето е ограничено и со дерогации на принципите на двоен криминалитет и двојно замрзнување. ЕУ има направено дополнителни чекори да ја олесни соработката преку воведување европски налог за истрага.

4.1.3 Одредби за меѓународна соработка.

Меѓународните правни инструменти се занимаваат со аспекти на криминализирање извесно однесување, процедурална (истражни инструменти) и меѓународна соработка, вклучително и правна основа за заемна правна помош. Конвенциите од Варшава и Будимпешта даваат решенија што може да се користат и комбинираат за да се постигнат најделотворни резултати при паралелна финансиска и истрага за (компјутерски) криминал. Соработката подлежи на домашни одредби со заштитни мерки за одлужување или одбивање барања (Варшавска Конвенција, Дел 5, Член 27, и Конвенцијата од Будимпешта, Член 25/4 и 27/4 и 5). Главните области на соработка се дадени подолу:

Одредби за меѓународна соработка	
Конвенцијата Од Будимпешта	Варшавската конвенција
Основни принципи	
<p>(Членови 23-25)</p> <p>Страните овозможуваат заемна помош за истраги или постапки во врска со:</p> <ul style="list-style-type: none"> - компјутерски криминал (Членови 2-10) - или за прибирање електронски докази за кривично дело. 	<p>(Член 15)</p> <p>Страните соработуваат за целите на истрагата и постапките за конфискување средства и приходи.</p> <p>Барање за:</p> <ul style="list-style-type: none"> - конфискување конкретни предмети - да се плати износ соодветен на вредноста на приходите - и за истражна помош и привремени мерки заради конфискација.
Спонтани информации	
<p>(Член 26)</p> <p>Една страна може, во рамки на своето домашно право и без претходно барање, да ѝ упати на друга страна информации прибавени во рамките на своите истраги во случај кога смета дека обелоденувањето на тие информации може ѝ помогне на другата страна да поведе или да изврши истраги или постапки за кривични дела утврдени во согласност со оваа Конвенција или може</p>	<p>(Член 20)</p> <p>Слична одредба</p>

да доведат до барање за соработка од таа страна според ова поглавје.	
Привремени мерки	
<p style="text-align: center;">(Членови 29-30)</p> <p>Итно сочувување зачувани компјутерски податоци. Итно обелоденување зачувани податоци за сообраќај.</p>	<p style="text-align: center;">(Членови 21-22)</p> <p>Замрзнување или заплenuвање за да се спречи располагање со имот, негов пренос или отуѓување, и спонтано обезбедување на сите релевантни информации за привремената мерка.</p>
Помош во истрагата	
<p style="text-align: center;">(Членови 31-34)</p> <p>Заемна помош за истражни овластувања:</p> <ul style="list-style-type: none"> - Пристап до зачувани компјутерски податоци; - Прекуграничен пристап до зачувани компјутерски податоци со согласност или каде што се јавно достапни; - Прибирање податоци за сообраќај во реално време; и - Пресретнување податоци за содржината. 	<p style="text-align: center;">(Членови 16-19)</p> <p>Страните помагаат во откривањето и следењето на средствата и приходите, што вклучува и обезбедување докази за постоењето, локацијата или движењето, природата, правниот статус или вредноста на таквиот имот. Таа помош вклучува и барања за:</p> <ul style="list-style-type: none"> - информации за банкарски сметки; - банкарски трансакции; и - следење банкарски трансакции.
	Конфискување
	<p style="text-align: center;">(Членови 23-25)</p> <ul style="list-style-type: none"> - Извршување наредба за конфискување; или - Поднесување на барањето до надлежните власти за да се добие наредба за конфискување и таа да се изврши, вклучувајќи и барање да се исплати износ соодветен на вредноста на приходите, или да се конфискува конкретен предмет или имот.
	<p style="text-align: center;">(Член 23/5)</p> <p>Мерки еквивалентни на конфискување:</p> <ul style="list-style-type: none"> - некриминални санкции (конфискување што не се заснова на осуда) - правила за делење средства (оштета за жртвите, легитимни сопственици).
Мрежи за соработка	
Мрежата 24/7 (Член 35)	Соработка меѓу УФР (Членови 46-47)

<p>Секоја страна назначува контакт точка достапна 24/7 за да се обезбеди непосредна помош за</p> <ul style="list-style-type: none"> - истраги или постапки за кривични дела поврзани со компјутерски системи и податоци, - или за прибирање електронски докази за кривично дело. <p>Таква помош вклучува помагање или, ако дозволуваат домашното право и практиката, директно извршување на следните мерки:</p> <ul style="list-style-type: none"> - давање технички совети; - сочувување податоци (Членови 29 и 30); - прибирање докази, - давање правни информации, - и лоцирање осомничени. 	<p>УФР спонтано или по барање ги разменуваат сите достапни информации што може да се релевантни</p> <ul style="list-style-type: none"> - за обработка или анализа на информации, или - за истрага од страна на УФР за финансиски трансакции поврзани со перење пари и за вклучените физички или правни лица. <p>Овластување на УФР да одложат сомнителни трансакции.</p>
---	--

ПРАШАЊА ЗА РАЗМИСЛУВАЊЕ

1. Кои услови треба да се исполнети за спонтано да се споделат информации со друга јурисдикција?
2. Кои основи се на располагање во вашето домашно законодавство за да се одбие соработка со меѓународно барање за помош?
3. Кои услови треба да се исполнети за да се добие наредба за итно обелоденување сочувани податоци за сообраќај?
4. Кои практични мерки се утврдени за да се овозможи управување со конфискувани средства, располагање со нив и нивно споделување со друга јурисдикција? Дали тоа се договара случај по случај?

4.2 Оценка на примената на одредбите за меѓународна соработка

Важно е да се забележат и разберат можностите и пречките за меѓународна соработка во областа на истрагите за финансиски и компјутерски криминал и електронските докази што ги имаат утврдено меѓународните организации.

4.2.1 Оценка за гонењето приходи од криминал

4.2.1.1 GENVAL

Во ЕУ⁷¹, во контекст на петтата рунда заемна оценка на „финансиски криминал и финансиски истраги“, Работната група за општи прашања вклучително и оценки

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

(GENVAL) во финалниот извештај⁷² од 2012-та година посочи клучни предизвици за оваа област, и тоа:

1. Управување со случаи (вклучувајќи и управување со време и ресурси) и соработка меѓу надлежните власти, во земјата и меѓународно,
2. Сложени и разнородни правни правила и традиции, во земјата и на ниво на ЕУ, заедно со некогаш слабото спроведување,
3. Докази и прашањето на електронски податоци, и
4. Време. Финансиските истраги често траат долго време и може да чинат многу ресурси, во поглед на време, луѓе и финансиски средства.

Извештајот содржи и низа препораки за земјите-членки и ЕУ што може да се релевантни за која било јурисдикција:

- Финансиска истрага треба да се води за сите случаи на сериозен и организиран криминал (коишто вклучуваат тероризам), а не само за чисто економските и финансиски кривични дела. Затоа треба да се изготви сеопфатна политика за финансиски криминал и финансиски истраги, којашто ќе ги опфати сите релевантни висти, вклучително и обвинителството, сè со цел да се забрзаат сложените и долги истраги во областа на финансискиот криминал. Таа треба да ги одразува релевантните приоритети договорени на ниво на ЕУ и да ги постави темелите за проактивни истраги. Треба да се обрне повеќе внимание на потенцијалните придобивки на меѓународната соработка, особено на ниво на ЕУ.
- Политиката за финансиски криминал и финансиски истраги треба да биде одразена во долгорочна државна стратегија. Кога е тоа можно, во стратегијата треба да се вклучи концепт за полициска работа водена од финансиското разузнавање за да се овозможи проактивно извршување на мерките врз основа на аналитички резултати. Стратегијата треба да се комбинира со редовна ревизија и проценка на методологијата, како и со добар механизам за известување за вклучените субјекти. При изготвувањето на таа стратегија, треба да се земат предвид некои основни критериуми, правила или насоки за да се појасни поделбата на задачи меѓу разните органи со поодделни надлежности, како и да се вклучат клучни приоритети и случаи на сериозен меѓународен криминал. На тој начин стратегијата треба да е поддржана од добро управување внатре во полицијата за да се поттикне проактивен пристап воден од разузнавачки информации.
- Земјите-членки треба да го спроведат сето законодавство на ЕУ во врска со заемното признавање и судската соработка за кривични прашања. Згора на тоа, земјите-членки и релевантните служби на ЕУ треба да направат ревизија на спроведувањето на релевантните рамковни одлуки и примената на механизмите за заемна правна помош. На тој начин, земјите-членки треба да ги откријат и совладаат пречките за ефикасна и проактивна размена на податоци со странски органи на прогонот, служби на ЕУ и други релевантни актери. Спонтаната размена на информации, во согласност со Одлуката на Советот 2007/845/ПВР од 6-ти декември 2007 за соработка меѓу службите на земјите-членки за враќање средства во областа на наоѓање и откривање приходи или друг имот поврзан со криминал, треба дополнително да се зајакне, и треба да се поттикне употребата на Одлуката на Советот

⁷² Конечен извештај на GENVAL од 2012-та година за петтата рунда заемна оценка - „Финансиски криминал и финансиски истраги“. Достапно на: <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012657%202012%20REV%202>

2006/960/ПВР од 18-ти декември 2006 за поедноставување на размената на информации и разузнавачки информации меѓу органите на прогонот на земјите-членки на ЕУ.

4.2.1.2 Прашалник на РС-ОС

Советот на стручњаци на Советот на Европа за функционирањето на европските конвенции за соработка во кривични прашања (РС-ОС) во 2014-та година го задржа вниманието на гонењето приходи од криминал. Одговорите на прашалникот⁷³ на РС-ОС покажаа, меѓу другото, дека има разлики меѓу страните во примената на одредбите од конвенциите од Стразбур и Варшава што се релевантни за меѓународната соработка.

Еве некои од аспектите со коишто се занимаваше прашалникот:

- Државите не се секогаш во можност да обезбедат да се спроведе барање врз основа на т.н. систем за конфискување заснован на вредност. Овој систем е даден во двете конвенции како систем со којшто е можно да се соработува и покрај т.н. систем за конфискување заснован на предмет. И во двата системи е потребна кривична осудителна пресуда. Во системот за конфискување заснован на вредност, се пресметува добивката од криминал. На крај, врз основа на тие пресметки, судијата наметнува обврска да се плати износ еднаков на стекнатата добивка од криминал. Наредбата за конфискување потоа може да се изврши од сите средства во сопственост на осуденото лице. Во овој поглед, нема потреба да се докаже дека тие средства се стекнати директно од кривичното дело.
- Неколку држави ја признаваат можноста за заплена и конфискување средства коишто *de facto* му припаѓаат на обвинетото/осуденото лице, но правно се смета дека се во сопственост на трето лице, најчесто т.н. фантом.
- Само некои држави се во можност да понудат заемна правна помош за или во врска со конфискација што не е заснована на осуда и други мерки (на пример, заплена на сомнителни средства). Тоа ја вклучува и фазата за собирање информации кога често се бараат кривични информации за употреба во постапка што не е заснована на осудителна пресуда, претрес, заплена и конфискување приходи од криминал.
- Некои држави се во положба да понудат помош во кривични, граѓански и управни постапки поврзани со одговорноста на правни лица заради заплена и конфискување приходи од криминал.
- Само некои држави се во положба да понудат помош во постапки поврзани со виртуелни валути, како на пример биткоини, особено во однос на заплена и конфискување.

4.2.1.3 MONEYVAL

Комитетот на стручњаци за проценка на мерките против перење пари и финансирање тероризам - MONEYVAL⁷⁴ е постојано мониторинг тело на Советот на Европа на коешто

⁷³ Прашалник за употребата и ефикасноста на инструментите на Советот на Европа за меѓународна соработка во областа на заплена и конфискување приходи од криминал, вклучително и управување со конфискувана стока и делење средства, *РС-ОС Mod (2015) 06Rev4*, 19.5.2016. Достапно на: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680666607>

⁷⁴ Комитет на стручњаци за проценка на мерките против перење пари и финансирање тероризам (MONEYVAL): http://www.coe.int/t/dqhl/monitoring/moneyval/default_en.asp?expandable=0

му е доверена задачата да ја оценува усогласеноста со главните меѓународни стандарди за сузбивање перење пари и финансирање тероризам, и делотворноста на нивното спроведување, како и задачата да им дава препораки на домашните власти за потребните подобрувања на нивните системи.

Преку динамичен процес на заемни оценки, рецензија и редовна проверка по извештаите, *MONEYVAL* има за цел да го подобри капацитетот на домашните власти за поделотворна борба против перењето пари и финансирањето тероризам.

Оценските извештаи се објавуваат на Интернет.⁷⁵

4.2.2 Оценка за компјутерски криминал

4.2.2.1 GENVAL

Седмата рунда заемни оценки на ЕУ е посветена на практичното спроведување и работа со европските политики за спречување и борба против компјутерски криминал. Завршените оценски извештаи се објавени и може да им послужат на други земји да си ги ревидираат законодавството и стратегијата за компјутерски криминал.⁷⁶

Истовремено, нацрт конечниот извештај нагласува некои проблематични аспекти во меѓународната соработка, на пример просечното време за одговор на барање за заемна правна помош изнесува неколку месеци и може да варира во зависност од тоа дали барањето се дава врз основа на меѓународен договор или реципроцитет. Во вториов случај, времето за одговор е уште подолго. Но со оглед на спецификата на компјутерскиот криминал, „траењето на постапките за заемна правна помош ги прави формалните канали за заемна правна помош доста неделотворни, со негативни последици за водењето и успехот на истрагите, бидејќи дигиталните докази се нестабилни и со нив треба да се работи брзо и ефикасно зашто доцнењето може да доведе до губење податоци. Затоа има општа потреба да се забрза работата на барањата за заемна правна помош во истрагите за компјутерски криминал.“ Нацрт-извештајот забележува и дека треба да се најдат меѓународни решенија за подобрување на постапките за заемна правна помош со трети земји, на пример во една земја-членка како најдобра практика е утврдено користење образец за барања за наредба итно прибавување, договорено од извршните власти во дадена држава. Слично на тоа, развивањето неформални и лични контакти кај надлежните власти на трети земји пред да се прати барањето за заемна правна помош се нагласува како корисна практика што може да доведе до подобра и побрза соработка во извршувањето на формалните барања.⁷⁷

На земјите-членки им беа изнесени следните препораки:

- Земјите-членки треба да го подобрат квалитетот на барањата за заемна правна помош што ги праќаат до други земји, и особено да се погрижат тие да се комплетни и да ги разгледаат начините за забрзување и подобрување на квалитетот на одговорите на барањата за заемна правна помош.

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

⁷⁶ Усвоените извештаи се наоѓаат на: <http://www.coe.int/da/web/octopus/blog/-/blogs/genval-evaluation-reports-on-cybercrime>

⁷⁷ Нацрт конечен извештај за седмата рунда заемни оценки за „Практичното спроведување и работа со европските политики за спречување и борба против компјутерски криминал“, јуни 2017. Видете стр. 82-88. Достапно на: <http://data.consilium.europa.eu/doc/document/ST-9986-2017-INIT/en/pdf>

- На земјите-членки им се препорачува да ја зајакнат делотворноста на комуникацијата со другите земји-членки и трети земји со формирање систем за регистрирање земна правна помош и систем за управување со заемна правна помош, со што ќе се овозможи еден случај да се следи од неговата регистрација до одговорот што се праќа до земјата-барател.
- Земјите-членки се поттикнуваат почесто да ги користат инструментите *Eurojust*, Европската судска мрежа и *Europol* и да развиваат неформални контакти со надлежните странски власти со цел да се добијат побрзи одговори на барањата за заемна правна помош од трети земји.
- ЕУ треба да размисли за координирање на напорите да се воспостави делотворен начин за пренесување и извршување барања за заемна правна помош од земјите-членки кон земји вон ЕУ, или да се направи рамка за директна соработка со релевантните интернет провајдери вон ЕУ.
- ЕУ треба да работи на решенија за подобрување и забрзување на комуникацијата меѓу земјите-членки и трети земји, особено САД, конкретно во врска со размената на оперативни информации и барањата за заемна правна помош и нивното извршување.

4.2.2.2 T-CY

Комитетот на Советот на Европа за конвенцијата за компјутерски криминал (*T-CY*) го следи спроведувањето на Конвенцијата од Будимпешта за компјутерски криминал и изготвува дополнителни стандарди и насоки за да се олеснат делотворната употреба и спроведувањето на Конвенцијата Од Будимпешта, меѓу другото и во светлина на правните, политички и технолошки случувања.

4.2.2.2.1 Заемна правна помош

Заемната правна помош останува главно средство за прибавување докази од странски јурисдикции за примена во кривичната постапка. Во декември 2014-та, *T-CY* направи оценка на функционирањето на одредбите за заемна правна помош од Конвенцијата од Будимпешта.⁷⁸ Се заклучи, меѓу другото, дека постапката за заемна правна помош генерално се смета за неефикасна, особено за прибавувањето електронски докази. Се чини дека времето на одговор од 6 до 24 месеци е вообичаено. Затоа многу барања и истраги се напуштаат. Ова влијае негативно на позитивната обврска на владите да ги штитат општеството и поединците од компјутерски криминал и друг криминал што вклучува електронски докази.

Оценскиот извештај заклучува и дека не сите видови податоци се потребни со иста зачестеност или итност: најчесто баран вид податоци што се бараат се информациите за претплатникот. Големиот број барања за такви информации им става тежок товар на властите одговорни за обработка и извршување барања за заемна правна помош и ги забавува, а често и ги спречува, кривичните истраги. Тоа налага дека решенијата за предизвиците за информации за претплатникот треба да ја направат заемната правна помош поефикасна.

Извештајот на *T-CY* ги посочува следните утврдени проблеми:

- Времето, обемот на работа и сложеноста на постапките што се потребни да се подготви или изврши барање за заемна правна помош

⁷⁸ *T-CY(2013)17rev*, 3-ти декември 2014, оценски извештај на *T-CY*: Одредби за заемна правна помош во Конвенцијата од Будимпешта за компјутерски криминал. Достапно на: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>

- Задоцнети (6 - 24 месеци) одговори на барањата генерално или во врска со конкретни земји
- Доцнење во давањето податоци за претплатникот
- Одбивањето на некои земји да соработуваат за „ситни“ дела
- Одбивањето да соработуваат или неодговарање од некои земји
- Проблем на соработка со контакт точките од мрежата 24/7
- Недавање потврда дека е примено барањето за заемна правна помош или дека се сочувани податоци
- Нејасни критериуми за „итни“ барања
- Проблеми со јазикот, квалитетот на преводот и терминологијата
- Примените барања се преопшти, за голем обем податоци
- Разлики меѓу правните системи, како на пример истражните овластувања
- Правни ограничувања (заштита на податоци)
- Одбивање на друга земја да соработува без барање за заемна правна помош. Но за таквите барања за заемна правна помош се потребни информации и докази што не може да се прибават без соработка од другата земја (маѓепсан круг)
- Барањето може да не го задоволува правниот праг или формалните услови на замолената земја, барањето може да не е комплетно, или бараниот праг/стандард да е превисок
- Несоодветни закони
- Не е задоволен условот на двоен криминалитет
- На барањето за заемна правна помош не му претходи барање за сочувување за да се обезбеди податоците да се сè уште достапни
- Податоците не се сочувуваат во другата земја и покрај барањето за сочувување
- Податоците не се веќе достапни во другата или домашната земја
- Различни политики на давателите на услуги за ставање податоци на располагање
- Непознато лице за контакт или надлежни власти за итни случаи во другата земја, проблеми да се откријат засегнатите, на пример давателот на услуги за хостирање
- Преоптовареност со премногу барања
- Ограничени технички вештини и разбирање на електронските докази во замолената земја.
- Ограничени овластувања на судската полиција
- Праг на „разумен сомнеж“.

T-CY усвои низа препораки за поефикасна постапка за заемна правна помош во однос на компјутерски криминал и електронски докази преку поделотворна употреба на постојните одредби од Конвенцијата од Будимпешта за компјутерски криминал и други договори, но и преку предлагање дополнителни решенија⁷⁹, како на пример:

- Страните треба во целост да ги спроведат овластувањата за сочувување од Конвенцијата од Будимпешта (Препорака 1), да ја следат делотворноста на постапката за заемна правна помош (Препорака 2), давање повеќе и подобро обучен персонал и повеќе ресурси за заемна правна помош (Препораки 3 и 4), зајакнување на улогата и капацитетите на лицата за контакт од мрежата 24/7 (Препорака 5), утврдување постапки за итни ситуации (Препорака 8) итн.

⁷⁹ Видете стр. 125-127 од оценскиот извештај на *T-CY*: Одредби за заемна правна помош од Конвенцијата од Будимпешта за компјутерски криминал

- Страните треба да размислат - можеби преку протокол на Конвенцијата од Будимпешта - да дозволат обелоденување податоци за претплатникот по забрзана постапка (Препорака 19), за можноста за меѓународни наредби за прибавување докази (Препорака 20), непосредна соработка меѓу судските власти (Препорака 21), да работат на практиката за непосредно прибавување информации од странски даватели на услуги (Препорака 22), заеднички истраги и/или заеднички истражни тимови меѓу страните (Препорака 23), да се дозволи испраќање барања на англиски јазик (Препорака 24).

4.2.2.2 Дополнителни практични предизвици

Дополнително ќе се осврнеме на некои дополнителни предизвици и аспекти на меѓународната соработка:

Услови за пристап до податоци за содржината од активен компјутер на осомничено лице, дури и податоците да се чуваат во странство, и поврзаното прашање на согласност и јурисдикција

Во конечниот извештај Групата за докази во Облакот (CEG) при T-CY за кривично-правен пристап до електронски докази во Облакот: Препораки за разгледување пред T-CY⁸⁰, се забележува дека по правило, органите на прогонот вообичаено се одредуваат по принципот на територијалност. Според овој принцип, една земја не може да наметне своја јурисдикција на територијата на друга суверена земја. Кривично-правниот пристап до податоци на сервери или компјутерски системи што генерално се наоѓаат во други јурисдикции без да се вклучат властите од тие јурисдикции предизвикува загриженост.

Сепак, во ситуации кога некој компјутер на место на дело или на лице што се истражува е активен (во функција), кривичните власти технички може да им пристапат на податоците (вклучително и оние што се чуваат на сервери во Облакот) без знаењето на јурисдикцијата во којашто се наоѓа серверот и се чуваат податоците. Член 32-б од Конвенцијата од Будимпешта нуди решение само за ограничени ситуации што се опишани во насоките усвоени од страна на T-CY во декември 2014-та година.⁸¹

Поради ограничувањата на Член 32-б од Конвенцијата од Будимпешта (доброволна согласност на осомничен за пристап до и-мејлот при истрага во живо), некои држави во пракса бараат унилатерални решенија. Се чини дека има раширена пракса органите на прогонот во дадена кривична истрага да пристапуваат до податоци не само на уредот на осомничениот, туку и на поврзаните уреди, како на пример и-мејлот или други профили во Облакот ако уредот е отворен или податоците за пристап се добиени законски, макар што знаат дека се поврзуваат во друга, позната земја.

CEG ја разгледа доктрината на долга рака на антимонополското право на ЕУ (Предмети *ICI* 48/69; *Woodpulp* 89/85) и забележа дека Европската комисија

⁸⁰ T-CY (2016)5, 16-ти септември 2016, Кривично-правен пристап до електронски докази во Облакот: Препораки за разгледување од страна на T-CY. Достапно на: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>

⁸¹ T-CY Насока бр. 3 за прекуграничен пристап (Член 32), 3-ти декември 2014. Достапно на: <https://rm.coe.int/16802e726a>

препорачува властите за конкуренција внатре во Европската унија да добијат пристап до сервери каде било во светот за да приберат докази во антимонополски постапки. За да имаат делотворни овластувања за прибирање електронски докази, важно е властите при остварувањето на своите инспекциски овластувања да прибираат дигитални информации што им се достапни на субјектот или лицето чии простории се предмет на инспекција, без оглед каде тие се чуваат, вклучително и сервери и други носачи што се наоѓаат вон територијата на соодветните домашни власти за конкуренција или вон Европската Унија. Условите и заштитните мерки за таквиот пристап до податоци треба да се дефинираат во протокол.

CEG заклучи дека рамката за прекуграничен пристап ќе треба да ги дефинира условите и заштитните мерки за таквиот пристап со цел да се заштитат правата на поединците и да се спречи повреда на овластувањата или правата на други влади или нивни субјекти.

Пристап до податоци за претплатникот

Податоците за претплатникот се помалку чувствителни на приватност и најчесто се бараат. Во многу земји е доволна полициска или обвинителска наредба за прибавување, но во некои од нив е потребна судска наредба во случај на динамична *IP* адреса бидејќи тоа вклучува и податоци за сообраќајот.

Затоа, конечниот извештај на *CEG* за кривично-правен пристап до електронски докази во Облакот го препорачува следното:

- Информациите за претплатникот се помалку чувствителни на приватност од податоците за сообраќај и содржина, па условите за наредби за прибавување информации за претплатникот треба да подлежат на послаби заштитни мерки од другите видови податоци или за други видови нападни овластувања.
- Полесен режим за прибавување информации за претплатникот ќе помогне во домашните истраги и меѓународната соработка во контекст на Облакот.

Испитани се и условите за користење домашна наредба за прибавување (Член 18 од Конвенцијата од Будимпешта) претплатнички податоци во случај на меѓународни даватели на услуги коишто нудат услуги на територијата на земјата, без оглед дали имаат седиште во странство и каде се наоѓаат податоците.

Кривично-правните власти можат или да утврдат јурисдикција за извршување преку ставање акцент на локацијата на компјутерскиот систем или уредот за чување (што е покриено со одредбите за претрес и заплена од Член 19 од Конвенцијата од Будимпешта), или на физичкото или правно лице (вклучително и даватели на услуги) што ги имаат или контролираат податоците што се бараат.⁸² Ова второто е покриено со Член 18 за наредби за прибавување.

Заемната правна помош претпоставува дека локацијата на бараните податоци е позната и дека така е познато и се знае на која држава и на кој надлежен орган да му се упати барањето за заемна правна помош. Сепак, за кривично-правните власти често не е очигледно во која јурисдикција се чуваат бараните податоци и/или кој правен режим важи за податоците. Давателот на услуги може да има седиште во една јурисдикција, да применува правен режим од втора јурисдикција, а податоците да се

⁸² На пример, Директива на Европската унија 2016/1148 за безбедноста на мрежни и информатички системи (*NIS* директива) од 6-ти јули 2016, Член 18 Јурисдикција и територијалност.

чуваат во трета јурисдикција. Податоците може да се пресликани во повеќе јурисдикции или да менуваат јурисдикции. Ако локацијата на податоците ја одредува јурисдикцијата, можно е давателот на услуги во Облакот систематски да ги преместува податоците за да спречи кривично-правен пристап.

Интернетот нема граници, па информациите за претплатникот што се потребни во истрагата може да се кај давател на услуги „којшто ги нуди своите услуги на територијата“ на земјата, иако самиот давател на услуги и серверите на коишто се чуваат бараните информации може да се наоѓаат во други јурисдикции.

CEG е на став дека логичното толкување на Член 18.1-6 од Конвенцијата од Будимпешта нуди решение. Надлежните власти во земјата треба да се во можност да побараат информации за претплатникот од давател на услуги што нуди услуги на нејзината територија, без оглед на тоа каде се чуваат информациите и каде се наоѓа давателот на услуги. Насоката број 10 за наредби за прибавување информации за претплатник⁸³ што ја усвои T-CY поттикнува такво толкување и примена на Член 18 од Конвенцијата од Будимпешта. Таквата примена фактички избегнува барање за заемна правна помош.

Насоката нагласува дека наредбата од Член 18.1-6 може да се примени во конкретни случаи за конкретни претплатници ако давателот на услуги ги има или контролира податоците на претплатникот и ако давателот на услуги „нуди услуга на територијата на земјата“, односно кога:

- Давателот на услуги им овозможува на лицата на територијата на земјата да се претплатат на неговите услуги (и, на пример, не спречува пристап до тие услуги); и
- ги насочува своите активности кон такви претплатници (на пример, преку локално рекламирање и рекламирање на јазикот на територијата на земјата), или ги користи претплатничките информации (или поврзаните податоци за сообраќај) во текот на своите активности, или контактира со претплатниците во земјата, и
- информациите за претплатникот што треба да се прибават се во врска со услугите на давателот на услуги што се нудат на територијата на земјата.

Исто така, одлуката на Врховниот суд на Белгија потврди такво толкување со пресудата дека давателот на услуги што работи на територијата на една земја подлежи и е обврзан на применливото домашно законодавство. Врховниот суд на Белгија во случајот на *Yahoo!*⁸⁴ досуди дека наредбата за прибавување информации за претплатник упатена до давател на услуги што нуди услуги и на тој начин е „присутен“ на територијата на земјата претставува домашна наредба (според Член 18.1-6) и не е прашање на меѓународна соработка, ниту екстериторијална јурисдикција. *Yahoo! Inc.* поднел жалба против претходна одлука на Апелациониот суд во Антверпен од 20-ти ноември 2013, со тврдење, меѓу другото, дека според меѓународното обичајно право, државата не може да бара екстериторијална јурисдикција.

⁸³ Насока бр. 10: Наредби за прибавување информации за претплатник (Член 18 од Конвенцијата Од Будимпешта), усвоена со писмена постапка од страна на T-CY на 28-ми февруари 2017.

Достапно на: <https://rm.coe.int/doc/09000016806f943e>

⁸⁴ Пресуда на Врховниот суд на Белгија во предметот против *Yahoo!* На 1-ви декември 2015, Врховниот суд на Белгија изрече конечна пресуда дека *Yahoo! Inc.*, регистрирана во Калифорнија, САД, има обврска да прибави податоци за претплатникот и подлежи на принудните мерки од Член 46-а од Белгиските правила за кривична постапка.

Достапно на холандски: http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1

Белгискиот Врховен суд одлучил дека:

- Општо земено, една држава може да примени принудни мерки единствено на својата територија и во друг случај би го повредила суверенитетот на друга држава.
- „Државата наметнува принудна мерка на својата територија ако има доволна територијална врска меѓу таа мерка и таа територија.“
- Член 46-а, дел 2 од Белгискиот кривичен законик „е единствено наменет да им наметне на операторите и снабдувачите што се активни во Белгија една мерка заради прибавување обични податоци за идентификација во случај на кривично дело или престап, чијашто истрага е во надлежност на белгиските обвинителски власти. Таа мерка не бара присуство во странство на белгиската полиција или обвинители, ниту на полномошници што делуваат во нивно име. Таа мерка не бара ниту материјално дејство или чин во странство. Затоа мерката има ограничен опсег и влијание, и нејзиното извршување не бара интервенција вон територијата на Белгија“.
- *Yahoo! Inc.* „како снабдувач на бесплатна услуга за и-мејл е присутен на белгиска територија и доброволно се подложува на белгиското право бидејќи активно учествува во белгискиот економски живот со тоа што конкретно го користи доменот *www.yahoo.be*, го користи локалниот јазик, прикажува реклами засновани на локацијата на корисниците на услугите, и е достапен во Белгија за тие корисници преку поставувањето сандаче за поплаки и служба за чести прашања.“
- „На јавниот обвинител не му треба ништо во САД од американски субјект, туку нешто во Белгија од американски субјект којшто нуди услуги на белгиска територија.“
- Затоа не се применува екстериторијална јурисдикција.

Директна соработка со меѓународни даватели на услуги

Соработката со САД е од особена важност бидејќи многу меѓународни даватели на услуги имаат седиште таму и бројот на барања за заемна правна помош расте. Конечниот извештај на *CEG* за кривично-правен пристап до електронски докази во Облакот нагласува дека давателите на услуги од САД може да им обелоденат информации за претплатник и податоци за сообраќај на странски власти врз основа на правно барање и дека тоа е во согласност со намерите на Член 18.1-б од Конвенцијата од Будимпешта. Сепак, се забележува дека нестабилноста на политиките на давателите на услуги⁸⁵ и непредвидливоста на обелоденувањето водат до неизвесност за органите на прогонот и клиентите и се покренуваат прашања за владеењето на правото.

Во случај на европски даватели на услуги, таквата соработка не е можна поради правилата за заштита на податоци и треба да се поднесе барање за заемна правна помош.

Давателите на услуги од САД прифаќаат барања за сочувување кои било податоци, добиени од странски власти со очекување дека на тоа ќе следи барање за обелоденување преку заемна правна помош. Европските даватели на услуги не

⁸⁵ За преглед на разни политики за даватели на услуги, видете: Кривично-правен пристап до податоци во Облакот: соработка со „странски“ даватели на услуги, Група за докази во Облакот при *T-CY*, мај 2016. Достапно на: <https://rm.coe.int/168064b77d>

прифаќаат барања за сочувување добиени директно од органите на прогонот во други јурисдикции.

Итни постапки

Препораката 8 од Оценскиот извештај на *T-CY* за заемна правна помош вели дека страните се поттикнуваат да воспостават итни постапки за барања во врска со ризици за живот и слични исклучителни околности. Истражувањето на *CEG*⁸⁶ од 2016-та година, во коешто учествувале 33 земји, покажува дека:

- Повеќето страни немаат законодавство што овозможува обелоденување податоци на домашните кривично-правни власти во итни ситуации;
- Помалку од 20% имаат постапки што им дозволуваат на домашните надлежни власти да им обелоденуваат податоци на странски власти во забрзана постапка;
- Само две страни им дозволуваат на давателите на услуги на својата територија да им обелоденуваат податоци на странски надлежни власти во итна ситуација.

CEG предлага Препораката 8 исто така да се реши со протокол на Конвенцијата од Будимпешта.

Дополнителен протокол на Конвенцијата од Будимпешта

CEG препорача да се почнат преговори за дополнителен протокол на Конвенцијата од Будимпешта за компјутерски криминал за да се овозможи поделотворна заемна правна помош, да се олесни директната соработка со даватели на услуги во други јурисдикции кога тоа е потребно, што ќе подлежи на услови и заштитни мерки, да се утврдат услови и заштитни мерки за постојните практики на прекуграничен пристап до податоци и да се утврдат услови за заштита на податоци.

Дополнителен протокол на Конвенцијата од Будимпешта ќе може:

- Да ги појасни постапките и условите за директна соработка со даватели на услуги во други јурисдикции, и допустливоста на добиените податоци во кривичната постапка;
- Да постави правна основа за директни барања за сочувување до странски даватели на услуги. Оваа практика веќе ја прифаќаат давателите на услуги од САД;
- Да уреди итни постапки што дозволуваат директна соработка со даватели на услуги во странски јурисдикции во конкретни исклучителни ситуации.

Можни елементи на протоколот:

- Одредби за поделотворна заемна правна помош:
 - поедноставен режим за барања за заемна правна помош за информации за претплатникот;
 - меѓународни наредби за прибавување;

⁸⁶ Итни барања за непосредно обелоденување податоци што се чуваат во друга јурисдикција преку директни барања до давателите на услуги, Група за докази во Облакот при *T-CY*, мај 2016 <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651a6f>

- директна соработка меѓу судски власти за барања за заемна правна помош;
 - заеднички истраги и заеднички истражни тимови;
 - барања на англиски јазик;
 - аудио/видео сослушување сведоци, жртви и вештаци;
 - итни постапки за заемна правна помош.
- Одредби што овозможуваат директна соработка со даватели на услуги во други јурисдикции за барања за информации за претплатникот, барања за сочувување, и итни барања.
 - Појасна рамка и посилни заштитни мерки за постојните практики за прекуграничен пристап до податоци.
 - Заштитни мерки, вклучително и услови за заштита на податоци.

Описот на проектот за подготовка на нацрт за втор дополнителен протокол на Конвенцијата од Будимпешта за компјутерски криминал беше усвоен на 17-тата пленарна седница на T-CY во јуни 2017-та година.⁸⁷

4.3 Користење шаблони и обрасци за заемна правна помош

Барањата за заемна помош се различни, дури и да се засноваат на меѓународни правни инструменти, бидејќи зависат од домашното законодавство на земјата барател, како и од законодавството и практичните очекувања на замолената земја. Обрасци за барања за заемна правна помош може да им помогнат на земјите во извесна мера и затоа се вложени напори да се изготват шаблони.

Комитетот PC-OC на Советот на Европа во 2016-та година изготви образец за барање заемна правна помош во кривични прашања⁸⁸.

T-CY во Оценскиот извештај од 2014-та година за одредбите за заемна правна помош во Конвенцијата од Будимпешта за компјутерски криминал, во Препорака 17 вели дека Советот на Европа треба во проектите за зајакнување капацитети да изготви или да упати на стандардизирани повеќејазични обрасци за барањата под Член 31⁸⁹.

Заклучоците на Советот на ЕУ за подобрување на кривичната правда во виртуелниот простор (јуни 2016) ја повикуваат Комисијата, меѓу другите, во соработка со земјите-членки, Eurojust и трети земји да разгледаат и дадат препораки како да се приспособат, каде што е тоа соодветно, постојните стандардизирани обрасци и постапки за барања да се обезбедат и прибават е-докази.

⁸⁷ T-CY(2017)3 Опис за подготовката на нацрт втор дополнителен проткол на Конвенцијата од Будимпешта за компјутерски криминал, јуни 2017. Достапно на: <https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b>

⁸⁸ Видете ги документите од 69-тиот состанок (мај 2016: Нацрт шаблон за заемна правна помош и практични насоки за практичари: <http://www.coe.int/en/web/transnational-criminal-justice-pcoc/pcoc-69th-meeting> <http://www.coe.int/en/web/transnational-criminal-justice-pcoc/model-request-form-for-mutual-assistance-in-criminal-matters>

⁸⁹ Одредбите за заемна правна помош во Конвенцијата од Будимпешта за компјутерски криминал, 3.12.2014 (T-CY(2013)17rev). (<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>)

Пример на образец за наредба за конфискување има во Рамковната одлука на Советот 2006/783/ПВР од 6-ти октомври 2006 за примената на принципот на заемно признавање наредби за конфискување⁹⁰.

Друг пример е Директивата на Европскиот парламент и Советот 2014/41/ЕУ од 3-ти април 2014 за европски налог за истрага за кривични прашања⁹¹.

Згора на тоа, *UNODC* има изготвено алатка за пишување барања за заемна правна помош⁹².

Очигледно е дека традиционалните пристапи за заемна правна помош не се веќе соодветни во свет со криминал на Интернет. Свесноста за можностите и предизвиците на двата инструменти на Советот на Европа, Конвенцијата Од Будимпешта (на пример, пристап до податоци во Облакот) и Варшавската Конвенција (извршување на наредби за замрзнување и конфискување), ќе придонесе да се подобрат резултатите кога се комбинираат истрагата за компјутерски криминал и паралелната финансиска истрага.

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 Виртуелни валути

Криптовалутите, особено *Bitcoin*, останува валута што се одбира за компјутерски криминал, било да се користи за плаќање за криминални услуги или за добивање исплати од жртви на изнудување. Сепак, клучни членови на *Bitcoin* заедницата, како берзите, сè повеќе се жртви на компјутерските криминалци⁹³. По воведот во виртуелни валути од основниот курс, напредниот курс дава подетални информации за функционирањето на виртуелните валути (особено *Bitcoin*) и ќе се осврнеме на ризиците поврзани со употребата на овие виртуелни валути. На крајот на овој дел ќе дадеме вовед во некои истражни и предизвици за замрзнување/заплена што се појавиле во однос на виртуелните валути.

5.1 Резиме од основниот курс

Според дефинициите на *FATF*⁹⁴, основниот курс ги дефинираше следните поими и категории во однос на виртуелните валути:

- Виртуелна валута
- Електронски пари/е-пари
- Дигитална валута
- Конвертибилни наспроти неконвертибилни виртуелни валути
- Централизирани наспроти децентрализирани виртуелни валути

Овие поими се резимирани во следната табела.

Виртуелна валута	„Виртуелна валута е дигитален приказ на вредност со којшто може да се тргува на Интернет и функционира како (1) средство за размена; и/или (2) пресметковна единица; и/или (3) резерва на вредност, но нема статус на законско платежно средство во ниту една јурисдикција“
Електронски пари/е-пари	„Виртуелната валута се разликува од е-пари коишто се дигитален приказ на обичните пари што се користат за електронски пренос на вредност искажана во обични пари.“
Дигитална валута	„Дигитална валута може да значи дигитален приказ било на виртуелна валута или електронски пари, и затоа често се користи синонимно со поимот виртуелна валута.“
Конвертибилни наспроти неконвертибилни виртуелни валути	Конвертибилните (или отворени) виртуелни валути имаат еквивалентна вредност во реална валута и може да се разменуваат од и во реална валута. Неконвертибилните (затворени) виртуелни валути се наменети за конкретен виртуелен домен или свет, и според правилата со коишто се уредува нивното користење, тие не може да се разменат за обични пари.
Централнизиран наспроти децентрализирани	Централизираните виртуелни валути имаат единствен административен орган (администратор), т.е. трето лице што го контролира системот. Администраторот ја емитува валутата,

⁹³ Оценка на заканата од организиран криминал на интернет (*IOCTA*) 2016, *Europol*. Достапно на: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016>

⁹⁴ Извештај на *FATF*, Виртуелни валути, главни дефиниции и потенцијални ризици за перење пари/финансирање тероризам, јуни 201. Достапно на: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

виртуелни валути	утврдува правила за нејзината употреба, одржува централен платен регистар, и има овластување да ја откупува валутата (да ја повлекува од оптек). Децентрализираните виртуелни валути се дистрибуирани, со отворен код, и математички <i>peer-to-peer</i> виртуелни валути коишто немаат централен административен орган и надзор.
-------------------------	---

5.2 Вовед во виртуелни валути

5.2.1 Повеќе терминологија за виртуелните валути⁹⁵

Криптовалута	Значи математичка децентрализирана виртуелна валута заштитена со криптографија, т.е. вклучува принципи на криптографија за да спроведе дистрибуирана и децентрализирана економија со безбедни информации. Криптовалутата употребува јавни и приватни клучеви за пренос на вредност од едно лице (физичко или правно) на друго и секој пренос треба да се потпише криптографски. Безбедноста, интегритетот и салдирањето на книгите на криптовалутите се обезбедува со мрежа на страни без меѓусебна доверба (кај <i>Bitcoin</i> тие се викаат рудари) коишто ја штитат мрежата во замена за можноста да добијат безредно дистрибуиран хонорар (кај <i>Bitcoin</i> , мал број новозодадени биткоини наречени „награда од блок“, а во некои случаи и провизиите што ги плаќаат корисниците, се поттик за рударите да ги вклучат тие трансакции во следниот блок). Дефинирани се стотици спецификации на криптовалути, главно изведени од <i>Bitcoin</i> , каде што се користи систем на доказ за работа за да се потврдат трансакциите и да се одржи низата од блокови наречена блокчејн. <i>Bitcoin</i> го даде првиот целосно спроведен протокол за криптовалута, но има сè поголем интерес за развивање алтернативни, потенцијално поефикасни методи за доказ, како на пример системи засновани на доказ за влог.
Bitcoin	Влезе во функција во 2009-та година и беше првата децентрализирана конвертибилна виртуелна валута и првата криптовалута. Биткоините се пресметковни единици составени од уникатни низи броеви и букви што претставуваат единици на валутата и имаат вредност единствено затоа што корисниците би платиле за нив. Корисниците тргуваат со биткоините дигитално и со голем степен на анонимност; тие може да се разменуваат (купуваат или повлекуваат) во американски докари, евра и други обични или виртуелни валути.
Etherum	Единствената криптовалута (со исклучок на нејзината гранка <i>Ethereum Classic</i>) што вклучува цел програмски јазик. Тоа може да се користи за создавање паметни договори - автоматски процедури, каде што се врши исплата штом се исполнат претходно утврдени услови.

⁹⁵ Извештај на FATF, Виртуелни валути, главни дефиниции и потенцијални ризици за перење пари/финансирање тероризам, јуни 2014. Достапно на: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

Altcoin	Значи која било математичка децентрализирана виртуелна валута, освен биткоините, првобитната таква валута. На пример, <i>Ripple</i> , <i>Peercoin</i> , <i>LiteCoin</i> , <i>Zerocoin</i> , <i>Anoncoin</i> и <i>Dogecoin</i> .
Monero	Создадена е во април 2014, и е криптовалута со отворен код што дава можеби највисоко ниво на приватност преку неколку технологии што го прават традиционалното следење неделотворно бидејќи и појдовните и целните адреси се скриени. Износот на трансакцијата е скриен. Приватните карактеристики на трансакциите се однапред зададени.
Точка	Компјутер што ги праќа трансакциите преку мрежата на <i>Bitcoin</i> до други точки.
Приватен клуч	Тајниот клуч овозможува да се вршат трансакции во биткоини и се користи да се создаде потпис за трансакцијата којшто не може да се фалсификува. Сопственикот на приватниот клуч ги контролира биткоините.
Јавен клуч	Јавно познат клуч изведен од приватниот клуч.
Трансакции во биткоини	Биткоините се пренесуваат од една адреса на друга. Кога се врши трансакција, корисникот користи <i>Bitcoin</i> паричник инсталиран на својот компјутер или сервис на интернет што ги нуди релевантните функционалности. Трансакцијата во биткоини е еднократна трансакција што не може да се преобрати. Трансакциите во биткоини се транспарентни и може да се видат на Интернет на разни начини. Може да се видат податоци како <i>Bitcoin</i> адресата на испраќачот, <i>Bitcoin</i> адресата на примачот, и износот на биткоини во трансакцијата.
Заплена	Движење на биткоини од адреса на осомничениот до адреса што ја контролираат органите на прогонот.
Анонимизатор (инструмент за анонимизирање)	Значи инструменти и услуги наменети да го скријат изворот на трансакцијата во биткоини и да овозможат анонимност.
Миксер (сервис за перење, тамблер)	Ова име го добива видот анонимизатор што го крие синцирот на трансакции во низата блокови на начин што ги поврзува сите трансакции од истата <i>Bitcoin</i> адреса и ги праќа заедно на начин да изгледа како да се пратени од друга адреса. Миксерот или тамблерот праќа трансакции преку сложена и полу-безредна низа фантомски трансакции, и така е особено тешко да се поврзат конкретни виртуелни средства (адреси) со конкретна трансакција. Миксерите функционираат по упатства од корисникот да се пратат средства на дадена <i>Bitcoin</i> адреса. Миксерот потоа ја меша оваа трансакција со други кориснички трансакции за да стане нејасно кому сакал корисникот да му ги прати средствата.
Tor (Onion рутер)	Тоа е името на подземна дистрибуирана мрежа од компјутери на Интернет којашто ја крие вистинската IP адреса, а со тоа и идентитетот на корисниците на мрежата преку пренасочување на комуникацијата низ повеќе компјутери по целиот свет и обвиткување во повеќе слоеви екрипција.
Dark паричник	Тоа е паричник инсталиран како додаток на пребарувачот, чијашто цел е да ја обезбеди анонимноста на трансакциите во биткоини со вклучување на следните карактеристики: авто-анонимизатор (миксер), децентрализирано тргување,

	платформи за <i>crowdfunding</i> без цензура, платформи и пазари на црно за информации, и децентрализирани пазари како <i>Silk Road</i> .
Ладно чување	Тоа е <i>Bitcoin</i> паричник што не е поврзан на интернет. Ладното чување е наменето да помогне во заштитата на зачуваната виртуелна валута од хакирање и кражба.
Топло чување	<i>Bitcoin</i> паричник на интернет, обратно од ладното чување.
Локален систем за размена и тргување (Local Exchange Trading Sytem - LETS)	Тоа е локално организирана економска организација што им овозможува на членовите да разменуваат стоки и услуги со други во групата. <i>LETS</i> користи локално создадена валута за искажување вредносни единици коишто може да се тргуваат или разменуваат за стоки и услуги. Теоретски, биткоините може да се усвојат како локална валута што се користи со <i>LETS</i> .

5.2.2 Учесници во виртуелната валута

Менувач (или берза за виртуелни валути)	Тоа е лице или субјект чијашто дејност е размената на виртуелни валути за реални валути, средства, или други облици на виртуелни валути, како и благородни метали, и обратно, за провизија. Менувачите генерално прифаќаат разни видови плаќање, вклучително и готовина, електронски трансакции, кредитни картички и други виртуелни валути, и може да се поврзани со администраторот, неповрзани, или од трето лице. Менувачите може да работат како берза или менувачница. Поединците вообичаено користат менувачи да депонираат или повлечат средства од сметките во виртуелна валута.
Администратор	Тоа е лицето или субјектот чијашто дејност е да емитира (да пушта во оптек) централизирана виртуелна валута, да утврдува правила за нејзината употреба, да води централен платен регистар, и има овластување да ја откупува (повлекува од оптек) виртуелната валута.
Корисник	Лице или субјект што стекнува виртуелна валута и ја користи за да купи вистински или виртуелни стоки или услуги, или праќа преноси во лично својство кон друго лице (за лична употреба), или ја држи виртуелната валута како (лична) инвестиција.
Рудар	Тоа е лице или субјект што учествува во децентрализираната мрежа на виртуелната валута со употреба на специјален софтвер за решавање сложени алгоритми во дистрибуиран систем за доказ за работа или друг дистрибуиран систем за доказ што се користи за потврдување трансакции во системот на виртуелната валута. Рударите може да бидат корисници ако самите произведуваат конвертибилна виртуелна валута исклучиво за свои цели. Рударите може да учествуваат во системот на виртуелната валута и како менувачи, да ја создаваат виртуелната валута како дејност со цел да ја продадат за обични пари или друга виртуелна валута.
Паричник за виртуелна валута (клиент)	Тоа е средство (софтверска апликација или друго) за држење, чување или пренос на биткоини или друга виртуелна валута.

Давател на услуги за паричници

Тоа е субјект што нуди паричници за виртуелни валути за држење, чување или пренос на биткоиини или друга виртуелна валута. Паричникот ги има приватните клучеви на корисникот коишто му овозможуваат на корисникот да ја троши виртуелната валута доделена на таа адреса за виртуелна валута во низата блокови. Давателот на услуги за паричници го помага учеството во системот на виртуелната валута со тоа што им овозможува на корисниците, менувачите и трговците полесно да ги вршат трансакциите во виртуелна валута. Давателот на услуги за паричници го води салдото на виртуелна валута на клиентот и вообичаено нуди и чување и безбедност на трансакциите.

И други субјекти може да учествуваат во систем на виртуелна валута и може да се поврзани или независни од менувачите и/или администраторите. Тие се, меѓу другите, даватели на услуги за веб-администрација (т.е. веб-администратори), обработувачи на плаќања од трети лица (помагаат прифаќање на трговците), програмери и даватели на апликации.

5.2.3 Bitcoin

Bitcoin е децентрализирана мрежа за плаќање од корисник на корисник (*peer-to-peer*), чијшто двигател се корисниците без централен орган и посредници. Сатоши Накамото ги има објавено првата спецификација за *Bitcoin* и концептот за доказ до криптографска група во 2009-та година⁹⁶. Во суштина, намената и работата на мрежата *Bitcoin* е водење и споделување јавен регистар на плаќања, познат како низа блокови или блокчејн (*blockchain*). Тој регистар ја содржи секоја трансакција од самиот почеток и со него се потврдува верноста на секоја трансакција⁹⁷. Интегритетот и хронолошкиот редослед на трансакциите во регистарот се одржуваат криптографски. Биткоините се конвертибилна, децентрализирана виртуелна валута, односно криптовалута.

Овде ќе дадеме опис како функционира виртуелната валута *Bitcoin*.

5.2.3.1 Пренесување вредност

Најочигледното прашање за виртуелната валута е како корисниците на валутата си пренесуваат вредност еден на друг. Во случајот на *Bitcoin*, секој корисник има една или повеќе *Bitcoin* адреси. Корисникот може да има колку сака *Bitcoin* адреси, па ако сака, дури и посебна адреса за секоја трансакција. Во пракса, софтверот и услугите за *Bitcoin* ги претставуваат биткоините на корисникот како да се чуваат во „паричник“. Паричникот може да претставува една *Bitcoin* адреса или повеќе адреси, во зависност од конкретните карактеристики на тој софтвер или услуга. Адресата служи како единствена идентификациска вредност со која се прикажува сопственоста на извесни биткоиини⁹⁸. За лицето А да му прати пари на лицето Б, праќа порака до мрежата *Bitcoin* со адресата на испраќачот, адресата на примачот, и износот на преносот во биткоиини. Секоја точка во *Bitcoin* мрежата што ќе ја добие оваа порака, ја ажурира својата копија од регистарот и ја пренесува пораката за трансакцијата до други точки.

⁹⁶ <https://bitcoin.org/en/faq>

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

⁹⁸ Строго гледано, секоја адреса е пар од јавен и приватен клуч. Јавниот клуч е адресата. Приватниот клуч е таен и се користи за дигитално потпишување на трансакциите со адресата, па со тоа и се потврдува автентичноста на трансакцијата.

За да се спречи напаѓачот лице В да прати порака во обид да пренесе биткоиини од паричникот на лицето А во паричникот на лицето В, автентичноста на трансакциите се обезбедува со присуството на дигитален потпис од лицето А. За да се создаде валидна порака за трансакција со којашто се пренесуваат биткоиини од паричникот на лицето А, лицето што ја создава пораката треба да ја има лозинката поврзана со приватниот клуч на паричникот.

5.2.3.2 Докажување сопственост

Како може примачот, лицето Б во примерот погоре, да знае дека добиените биткоиини му припаѓале на лицето А? За да се конструира валидна порака за пренос на биткоиини, испраќачот на биткоиините треба да докаже дека е моменталниот сопственик на тие биткоиини.

Да речеме дека лицето А му праќа пет биткоиини на лицето Б. Лицето А во трансакцијата треба да вклучи референци на претходни трансакции каде што примачот во трансакцијата било лицето А, и вкупната вредност на претходните трансакции била поголема од пет биткоиини. Тие се нарекуваат влезни податоци во трансакцијата.

Сите корисници на *Bitcoin* мрежата водат копија од регистарот (*blockchain*) којшто ја содржи историјата на сите претходни трансакции. Лицето Б тогаш може да потврди дека биткоиините наведени во влезните податоци на трансакцијата на лицето А навистина му припаѓаат на лицето А. За да се поедностави овој процес, има правила дека трансакциите мора да се салдираат. Со други зборови, бројот на биткоиини во влезните податоци на една трансакција мора да биде еднаков на бројот на биткоиини во излезните податоци на таа трансакција. Ако има неусогласеност, лицето А може да си го префрли преостанатото салдо од влезните податоци на себе.

5.2.3.3 Двојно трошење

Во *peer-to-peer* мрежа како *Bitcoin* мрежата нема гаранција дека редоследот во којшто трансакциите ги прима некоја точка во мрежата го претставува истиот редослед по којшто се направени. Практично гледано, тоа носи можност лицето А да состави порака за трансакција да му прати биткоиини на лицето Б и потоа истовремено да состави втора порака за трансакција да му прати биткоиини на друго лице. Тоа се нарекува двојно трошење. Сосема е можно некои точки во *Bitcoin* мрежата прво да ја добијат втората трансакција. Кога првата трансакција ќе пристигне кај тие точки подоцна, таа ќе се смета за неважечка затоа што повторно користи влезни податоци што се веќе употребени, од нивна перспектива, во друга трансакција. Главниот технолошки исчекор на протоколот на *Bitcoin* е механизмот со којшто се решава ова прашање.

Трансакциите се собираат во групи, наречени блокови, и блоковите се поврзани во низа блокови наречена блокчејн (*blockchain*). Трансакциите во еден блок се смета дека се случиле во исто време. Блоковите се редат така што секој блок упатува на претходниот во низата. Трансакциите што сè уште не се во блок се нарекуват непотврдени. Секоја точка во мрежата може да собере група непотврдени трансакции, да ги собере во блок и да ги предложи како следниот блок во низата. Предложениот блок мора да содржи решение на сложен математички проблем што компјутерски

тешко се пресметува⁹⁹. *Bitcoin* мрежата динамички ја приспособува тежината на математичкиот проблем, така што се додава нов блок во низата во просек на десет минути¹⁰⁰.

Иако е тешко веројатно, може да се случи повеќе точки во *Bitcoin* мрежата да предложат блокови во приближно исто време. Во тој случај, низата блокови привремено се разгранува кога различни точки во мрежата додаваат различни блокови во низата. Ситуацијата се решава кога ќе се додаде следниот блок во низата. Како што веќе рековме, новиот блок содржи референца на претходниот блок во низата. Така ќе се прикачи на една од двете можни гранки во низата и едната гранка ќе биде подолга. Правилото на *Bitcoin* мрежата е дека точките треба да се префрлат на најдолгата достапна гранка и резултатот е дека низата многу брзо се стабилизира. Понатаму, сите точки се согласуваат за сите блокови што се неколку блока поназад од крајот на низата. Затоа се смета дека е побезбедно да се почека извесно време пред да се испорача стока врз основа на пренос на биткоини. За секој блок требаат околу десет минути да се додаде на низата, па да се почекаат шест блока значи да се почека еден час.

5.2.3.4 Копање

Гореописаниот процес на додавање блокови и нивно прикачување на низата блокови се нарекува копање. Секој што ќе го реши блокот и ќе го додаде на низата добива награда од 25 биткоини. На секои четири години наградата за еден блок се преполовува сè додека нема веќе да се емитираат биткоини. Ќе се создадат вкупно 21 милион биткоини.

Згора на наградата во биткоини, рударите може да добијат и провизија што по избор се вклучува во трансакциите. Моментално главната награда за копање е наградата за блокот, но со тек на времето, провизиите за трансакции ќе станат стимул за копање.

Најголем дел од копањето не го вршат поединци, туку организирани групи наречени рударски групи. Наградата за пресметување на блокот ја делат членовите на групата сразмерно со компјутерската моќ што секој член ја дал во групата.

5.3 Ризици од виртуелни валути

Конвертибилните виртуелни валути што може да се разменат за вистински пари или други виртуелни валути се потенцијално ранливи на злоупотреба за перење пари и финансирање тероризам поради повеќе причини. Во овој дел ќе ги опишеме наброените ризици во однос на овие две закани за финансискиот интегритет¹⁰¹.

Прво, тие овозможуваат поголема анонимност од традиционалните безготовински начини за плаќање. Системите за виртуелни валути може да тргуваат на Интернет, генерално ги карактеризира далечинскиот однос со клиентите, и тие може да дозволат

⁹⁹ Точката што го создава блокот треба да најде нумеричка вредност што кога ќе се искомбинира со другите податоци од блокот, на добиените комбинирани податоци им дава криптографска хаширана вредност под извесен праг.

¹⁰⁰ Тоа се постигнува преку намалување на прагот во пресметката на хашираната вредност, што значи дека има помал број прифатливи одговори и со тоа идентификацијата на валидна вредност е отежната.

¹⁰¹ Европското тело за банкарски надзор - EBA, има изготвено одличен документ каде што се набројуваат ризиците кон финансискиот систем што ги претставуваат виртуелните валути. Достапно на: <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>

анонимно финансирање (финансирање во готово или од трети страни преку виртуелни менувачи што не го откриваат соодветно изворот на финансирање). Тие може да дозволат и анонимни преноси ако испраќачот и примачот не се соодветно идентификувани. Децентрализираните системи се особено ранливи на ризици од анонимност. На пример, *Bitcoin* адресите, кои функционираат како сметки, по природа немаат имиња, ниту друга идентификација на клиентот, а системот нема главен сервер или давател на услуги. *Bitcoin* протоколот не бара, ниту дава идентификација и потврда на учесниците, ниту пак создава историски запис на трансакциите поврзани со реалниот идентитет.

Нема централно надзорно тело, ниту софтвер за спречување перење пари за следење и откривање шеми на сомнителни трансакции. Органите на прогонот не можат да одат на една главна локација или субјект (администратор) за истражување и заплена на средства (иако властите може да одат кај поединечни менувачи по информации за клиентот што менувачот можеби ги собира). Така се нуди ниво на потенцијална анонимност што е невозможно со традиционалните кредитни и дебитни картички или поетаблирани платни системи на Интернет, како на пример *PayPal*. Глобалното присуство на виртуелните валути исто така го зголемува потенцијалот за ризик од перење пари/финансирање тероризам.

До системите за виртуелни валути се пристапува преку Интернет (вклучително и преку мобилни телефони) и тие може да се користат за прекугранични плаќања и пренос на средства. Згора на тоа, виртуелните валути вообичаено се потпираат на сложена инфраструктура што вклучува неколку субјекти, често расфрлани во повеќе земји, за пренос на средства или извршување плаќања. Таквата поделба на услугите значи дека може да не е јасна одговорноста за следење на правилата за перење пари/финансирање тероризам и за надзор/извршување. Освен тоа, записите за клиентите и трансакциите може да се чуваат кај различни субјекти, често во различни јурисдикции, со што се отежнува пристапот до нив на органите на прогонот и регулаторите. Овој проблем се влошува со брзиот развој на технологијата и деловните модели со децентрализирани виртуелни валути, вклучително и променливиот број и видови/улоги на учесници што даваат услуги во платните системи со виртуелни валути. Важно е дека елементи од системот на виртуелната валута може да се наоѓаат во јурисдикции што немаат соодветни контроли за перење пари/финансирање тероризам. Централизираните системи за виртуелни валути може да учествуваат во перење пари и намерно да бараат јурисдикции со слаб режим за перење пари/финансирање тероризам. Децентрализираните конвертибилни виртуелни валути што дозволуваат анонимни трансакции од лице до лице може да се чини дека постојат во дигитален свет сосема вон дофатот на која било конкретна земја.

Оценката на *FATF* за ризикот од виртуелни валути¹⁰² укажува дека барем краткорочно, единствено конвертибилните виртуелни валути што може да се користат да пренесуваат вредност во и од обични пари и регулираниот финансиски систем може да претставуваат ризик за перење пари/финансирање тероризам. Следствено, според пристапот заснован на ризик даден во референтниот извештај, земјите треба да ги концентрираат напорите за спречување перење пари/финансирање тероризам на високоризични конвертибилни виртуелни валути.

Оценката на ризикот налага и дека контролите за спречување перење пари/финансирање тероризам треба да се занимаваат со точки за конвертибилни

¹⁰² Виртуелни валути - Водич за пристап заснован на ризик, Работна група за финансиска акција, јуни 2015. Достапно на: <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>

виртуелни валути, т.е. пресечни точки што претставуваат врати во регулираниот финансиски систем, а не да одат на регулирање корисници коишто стекнуваат виртуелни валути за да купуваат стоки или услуги. Тие точки вклучуваат, меѓу другото, трети лица коишто менуваат конвертибилни виртуелни валути. Во тој случај, тие треба да се регулираат според препораките на FATF¹⁰³. Земјите треба да размислат на менувачите на конвертибилни виртуелни валути да им се наметнат релевантните услови за спречување перење пари/финансирање тероризам наведени во меѓународните стандарди, како и на секоја друга институција што функционира како точка каде што активностите на конвертибилните виртуелни валути доаѓаат во допир со регулираниот финансиски систем на обични пари.

Според пристапот заснован на ризик на FATF, земјите може да размислат да ги регулираат финансиските институции или другите субјекти коишто праќаат, примаат и чуваат виртуелни валути, но не нудат услуги за размена или депонирање/повлекување меѓу виртуелните и обичните пари.

Измените и дополнувањата на петтата Директива¹⁰⁴ за спречување перење пари ќе ги стават платформите за размена на виртуелни валути и сервисите за паричници во рамките на прописите за спречување перење пари што ги наметнува Директивата што дефинира „субјекти со обврски“.

ПРАШАЊА ЗА РАЗМИСЛУВАЊЕ

1. Каде се случува размената од виртуелна валута во вистинска валута?
2. Како се идентификуваат страните во трансакцијата во системот на виртуелната валута *Bitcoin*?
3. Која суштинска карактеристика на децентрализираните виртуелни валути ги прави тешки за регулирање?
4. Како се вика јавниот регистар на трансакции во биткоиини?

5.4 Предизвици на истрагите¹⁰⁵

5.4.1 Сознание дека се користеле виртуелни валути

Првиот предизвик на истрагите со виртуелни валути е да се открие употребата на виртуелни валути и/или дали средства од криминал се чуваат во облик на виртуелна

¹⁰³ За да се избегне сомнеж, Препораки од FATF - Меѓународни стандарди за сузбивање перење пари и финансирање тероризам и ширење, Работна група за финансиска акција, февруари 2012. Достапно на: <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_TITLE=&CONTENTS=&DOC_ID=15849%2F17&DOC_INTERINST=&DOC_SUBJECT=&DOC_SUBTYPE=&DOC_DATE=&document_date_from_date=&document_date_to_date_submit=&document_date_to_date=&document_date_to_date_submit=&MEET_DATE=&meeting_date_from_date=&meeting_date_to_date_submit=&meeting_date_to_date=&meeting_date_to_date_submit=&DOC_LANCD=EN&ROWS=25&NRROWS=500&ORDERBY=DOC_DATE+DESC

¹⁰⁵ Имајте редвид дека дискусијата што следи на некои места упатува на *Bitcoin* како пример за децентрализирана виртуелна валута. Предизвиците што се дадени тука важат за најголем дел од виртуелните валути, а особено децентрализираните виртуелни валути.

валута. Кај виртуелните валути, приказот на вредноста е речиси секогаш во целосно електронски облик¹⁰⁶.

Затоа истражителите треба да се свесни за можноста средствата од криминалот да се претворени во виртуелна валута. Дигиталните форензичари исто така треба да имаат технички капацитет и способност да разберат каде/како да ги бараат виртуелните валути на заплениети носачи за електронско чување.

5.4.2 Анонимност на трансакцијата

Уште од почетокот на дистрибуираните виртуелни валути, една од често спомнуваните карактеристики на нивното работење е наводната анонимност на трансакциите. Затоа можеби клучниот истражен предизвик за *Bitcoin* е поврзувањето на активностите на конкретен *Bitcoin* паричник со вистинско лице.

И покрај тоа што сите трансакции во биткоиини и содржината на паричниците се видливи за сите во низата блокови, ако го немате приватниот клуч, не можете да му пратите биткоиини на друг имател на сметка¹⁰⁷. Сепак, вистинското лице што има конкретен приватен клуч не се открива преку вршењето на трансакција со биткоиини.

Откриени се техники коишто во извесни околности овозможуваат да се поврзат *IP* адреси со конкретни трансакции¹⁰⁸. Една од првите техники за откривање е дадена во академски труд објавен од Филип и Дијана Коши во 2014-та година¹⁰⁹. Тие изградиле своја верзија на *Bitcoin* софтверот и презеле копија на секој пакет податоци што го пренел секој компјутер во *Bitcoin* мрежата. Преку анализата на овие податоци, тие успеале да откријат извесни шеми на податоци што овозможуваат да се откријат *IP* адресите зад конкретни трансакции со биткоиини. Сепак, сега засега, тие техники тешко веројатно се достапни за мнозинството кривични истраги поради компјутерските предизвици.

5.4.3 Откривање на изворот на средства

Во истрагите каде што е утврдено дека се користеле виртуелни валути, некогаш можеби ќе треба да се утврди дека средствата се стекнати нелегално. Осомничениот може да се испита за тоа, но во случаи кога осомничениот не соработува и/или осомничениот сè уште не е свесен дека е под истрага, може да е тешко да се утврди како биле купени виртуелните валути.

Во овој контекст, помошта од приватниот сектор е клучна. Менувачите на виртуелни валути коишто соработуваат¹¹⁰ ќе можат да дадат информации за поединечни клиенти, вообичаените имиња за чување, проверените детали за контакт, *IP* записите, записите за активност, сите адреси за виртуелни валути што ги користи корисникот на берзата, личните пораки, информациите за плаќањата, доказ за лична идентификација и доказ за домашна адреса.

¹⁰⁶ Има некои организации што продаваат физички варијанти на вредноста на виртуелната валута, но тие се мошне невообичаени и без широка употреба. Видете, на пример <http://www.coindesk.com/10-physical-bitcoins-good-bad-ugly/>

¹⁰⁷ Видете го примерот во биткоиини погоре за опис како функционира *Bitcoin*.

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

¹⁰⁹ Анализа за анонимноста во *Bitcoin* преку користење сообраќај преку *P2P* мрежа, *Koshy* и слично. http://fc14.ifca.ai/papers/fc14_submission_71.pdf

¹¹⁰ Усогласените субјекти според законодавството за спречување перење пари/финансирање тероризам не се ограничени на менувачите на виртуелни валути; агенти за обработка на плаќања, паричници на интернет, интернет странци за игри и други сервиси на Интернет може исто така да помогнат во истрагите.

Со користење на процедуралните овластувања што ги дава Конвенцијата од Будимпешта за компјутерски криминал се овозможува пристап до податоци што ги имаат менувачите и други учесници во екосистемот на виртуелните валути (на пример, преку наредби за сочувување, прибирање податоци за сообраќај во реално време итн.).

Предизвикот да се открие изворот на средствата во трансакција на биткоини е дотолку потежок поради употребата на миксери. Тие сервиси функционираат така што прифаќаат трансакции од повеќе лица, ги делат префрлените средства во мали износи и ги мешаат со средства префрлени од други корисници на услугата. Тоа значи дека од аспект на примачот на средствата, првобитниот извор на средствата е во најмала рака многу скриен и е можеби целосно анонимизиран¹¹¹.

5.4.4 Повлекување/реализација и конверзија на приходите

Во моменот кога вредноста претставена во виртуелни валути се конвертира во обични пари, постои можност за органите на прогонот. Конверзијата вообичаено се случува на берза за виртуелни валути и затоа препораките на *FATF* за виртуелни валути, на коишто кусо се осврнавме и упативме во Дел 5.3, се концентрираат на регулирањето на точките за виртуелни валути. „Точки“ во овој контекст ги означува местата каде што светот на виртуелните валути доаѓа во допир со традиционалниот финансиски свет, којшто ги вклучува, меѓу останатите, и берзите за виртуелни валути.

Онаму каде што берзите за виртуелни валути се регулирани, тие треба да преземат мерки за проверка да ги идентификуваат своите клиенти. Во конкретниот случај на *Bitcoin*, сите трансакции се јавно достапни во низата блокови. Тоа значи дека во случаи каде што органите на прогонот се свесни дека извесна адреса за виртуелни валути е под контрола на некој осомничен, преку анализа на трансакциите извршени од страна на осомничениот можно е да се открие употребата на некоја берза за виртуелни валути. Во такви случаи, органите на прогонот може да достават судска наредба до соодветната берза за виртуелни валути да ги открие деталите на клиентот, како на пример, идентификација, домашна адреса, *IP* адреси, и-мејл адреси, телефонски број, историја на трансакции, адреси за депонирање и подигнување, име на банка, број на сметка и информации за трансакциите.

На пример, во јануари 2016-та година во Холандија биле уапсени десет лица во рамки на меѓународна акција против нелегални пазари за дрога на интернет. Лицата биле фатени како ги менуваат своите биткоини во евра на банкарски сметки преку комерцијални сервиси за *Bitcoin*, а потоа подигнуваат милиони во готово од банкомати. Наводно, трагата од *Bitcoin* адреси ги поврзала парите со нелегалната продажба на дрога на интернет што ја следеле *FBI* и *Interpol*. *FATF*, во извештајот од 2014-та година за виртуелни валути („Виртуелни валути: главни дефиниции и потенцијални ризици за перење пари/финансирање тероризам“), дава пример на дрги познати акции на органите на прогонот за виртуелни валути.¹¹² Секој што го интересира тоа, може да ги разгледа тие примери за да научи повеќе за обемот и комплексноста на претходните истраги со виртуелни валути.

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

¹¹² Извештај на *FATF*, Виртуелни валути, главни дефиниции и потенцијални ризици за перење пари/финансирање тероризам, јуни 2014. Достапно на: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

Сепак, како што кажавме и претходно, и понатаму има предизвици поради глобалната природа на виртуелните валути. Тие предизвици се разни, од фактот дека берзите за виртуелни валути се различно регулирани во целиот свет, па до практичните потешкотии сврзани со меѓународните истраги.

5.5 Предизвици за замрзнување/заплена

5.5.1 Виртуелни валути како приходи од криминал

Во многу земји не треба да се наведе природата на приходите од криминал. Во такви случаи, резервата на вредност како биткоини треба да се смета како приходи од криминал ако приходите се стекнати од криминална активност. Сепак, тоа треба да се утврди во дадената јурисдикција.

5.5.2 Откривање на постоењето на виртуелна валута

Првиот предизвик е да се открие постоењето на виртуелна валута и да се утврди дека е под контрола на осомничениот. Некои од прашањата што произлегуваат овде веќе ги дискутиравме во Дел 5.4. Постоењето и контролата на виртуелната валута може да биде очигледно, на пример, од набљудување, посебни истражни мерки, па дури и признанија.

5.5.3 Замрзнување/преземање контрола на виртуелна валута

Откако ќе се открие дека приходите од криминал се чуват во облик на виртуелни валути, следното прашање е да се имобилизира виртуелната валута и да се пречи таа да исчезне. Дел од предизвикот при замрзнувањето на виртуелната валута е нејзината виртуелна природа, што значи дека може да постојат многу копии на паричникот со виртуелната валута. Дури и во случаи кога еден паричник на Интернет е запленил или кога е запленил паричник што стои на компјутерот на осомничениот, тоа не дава сигурност дека виртуелната валута е тргната вон контролата на осомничениот. Се случува осомничениот да има резервни клучеви/паричник на друго место во Облакот (простор за чување на Интернет). Затоа, обидите да се контролира паричникот со виртуелна валута на осомничениот не даваат сигурност дека средствата се тргнати вон контролата на осомничениот.

Треба да се нагласи дека виртуелните валути не се чуваат на самиот уред. Во случајот на биткоините, приватниот клуч е она што овозможува некому да ги троши. Има два главни начини да се запленил биткоини, и тоа преку пристап до приватниот клуч на осомничениот или преку соработка со приватниот сектор (на пример, менувачи) што го контролира приватниот клуч на осомничениот. Кога истражителите ќе го добијат приватниот клуч на осомничениот, за да се заврши запленил, тие средства треба да се пренесат затоа што осомничениот или друго лице што го контролира приватниот клуч може да ги пренесе средствата на друга адреса. Средствата треба да се пренесат на *Bitcoin* адреса што ја контролираат органите на прогонот (истражители или јавното обвинителство). Треба да се има предвид дека постапката зависи од постојното домашно законодавство.

Обвинителот може да прибави судска забрана или посебна наредба за замрзнување да ги спречи осомничениот или неговите полномошници да ја тргнат виртуелната валута. Тоа нема да ги спречи ополномоштените лица во странство, каде што наредбата можеби нема дејство, да ја префрлат или тргнат виртуелната валута.

Ако е тоа можно, обвинителството теба да се обиде да го ликвидира салдото во виртуелна валута што е можно поскоро (в. Дел 5.5.4). Тоа бара навремено извршување на постапката за преземање контрола на средствата, во случај осомничениот да има пристап до резервна копија на целниот паричник со виртуелна валута. Освен тоа, виртуелните валути често имаат нестабилна вредност и преку ликвидирањето и пренесувањето на салдото на владина сметка се обезбедува да се сочува вредноста што ја претставува виртуелната валута во времето на истрагата и таа да биде достапна за евентуално конфискување во случај на осудителна пресуда.

5.5.4 Управување со средства

Препорачаната најдобра практика е да се ликвидира вредноста во виртуелна валута. Тоа се заснова на потребата да се задржи вредноста на заплнатите стоки (на пример, како кога се заплнуваат хартии од вредност и девизи во готово). Така се сочувува вредноста на средствата и таа се штити од нестабилноста на пазарот. Исто така, тоа е гаранција дека виртуелната валута не може да се премести, префрли или тргне вон дофатот на судот. Повеќето јурисдикции имаат одредба во законодавството да се ликвидираат средствата за да се сочува вредноста за евентуално конфискување, меѓутоа тоа треба да се утврди во вашата конкретна јурисдикција.

Директивата на ЕУ за конфискување¹¹³ препорачува да се формира служба за управување со заплнети и конфискувани средства¹¹⁴. Ако во вашата јурисдикција има формирано таква служба, можеби вреди да се запознаете со капацитетите на таа служба да ликвидира вредност што се чува во виртуелна валута. А, ако не постои таква служба, можноста да се ликвидира вредност во виртуелна валута ќе зависи од капацитетот на утврдените процедури за управување со средства пред конфискување.

ПРАШАЊА ЗА РАЗМИСЛУВАЊЕ

1. Зошто е најдобра практика да се ликвидира виртуелната валута што поскоро?
2. Дали во вашата јурисдикција е потребно да се утврди нелегалниот извор на дадени приходи од криминал? Ако е така, како може да се направи тоа во случај на виртуелна валута?
3. Кои се условите да се добие наредба за заплена на виртуелна валута?
4. Кои мерки може да се употребат за да се открие постоењето или употребата на виртуелни валути? Кои се заштитни мерки се уредени за да се заштитат интересите на невини трети лица?

¹¹³ Директива 2014/42/ЕУ на Европскиот парламент и Совет од 3-ти април 2014 за замрзнување и конфискување инструменти и приходи од криминал во Европската унија.

¹¹⁴ *Ibid* Преамбула став 32.

6 Практична работа/Примери

6.1 Пребарување литература

Ве молиме да упатите на релевантните членови од вашето домашно законодавство и релевантната судска пракса, со кус опис, во однос на следните точки:

1. Конфискување приходи од криминал како обврска според Кривичниот законик или Законот за кривична постапка/специјалниот закон.
2. Дефиниција на финансиска истрага, кога се одвива финансиската истрага, кој ја води финансиската истрага?
3. Пристап до банкарски податоци и следење банкарска сметка.
4. Дефиниција и употреба на посебни истражни мерки.
5. Пристап до други бази на податоци за сопственост (катастар, регистар на возила, и сл.)
6. Наредба за замрзнување.
7. Одлука за конфискување.
8. Режим на конфискување (кривична постапка, конфискување засновано на вредност, проширено конфискување, презумпција на нерамнотежа, конфискување незасновано на осудителна пресуда (*in rem*)).
9. Заемна правна помош.
10. Специјализирани институции.
11. Формирање работна група (обвинителство, полиција, УФР, даночни служби, царина).
12. Пристап до податоци за претплатникот (IP адреса, интернет страница, и-мејл).
13. Пристап до податоци за сообраќајот и содржината.
14. Барање за сочувување.
15. Заплена на електронски докази.

6.2 Пример 1: Разгледување на правната основа за дејство

Вашата полиција повела истрага против осомничените А, Бе и Це коишто формираат организирана криминална група за да им продадат големо количество марихуана на купувачите Де и Е.

Преку тајни мерки (тајно набљудување и набљудување телекомуникации), утврдено е дека на 15-ти октомври 2016 лицето А му доставило 1 кг марихуана на лицето Де, коешто платило 1.000 евра во готово во куферче. Овластено е одложување на заплена и апсењето. Истиот ден лицето А му го доставило куферчето со парите на лицето Бе. Понатаму е утврдено дека лицето А по телефон се договорило со лицето Е да му продаде 2 кг марихуана, за коишто ќе се префрлат 2.000 евра на банкарската сметка број 11.

Решавате дека ви треба пристап до податоците за сопственикот на банкарската сметка број 11, вклучително и сопственикот на сметката и податоците за трансакциите во изминатите Икс месеци. Исто така, решавате дека треба да започнете следење на трансакциите на сметките на лицата А, Бе и Е.

ПРАШАЊЕ: Опишете ја правната основа во вашето домашно законодавство, посочете ги конкретните членови и условите за пристап до банкарските податоци, податоците за трансакциите, и за следењето на сметките.

Преку оваа мерка сте откриле дека лицата А, Бе и Е имаат банкарски сметки во вашата земја. Исто така, сте откриле и банкарска сметка на лицето Бе во Австрија.

Решавате да побарате судска наредба за банкарски податоци, податоци за трансакциите и следење на сметката на лицето Бе во Австрија, како и да побарате заемна правна помош за оваа работа.

ПРАШАЊЕ: Изнесете ја правната основа во вашето домашно законодавство, и посочете ги конкретните членови и условите за заемна правна помош.

Преку анализата на банкарските сметки на лицата А, Бе и Е станува јасно дека има чести трансакции меѓу лицата А и Бе, чести трансакции од лицето Е до лицето Бе, како и трансакции од лицето Бе во странство (во друга земја во регионот и во Луксембург). Ја споредувате и поврзувате динамиката на трансакциите со наодите од кривичната истрага.

Телефонското следење открива дека лицето Бе преговара со лицето Це, кое престојува во вашата земја и во друга земја во регионот, за снабдување поголемо количество марихуана за еден месец, на 15-ти декември 2016. Лицето Це бара да се плати однапред, до 1-ви декември 2016, половина од цената (100.000 евра) на банкарската сметка 22 (во сопственост на правно лице ДОО), а останатите 100.000 евра да се платат на банкарската сметка 33, во банка во Луксембург.

Решавате да побарате податоци за банкарските сметки на Це во вашата земја и во другата земја во регионот, и да дадете наредба за следење. Исто така, решавате да ја утврдите сопственоста на правното лице ДОО и неговите банкарски сметки, и да побарате податоци за трансакциите во изминатите Икс месеци и следење на сметките на ДОО.

ПРАШАЊЕ: Изнесете ја правната основа во вашето домашно законодавство, со упатување на членовите и условите за пристап до податоци за правни лица, банкарски и податоци за трансакции на правни лица, и даночни досиеја на правни лица.

Со помош на даночните служби, решавате да утврдите како работи ДОО и кои се деловните партнери. Откривате дека ДОО тргува и со индустриски коноп.

Барате документација за банкарската сметка 33 во Луксембург и гледате дека таа му припаѓа на правно лице во вашата земја во сопственост на лицето Це.

ПРАШАЊЕ: Дали има сомнеж за перење пари? Во кој момент се јавува тој сомнеж? Дали треба да ја вклучите УФР во истражната работна група? Како може да ви помогне УФР? Кои можни типологии за перење пари се користат овде? Изнесете ги правната основа, елементите и условите во вашето домашно законодавство за перење пари. Изнесете ги правната основа и условите во вашето домашно законодавство за вклучување на УФР.

Со телефонско следење се утврдува дека лицето Бе упатува на комуникација по и-мејл со лицето А, којашто содржи информации за трансакции со дрога и плаќање во биткоиини.

Решавате дека треба да се откријат и-мејл адресите на лицето А и лицето Б, како и содржината на пораките. Утврдувате дека лицето А користи и-мејл адреса кај локален интернет провајдер.

ПРАШАЊЕ: Изнесете ја правната основа во вашето домашно законодавство, и посочете ги членовите и условите за соработка со интернет провајдери и пристап до содржината на мејловите.

Преку содржината на мејлот на лицето А откривате трансакции со дрога до лицето Де и лицето Е и други лица, како и префрлање пари на банкарски сметки, но и префрлање износи во биткоиини.

Решавате да побарате помош од УФР да ги анализирате банкарските трансакции и да побарате врски и податоци за сопствениците на релевантните сметки во странство (во Австрија и Луксембург, како и во другите земји во вашиот регион).

ПРАШАЊЕ: Изнесете ја правната основа во вашето домашно законодавство, и посочете ги членовите и условите за пристап до банкарските податоци од страна на УФР и меѓународна соработка меѓу различни УФР.

Преку истрагата откривате дека следува исплата во биткоиини од лицето Це кон лицето Бе на 15-ти декември 2016. Откривате дека паричникот со биткоиини на лицето Бе се наоѓа на берза за биткоиини во Луксембург.

ПРАШАЊЕ: Изнесете ја правната основа во вашето домашно законодавство, и посочете ги членовите и условите за барање информации за претплатник од берза за биткоиини. Дали една берза за биткоиини во вашата земја би била обврзана да чува податоци и да соработува?

ПРАШАЊА:

- Кои мерки би ги презеле во врска со планираното плаќање на 1-ви декември 2016 на сметката 22 на правното лице ДОО?
- Дали однапред би наредиле замрзнување на трансакцијата? Кога се открива наредбата за замрзнување? Дали наредбата за замрзнување на трансакцијата на сметката на ДОО ја загрозува заплената на големото количество дрога што е предвидено за достава на 15-ти декември 2016?
- По апсењето на осомничените, кои мерки би се презеле во врска со готовинското плаќање на 15-ти декември 2016?
- Со оглед на тоа дека групата со лицата А, Бе и Це долго време работи со дрога, колку и кои средства може да се конфискуваат? Изнесете ја основата во вашето домашно законодавство за вашиот одговор.
- Дали правното лице ДОО може да се обвини за шверц со дрога и/или перење пари? Ако е така, изнесете ја правната основа во вашето домашно законодавство, како и условите за осудување правно лице. Посочете пример на одлука и образложение за конфискување од правно лице.

Преку анализата на и-мејл комуникацијата меѓу лицето Бе и лицето А, откривате дека групата продава дрога и преку конкретна интернет страница на Даркнетот. Тоа го потврдува и еден од купувачите којшто во текот на распитот открива како

функционира на рачунањето и доставата на дроги на Даркнетот и како се бара плаќање било на банкарска сметка или во биткоиини¹¹⁵.

ПРАШАЊЕ: Какви дејства би презеле во врска со доказите за активности на Даркнетот. Дали би можеле да почнете тајна истрага како купувач и да купите дрога, да ги откриете релевантните банкарски сметки и паричници за биткоиини, и да замрзнете пари и имот?

6.3 Пример 2: Разгледување на интеракцијата меѓу УФР и органите на прогонот

Управата за финансиско разузнавање (УФР) во вашата земја добива извештај од банка дека има сомнежи за некои трансакции што се одвиваат преку интернет банкарство. Институцијата утврдила дека се пренесени големи износи на неколку сметки, а тие износи не се вообичаени за клиентите во прашање. Освен тоа, финансиската институција забележува дека клиентите се најавуваат за интернет банкарство од IP адреси во Романија, од каде што ниту еден од клиентите се нема најавено претходно. Таквото однесување е забележано кај вкупно 20 сметки со вкупно пренеси од 750.000 евра.

УФР врши анализа и наоѓа и други извештаи за сомнителни трансакции на сметките на клиентите во други банки. УФР подготвува извештај и го испраќа до полицијата.

Истражувањето на полициските разузнавачки информации открива дека веќе тече полициска истрага за романските субјекти (всушност молдавски, но престојуваат во вашата земја) во врска со лажни документи за идентификација.

Полицијата ги апси субјектите, врши претрес на нивните простории и заплenuва неколку лаптопи. Вештачењето на лаптопите открива дека се користеле за контролирање над 200 банкарски сметки што се користеле за примање и перење пари од банкарските сметки на поединци чии компјутери биле заразени со тројанецот *Dridex*¹¹⁶, којшто ги собирал нивните податоци за интернет банкарство. Вкупниот износ испран преку овие сметки е над три милиони евра.

Осомничените се гонат и добиваат затворски казни од 8 и 5 години. Приходите од криминал не се вратени.

ПРАШАЊЕ: Која е правната основа за УФР да го пријави случајот во полиција?

Може да има законска основа за таква интеракција, но во многу случаи полицијата и УФР (и други организации како даночните власти, царината итн.) потпишуваат меморандум за разбирање што овозможува да се разменуваат информации. Основата може да зависи и од природата на пријавата во полиција. На пример, информациите што се праќаат до полицијата може да се сметаат (од страна на полицијата) за разузнавачки извештаи или кривична пријава.

¹¹⁵ Видете на пример: <https://www.bitstamp.net/help/what-is-bitcoin/>

¹¹⁶ *Dridex* е агресивен тројанец што главно се користи за крадење банкарски податоци. Малверот е конфигуриран да цели на клиенти од речиси 300 различни организации во повеќе од 40 региони. *Dridex* главно се концентрира на клиенти на финансиски институции во богати земји од англиското јазично говорно подрачје, и повеќето нападнати организации се наоѓаат во тие земји. Напаѓачите даваат приоритет и на други европски нации, како и некои региони од Азија и Пацификот.

Ве молиме да ја испитате ситуацијата во вашата земја.

ПРАШАЊЕ: Кои одредби од вашиот закон за кривична постапка се релевантни за полициската истрага?

Во врска со компјутерскиот криминал, финансиските истраги и перењето пари, има повеќе дејства што ги презема полицијата во ова сценарио; се врши претрес на лица и простории, се заплenuваат и вештачат лаптопи, се прибираат докази од компромитирани банкарски сметки.

Целта на ова прашање е да се разгледа правната основа за овие дејства во вашиот закон за кривична постапка.

ПРАШАЊЕ: Кои одредби од вашиот кривичен законик го криминализираат заразувањето со вирус на компјутер на клиент?

Ако вашата земја ја има ратификувано Конвенцијата од Будимпешта, тогаш заразувањето компјутер со вирус е криминализирано. Која е одредбата во вашиот кривичен законик каде што е пренесен релевантниот член од Конвенцијата од Будимпешта?

Ако вашата земја ја нема ратификувано Конвенцијата од Будимпешта, имате ли еквивалентни одредби? Како се криминализираат делата од компјутерски криминал?

ПРАШАЊЕ: Како би ја поврзале активноста на тројанецот *Dridex* со обвинетите?

Осомничениот имаат употребено малвер за да ги соберат лозинките за интернет банкарство. Сепак, тие лозинки се собрани од компјутерите на жртвите, а не од компјутерите на осомничените. Како ќе ја поврзете активноста на тројанецот со осомничените? Дали можете да оформите причинско-последична врска од поседувањето детали за компромитираната банкарска сметка (што може да се утврди со нивното присуство на осомничените лаптопи) до чинот на компромитирање на тие детали за сметката со тројанецот? Ако да, како би му пристапиле на тоа? Ако не, дали има и кои се импликациите за тужбата што може да се покрене против осомничените?

ПРАШАЊЕ: Како може да се утврди врквата меѓу Романците/Молдавците и контролорот на банкарските сметки каде што се пренесувале парите и лицето што го раширило вирусот? Како може да се утврди дали има имот на осомничените (во вашата земја или во странство)?

Поврзано со претходното прашање, присуството на деталите за банкарските сметки на лаптопот на осомничениот може да покаже или не дека осомничените ги контролирале банкарските сметки во моментот кога се пренесувале парите за кои станува збор. Дали тоа треба да се утврди засебно или може да се извлече од поседувањето на банкарските сметки? Ако не, што друго треба да се утврди?

ПРАШАЊЕ: Дали може да се гони за кражба преку компјутер?

Во овој случај компјутерите биле употребени како суштински дел на кражбата. Дали има одредба во вашето домашно законодавство за криминализирање на употребата на компјутерите како инструмент во кражба/измама?

ПРАШАЊЕ: Кои процедурални одредби во вашето домашно законодавство ги уредуваат прибавувањето и примената на електронски докази?

Во вакви случаи, доказите од лаптопите на осомничените може да се клучни. Кои се одредбите во вашето домашно законодавство што дозволуваат прибавување и примена на електронски докази?

ПРАШАЊЕ: Дали вашата земја има капацитети за вештачење компјутери? Како работите со капацитетите за вештачење компјутери?

Практично гледано, прибирањето и управувањето со електронски докази бара специјалистички инструменти и вештини. Како е уредено тоа во вашата земја?

ПРАШАЊЕ: Дали во овој случај треба да се води финансиска истрага? Во кој момент треба да се започне финансиската истрага?

Како што е дадено во сценариото, јасно е дека има значајни финансиски импликации поврзани со активноста на осомничените. Дали во вашата земја во овој случај може (и треба) да се води финансиска истрага? Ако да, во кој момент треба да се започне финансиската истрага?

ПРАШАЊЕ: Со кои одредби во вашето домашно законодавство се уредуваат претресот, заплена и конфискувањето средства во овој случај? Како би ги вратиле украдените пари? Дали може да ги замрзнете (преку УФР или полицијата/обвинителството)?

Сценариото вели дека осомничените добиле затворски казни. Дали домашните одредби бараат елементот за конфискување средства во постапката да се одвива по кривичната постапка или се одвива заедно со постапката?

Дали измамените жртви имаат можност да ги вратат украдените средства? Дали можете да ги обештетите жртвите ако вратите дел или сите пари? Кои одредби од домашното законодавство го овозможуваат ова?

ПРАШАЊЕ: Кои одредби од вашето домашно законодавство го опишуваат делото перење пари? Дали имало случај на перење пари?

Како е дефинирано делото перење пари во вашето домашно законодавство? Имајќи ги предвид фактите на случајот во сценариото, дали се случило дело перење пари?

ПРАШАЊЕ: Дали би гонеле и за перење пари и за кражба/измама? Зошто/зошто не?

При работата на овој случај, дали би вклучиле обвинение за делото перење пари покрај кражба/измама? Ако да, зошто? Ако не, зошто не?

ПРАШАЊЕ: Жртвите се раштркани во повеќе земји, па како би ја координирале истрагата со тие земји?

Поради безграничната природа на Интернетот, речиси сите случаи со елемент на компјутерски криминал имаат и меѓународен елемент. Во овој случај, ако има жртви

во повеќе земји, дали би се координирале со тие земји? Што ако со истрагата откриете и други жртви што биле претходно непознати?

ПРАШАЊЕ: Дали има временски рокови за поднесување докази и дали барањата за заемна правна помош би ги пробиле тие рокови? Како би го намалиле доцнењето во барањата за заемна правна помош?

Ако има меѓународен елемент, може да треба да се употреби постапката за заемна правна помош, којашто може да донесе значително доцнење во постапката. Дали времето што е потребно за постапката за заемна правна помош носи предизвици за истрагите во вашата земја? Како може да се намали тоа доцнење? Дали може, на пример, да се користат заеднички истражни тимови? Дали може да се употребат неформалните канали за комуникација да се олеснат барања пред самата заемна правна помош?

6.4 Пример 3: Интеракција во случај на компјутерски криминал/перење пари

Неколку граѓани во вашата земја пријавиле дека компјутерите им се заразени со малвер што им ги енкриптирал сите слики и документи. Малверот потоа барал исплата во биткоини за да ги декриптира сликите и документите. Во неколку случаи, граѓаните го платиле откупот.

Во текот на истрагата, полицијата стапува во контакт со УФР за да помогне да се следат биткоините. УФР успева да ги најде биткоините на берзата каде што биткоините се конвертирале во обични пари. Берзата за биткоини се наоѓа во САД.

Пратено е барање за заемна правна помош во САД, во коешто се бараат детали за профилите што ги реализирале трансакциите. Кога доаѓа одговорот од САД, се открива дека вредноста во биткоини е пренесена на банкарски сметки во вашата земја од страна на лица што користеле *IP* адреси во вашата земја.

ПРАШАЊЕ: Како би ги идентификувале осомничените (*IP* адреса)? Како може да прибавите такви податоци - во земјата или во странство? Што ако *IP* адресите не биле во вашата земја?

Врската меѓу *IP* адресата и вистинското лице е еден од најважните аспекти на секоја истрага на интернет. Ако *IP* адресата е во вашата земја, како работите со домашниот интернет провајдер за да добиете пристап до тие податоци? Кои законски одредби го овозможуваат таквиот пристап? Какви се обврските за интернет провајдерите да ги чуваат и направат достапни овие податоци?

Размислете за ситуација каде што *IP* адресата не е во вашата земја. Што е разликата? Како би ѝ пристапиле на ситуацијата во тој случај?

ПРАШАЊЕ: Како може да се утврди врската меѓу сопствениците на банкарската сметка (трет пасус во сценариото), сопствениците на паричниците со биткоини и лицата што го употребиле малверот. Дали во овој случај треба да се води финансиска истрага?

Одговорот на барањето за заемна правна помош ги укажува *IP* адресите и деталите за од сметките што биле употребени за конвертирање на биткоините во обични пари.

Како (а) ќе откриете кај која финансиска институција се води сметката, ако веќе не знаете; и (б) ќе работите со финансиската институција за да добиете информации за сопственикот на банкарската сметка? Кои законски одредби го овозможуваат таквиот пристап? Какви се обврските за финансиските институции да ги чуваат и направат достапни овие податоци?

Размислете повторно за ситуација каде што банкарските сметки се во друга земја. Што е различно и како би ѝ пристапиле на ситуацијата во тој случај?

ПРАШАЊЕ: Дали треба да се поведе финансиска истрага и, ако да, во кој момент?

Како што е дадено во сценариото, јасно е дека има значајни финансиски импликации поврзани со активноста на осомничените. Дали во вашата земја во овој случај може (и треба) да се води финансиска истрага? Ако да, во кој момент треба да се започне финансиската истрага?

ПРАШАЊЕ: Кои одредби од вашето домашно законодавство го опишуваат делото перење пари? Дали имало случај на перење пари?

Како е дефинирано делото перење пари во вашето домашно законодавство? Имајќи ги предвид фактите на случајот во сценариото, дали се случило дело перење пари?

ПРАШАЊЕ: Сценариото ја опишува заедничката активност на полицијата и УФР за анализа и следење на активноста со биткоини. Каква правна основа постои за оваа соработка?

Може да има законска основа за таква интеракција, но во многу случаи полицијата и УФР (и други организации како даночните власти, царината итн.) потпишуваат меморандум за разбирање што овозможува да се разменуваат информации.

Ве молиме да ја испитате ситуацијата во вашата земја.

ПРАШАЊЕ: Како се регулирани виртуелните валути, особено биткоините, во вашата земја?

Низ светот има различни регулаторни режими за биткоини. Каква е ситуацијата кај вас?

ПРАШАЊЕ: Дали во вашата земја виртуелните валути се обврзани субјекти и се задолжени да пријавуваат сомнителни трансакции?

Поконкретно, дали субјектите со виртуелни валути, како на пример берзите или сервисите за паричници, имаат обврска да пријават сомнителни активности?

7 Прилог: Список за релевантна литература

7.1 Совет на Европа

- Конвенција за компјутерски криминал, ETS 185, 23.11.2001:
<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
- Дополнителен протокол на Конвенцијата за компјутерски криминал, во врска со криминализацијата на чинови од расистичка и ксенофобична природа извршени преку компјутерски системи, ETS 189, 28.01.2003:
<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189>
- Конвенција за перење, претрес, заплена и конфискување приходи од криминал и за финансирање тероризам, CETS 198, 16.05.2005:
<http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/198>
- Конвенција за перење, претрес, заплена и конфискување приходи од криминал, Стразбур, ETS 141, 08.11.1990:
<https://rm.coe.int/168007bd23>
- MONEYVAL/глобален проект за компјутерски криминал, криминални парични текови на интернет - истражување за типологија, март 20012:
[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)
- Студија на Советот на Европа за филтрирање, блокирање и отстранување нелегална содржина на интернет, јуни 2016:
<https://www.coe.int/en/web/cybercrime/-/study-on-filtering-blocking-and-take-down-of-illegal-content-on-the-internet>
- Прашалник за употребата и ефикасноста на инструментите на Советот на Европа за меѓународна соработка во областа на заплена и конфискување приходи од криминал, вклучително и управување со конфискувана стока и делење средства. PC-OC Mod (2015) 06Rev4, 19.05.2016:
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680666607>
- Законодавство за компјутерски криминал - профили на земји:
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp
- Функционирање на контакт точките во мрежата 24/7 за компјутерски криминал (дискусија изготвена од Проектот за компјутерски криминал), април 2009:
<https://rm.coe.int/16802fb3be>
- Водич за електронски докази - основен водич за полициски службеници, обвинители и судии (март 2013). Достапно по барање на:
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp

- T-CY (2006)04 - Зајакнување на соработката меѓу органите на прогонот и приватниот сектор - примери како приватниот сектор блокирал интернет страници со детска порнографија, 20-ти февруари 2006:
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e6ed1>
- T-CY(2013)17rev - оцески извештај на T-CY: Одредби за заемна правна помош од Конвенцијата од Будимпешта за компјутерски криминал, 3-ти декември 2014:
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>
- T-CY(2014)17 - Правила за прибавување извештај со информации за претплатникот, декември 2014:
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7ad1>
- T-CY(2015)10 - Кривично-правен пристап до податоци во Облакот: предизвици, дискусија изготвена од Групата за докази во Облак при T-CY, мај 2015:
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59>
- T-CY(2016)13 - Итни барања за непосредно обелоденување податоци во друга јурисдикција преку канали за заемна правна помош или преку директни барања до даватели на услуги, Група за докази во Облакот при T-CY, мај 2016:
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651a6f>
- T-CY (2016)2 - Кривично-правен пристап до податоци во Облакот: соработка со „странски“ даватели на услуги. Прирачен документ подготвен од Групата за докази во Облакот при T-CY, мај 2016:
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d>
- T-CY(2016)7 - Кривично-правен пристап до електронски докази во Облакот: Препораки за разгледување од страна на T-CY, конечен извештај на Групата за докази во Облакот при T-CY, септември 2016:
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>
- T-CY(2015)16 Усвоен водич за наредби за прибавување (Член 18) - Верзија 01, март 2017 (усвоен со писмена процедура на 28-ми февруари 2017):
<https://rm.coe.int/16806f943e>

7.2 Европска Унија

- Директива 2014/42/EУ на Европскиот парламент и на Советот од 3-ти април 2014 за замрзнување и конфискување на инструментите и приходите од криминал во Европската Унија OJ L 127/39, 29.4.2014

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

Директива 2015/849 на Европскиот парламент и на Советот од 20-ти мај 2015 за спречување на користењето на финансискиот систем за перење пари или финансирање тероризам, со којашто се изменува Регулативата (ЕУ) бр. 648/2012 на Европскиот парламент и на Советот, и се укинува Директивата 2005/60/ЕЗ на Европскиот парламент и на Советот и Директивата 2006/70/ЕЗ на Комисијата: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849>

- Заедничко дејство 98/699/ПВР од 3-ти декември 1998 усвоено од страна на Советот врз основа на Член К.3 од Договорот за Европската Унија, за перење пари, откривање, следење, замрзнување, заплена и конфискување инструменти и приходи од криминал (ОЈ L 333, 9.12.1998, стр. 1): <http://eur-lex.europa.eu/legal-content/NLN/TXT/?uri=celex:31998F0699>

Рамковна одлука на Советот 2001/500/ПВР од 26-ти јуни 2001 за перење пари, откривање, наоѓање, замрзнување и конфискување инструменти на криминал и приходи од криминал (ОЈ L 182, 5.7.2001, стр. 1): <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001F0500>

- Рамковна одлука на Советот 2005/212/ПВР од 24-ти февруари 2005 за конфискување приходи, инструменти и имот поврзани со криминал (ОЈ L 68, 15.3.2005, стр. 49): <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:068:0049:0051:en:PDF>
- Рамковна одлука на Советот 2003/577/ПВР од 22-ри јули 2003 за извршувањето на налози за замрзнување имот или докази во Европската унија (ОЈ L 196, 2.8.2003): <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003F0577>
- Рамковна одлука на Советот 2006/783/ПВР од 6-ти октомври 2006 за примена на принципот на заемно признавање наредби за конфискување (ОЈ L 328, 24.11.2006): <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32006F0783>
- Одлука на Советот 2007/845/ПВР од 6-ти декември 2007 за соработката меѓу службите за враќање средства на земјите-членки во областа на наоѓање и откривање приходи или друг имот поврзан со криминал (L 332/103, 18.12.2007): <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007D0845>
- Директива 2013/40/ЕУ на Европскиот парламент и на Советот од 12-ти август 2013 за напади на информатички системи што ја заменува Рамковната одлука на Советот 2005/222/ПВР: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040>
- Директива на Европската унија 2016/1148 за безбедноста на мрежни и информатички системи (NIS директива) од 6-ти јули 2016: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L.2016.194.01.0001.01.ENG>

- Конечен извештај на *GENVAL* за петтата рунда заемна оценка - „Финансиски криминал и финансиски истраги“:
<http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012657%202012%20REV%202>
- Нацрт конечен извештај за седмата рунда заемни оценки за „Практичното спроведување и работа со европските политики за спречување и борба против компјутерски криминал“, јуни 2017.
<http://data.consilium.europa.eu/doc/document/ST-9986-2017-INIT/en/pdf>

7.3 Обединети нации

- Конвенција на ОН против незаконска трговија со наркотични дроги и психотропни супстанции, Виена, 19.12.1988:
<https://www.unodc.org/unodc/en/treaties/illicit-trafficking.html>
- Конвенција на Обединетите нации против меѓународен организиран криминал, Њујорк, 15.11.2000:
<https://www.unodc.org/unodc/en/treaties/CTOC/>
- Конвенција на Обединетите нации против корупција, Њујорк, 31.10.2003:
<http://legal.un.org/avl/ha/uncc/uncc.html>

7.4 Работна група за финансиска акција - *FATF*

- Меѓународни стандарди за сузбивање перење пари и финансирање тероризам и ширење, Препораки на *FATF*, 2012:
<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>
- Перење пари со нови начини на плаќање, октомври 2010:
<http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf>
- Главни дефиниции за виртуелни валути и потенцијални ризици за перење пари/финансирање тероризам, јуни 2014:
<http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

Виртуелни валути - Водич за пристап заснован на ризик, Работна група за финансиска акција, јуни 2015: <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>

7.5 Судска пракса

-
- Пресуда на Европскиот суд за човекови права (ЕСЧП) во К. У. против Финска, 2-ри декември 2008, за обврската на владите да ги штитат поединците од криминал, вклучително и преку кривично право:

[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]]})

- Судска пракса на ЕЧП за заштита на лични податоци:
http://www.echr.coe.int/Documents/FS_Data_ENG.pdf
- Судска пракса на ЕЧП за нови технологии:
http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf
- Судска пракса на ЕЧП за масовно следење:
http://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf
- Пресуда на Судот на правдата на Европската унија во споените предмети C-293/12 и C-594/12 . *Digital Rights Ireland* и *Seitlinger* и други:
<http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>
- Пресуда на Судот на правдата на Европската унија во предметот C-582/14, 19-ти октомври 2016, динамични IP адреси може да претставуваат „лични податоци“ според законите на ЕУ за приватност:
<http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1034974>
- Пресуда на Судот на правдата на Европската унија во предметот C-264/14, 22-ри октомври 2015, „виртуелната валута биткоин нема никаква друга намена, освен да биде средство за плаќање и да биде прифатена за таа цел од извесни оператори“:
<http://curia.europa.eu/juris/document/document.jsf?text=&docid=170305&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=160800>
- Пресуда на Врховниот суд на Белгија во предметот Белгија против *Yahoo!*:
http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1
- Пресуда на Апелациониот суд на САД во предметот *Microsoft* против САД:
<http://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412>

7.6 Други референци

- Чување податоци по пресудата на Судот на правдата на Европската унија, проф. д-р Франциска Бем и други, Мунстер/Луксембург, 30-ти јуни 2014:
http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf
- Енкрипција, прашање на човекови права, извештај на *Amnesty International*, март 2016. Достапен на:
http://www.amnestyusa.org/sites/default/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf
- „Брошура: Шест работи што треба да се знаат за финансиската истрага“, февруари 2016:

- <https://english.eu2016.nl/documents/publications/2016/02/10/brochure-the-6-need-to-knows-about-financial-investigation>
- „Оценка на потребите за инструменти и методи за финансиска истрага во Европската унија“, ECORYS, декември 2015:
https://www.wodc.nl/binaries/2612-summary_tcm28-74130.pdf
- Мислење на Европското банкарско надзорно тело за виртуелни валути, ЕВА/Оп/2014/08, јули 2014:
<https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>
- Анализа на анонимноста во *Bitcoin* со сообраќај во *P2P* мрежа, *Koshy* и други, *Pennsylvania State University*:
http://fc14.ifca.ai/papers/fc14_submission_71.pdf
- Оценка на заканата од организиран криминал на интернет (IOCTA) 2016, *Europol*:
<https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016>
- Оценка на заканата од организиран криминал на интернет (IOCTA) 2017, *Europol*:
<https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>