ПРАЊЕ НОВЦА ПУТЕМ ИНТЕРНЕТА

Сандра Ковачевић[1]

Резиме: Убрзаним развојем информационе технологије унапредиле су се све области живота, па су се јавиле могућности за сложеније и опасније облике злоупотреба. Специфичне карактеристике рачунарског криминалитета утицале су да се у теорији све више разматрају могобројни аспекти ове друштвене појаве, као и да се мења легислатива у правцу квантитативно и квалитатитвно бољег регулисања ове области. Постоји велика „тамна бројка“ рачунарског криминалитета, посебно кривичног дела прања новца путем интернета јер ово кривично дело омогућава велику материјалну корист. Прање новца представља глобални проблем на који није ни једна држава света имуна. Прање новца представља деривативан облик криминалитета јер му по правилу увек претходи неко кривично дело/или више њих, на основу којег је стечена имовинска корист, односно новац за који постоји потреба да се опера и прикаже као легалан. У овом раду ће бити приказане карактеристике прања новца на интернету, ризици и угроженост од прања новца на интернету као и типологије прања новца.

Кључне речи: рачунарски криминалитет, прање новца, интернет, имовинска корист, ризици

ONLINE MONEY LAUNDERING

Abstract: With the accelerated development of information technology, all areas of life have improved, so there are opportunities for more complex and dangerous forms of abuse. The specific characteristics of computer crime have influenced the consideration of possible aspects of this social phenomenon in theory, as well as the change of legislation in the direction of quantitatively and qualitatively better regulation of this area. There is a large "dark number" of computer crime, especially the crime of money laundering via the Internet, because this crime provides great material benefits. Money laundering is a global problem to which no country in the world is immune. Money laundering is a derivative form of crime because, as a rule, it is always preceded by a criminal offense and / or more of them, on the basis of which material gain was obtained, ie money for which there is a need to be laundered and presented as legal. This paper will present the characteristics of money laundering on the internet, the risks and threats of money laundering on the internet, as well as the typology of money laundering.

Keywords: *computer crime, money laundering, internet, property gain, risks.*

1. УВОД

Развој компјутерске технологије у великој мери је допринео побољшању и унапређењу привредне делатности, посебно када је реч о производњи, комуникацији и фнансијском пословању. Са друге стране, развој компјутерске технологије је донео нове и драстичне промене у све сегменте друштва, где се поред позитивних новина створили низ могућности злоупотреба те технологије и развој нових кривичних дела високотехнолошког криминалитета. Високотехнолошки криминалитет представља савремени облик криминалитета којег карактерише низ специфичности у погледу структуре, особености и заступљености. Будимпештанском конвенцијом о високотехнолошком криминалу (која је потврђена и у Републици Србији)[1] се високотехнолошки криминал посматра као: 1. кривична дела против рачунарских система и података и 2. кривична дела начињена уз помоћ рачунара и електронских података (укључујући и преваре начињене уз помоћ рачунара). Инструменти и инфраструктура високотехнолошког криминалитета састоје се од малвера, ботнетова, кажњиве злоупотребе домена, подземне економије која обезбеђује робу и услуге стечене кривичним делима, а посебно мазги за пренос новца (појединци који на своје

[1] Академија струковних студија Шабац, Добропољска бр.5 Шабац, e-mail:sandrakovacevic@gmail.com

легитимне рачуне примају уплате украденог новца које затим брзо пребацују на рачуне криминалаца уз занемарљиву надокнаду), које су значајан саставни део токова прања новца на интернету. Друштвене мреже нуде нове платформе за високотехнолошки криминалитет и нове изазове органима реда. Сложене преваре и ова инфраструктура имају све особине структуираног организованог криминала.

Прибављање економске или друге користи било је једна од мотивација сајбер-криминалаца од самог почетка.[2] Међутим, сада постоји консензус да је остваривање материјалне користи постало главна сврха високотехнолошког криминалитета а интернетом кружи велики износ прљавог новца. Тешко се процењује количина прљавог новца који тече интернетом, и у овом тренутку нема свеобухватне студије о томе. Како се друштво све више ослања на информационе технологије где постоји глобална мрежа комуникације, све је више дела учињена из користољубља која су све више интернационализована и постоје електронски доказни материјали, где се компјутер у криминалној делатности може користити као објект напада, средство извршења, средство за планирање извршења кривичног дела, као и средство за спречавање разјашњавања и доказивања кривичних дела. У том смислу, компјутер се показао као средство којим се могу извршавати разноврсна сложена кривична дела, као што су пљачке, проневере, финансијске малверзације, шпијунажа, тероризам, као и различити облици злоупотреба. Једно од кривичних дела је и прање новца путем интернета.

2. ПРАЊЕ НОВЦА – ОСНОВНЕ КАРАКТЕРИСТИКЕ

Прање новца представља процес прикривања незаконитог порекла новца или имовине који су стечени извршењем криминалних активности. Прање новца има три основне фазе:[3] 1. фаза „улагање", тј. прекидање директне везе између новца и незаконите активности којом је он стечен (у њој се незаконито стечени новац уводи у финансијски систем, 2. фаза „прикривање", када се новац, након што је ушао у легални финансијски систем, пребацује с рачуна на који је положен на друге рачуне (главни циљ тих трансакција јесте прикривање везе између новца и криминалне активности од које потиче) и 3. фаза „интеграције", у којој се „прљав" новац јавља као новац који потиче од дозвољене делатности. Прањем новца, у смислу Закона о спречавању прања новца и финансирања тероризма сматра се:[4] 1. конверзија или пренос имовине стечене извршењем кривичног дела, 2. прикривање или нетачно приказивање праве природе имовине, њеног порекла, места налажења, кретања, располагања, власништва или права у вези са имовином која је стечена извршењем кривичног дела и 3. стицање, држање или коришћење имовине стечене извршењем кривичног дела. Поменуте активности извршене изван територије Републике Србије такође се сматрају прањем новца. Последице прања новца су: подривање стабилности, транспарентности и ефикасности финансијског система земље, економски поремећаји и нестабилност, угрожавање програма реформи, смањење инвестиција, губљење угледа државе и угрожавање националне безбедности при финансирању тероризма.

3. РИЗИЦИ И УГРОЖЕНОСТ ОД ПРАЊА НОВЦА НА ИНТЕРНЕТУ

Због брзог раста и развоја технологије, системи плаћања су веома напредовали. Развој система плаћања ствара нове могућности за прање новца и чини откривање потенцијално сумњивих трансакција све тежим. Поред тога, криминалци високотехнолошког криминала за исте преваре сада комбинују класичне и нове методе плаћања, вишеструко их мешајући и користећи готовину, банковне трансфере, припејд картице, службе за дознаке, е-новац и друге системе електронског плаћања. Код неких

метода плаћања је ризик од прања новца и већи него код других, у зависности од степена анонимности трансфера, локације пружаоца услуга, сегментације посредника и под-посредника, односа са кредитном или финансијском институцијом у јурисдикцији која поштује (или не поштује) међународне стандарде у области у борби против прања новца. Финансијска акциона радна група (FATF) наводи четири потенцијална фактора ризика у вези са прањем новца: 1. анонимни рачуни, 2. анонимно финансирање и пријем средстава (АТМ), 3. високи или непостојећи лимити финансирања рачуна и 4. пружаоци услуга у другим земљама који не морају да поштују законе у другим јурисдикцијама. Фактори смањивања тих ризика су: 1. одговарајући захтеви и поступци за идентификацију држаоца рачуна, 2. одржавање евиденција трансакција у којима су наведени уплатилац и прималац, 2. праћење трансакција и пријављивање сумњивих активности, 3. ограничавање опција финансирања и 4. примена блокирања рачуна и ограничавање приступа услугама.[5]

3.1. Технолошки ризици

Ови ризици се огледају у све лакшем и већем приступу савременој и брзој опреми и конекцијама, као и готово универзална распрострањеност интернет конекција, где се, повећава могућност вршења читавог низа финансијских трансакција на лак и јефтин начин. Софтвер је напредовао и створио пријатељско место контакта јавности и онлајн финансијских услуга, тако да непоседовање рачунарских вештина више није препрека. Релативна лакоћа вршења прања новца представља потенцијалну претњу. С друге стране, информационе технологије су потенцијално примењиве за сврхе истражних и надзорних активности органа реда, али такође нуде криминалцима лак и јефтин приступ брзим, ефикасним и све анонимнијим системима плаћања. Данас има специјализованих одељења који се баве спровођењем закона, финансијске обавештајне службе и надзорни органи за високотехнолошки криминал, али често се не поседује довољно знања о функционисању механизама нових система плаћања. У одсуству ваљаних надзорних механизама, евидентиране су тешкоће у остваривању сарадње са јавним интернет провајдерима (сајбер кафеи, универзитетске мреже, итд.).

3.2. Анонимност

Приликом остваривања односа са интернетским пружаоцем услуга плаћања, непосредан контакт између клијента и оператера је или минималан, или уопште не постоји, трансакције се не обављају лицем у лице, тако да не долази до упознавања клијената, што значи да анонимност представља значајан ризик. Услуге се добијају путем компјутерског терминала, а улаз и излаз новца се обавља преко поседника што је најчешће банка. Опасност од прања новца би се могла смањити уколико би се методе финансирања обављале преко агената који су поуздани и примењују мере провере клијената што би било у складу са стандардом FATF. Велика количина прљавог новца у интернет систему постоји и због могућности отварања анонимних рачуна, са којих се новац може послати на било које место на свету, без коришћења постојећег банкарског система. Методи анонимног финансирања, уз мањак података о идентитету клијента, могли би да доведу до недовољних трагова трансакције и порекла новца, или пак до одсуства сваког трага, у случају кривичних истрага, и да представљају озбиљну сметњу било каквој истрази о прању новца. У таквим околностима, релевантни међународни стандарди и на њима засновани национални прописи у вези са познавањем идентитета клијента не примењују се у довољној мери од стране финансијских посредника.

3.3. Неповољан надзор над пружаоцима услуга

Што се тиче надзора над ризицима од прања новца путем интернета постоји проблем јер рад пружалаца услуга преко интернета је недовољно законски уређен, нити надзиран у погледу њихових обавеза према спречавању прања новца. Кључни фактор ризика је непостојање регулаторне контроле окружења и непостојећи или неодговарајући систем кажњавања. Проблем представља и чињеница да често јурисдикција у којој раде није она у којој су регистровани. У неким случајевима је проблем чак и непостојање правних прописа усмерених директно ка таквим ентитетима. Понекад пружаоци услуга плаћања преко интернета успевају да намерно избегну законске обавезе тако што се региструју у „слабо“ регулисаној јурисдикцији, а финансијске операције врше у другим земљама. Још једна тешкоћа код обављања ваљаног надзора над пружаоцима поменутих услуга лежи у њиховом виртуалном профилу. Не постоји права мењачница, нити продавница, нити други продајни објекат.. Проблем је како вршити надзор на лицу места када је у питању виртуелна трговина. Шта више, када би се такав надзор изводио, надзорним органима би требало да буду на располагању нова технолошка средства и специјализована обука инспектора како би се обезбедиле делотворне финансијске ревизије књиговодства, и ваљане анализе интерних процедура и других обавеза у вези са спречавањем прања новца и финансирања тероризма. У вези с овим би требало да буде усвојен заједнички став, према коме би питање лиценцирања и надзора могло на неки начин да буде подељено између јурисдикције регистрације и јурисдикције испоруке услуга.

3.4. Географски и јурисдикциони ризици

Ширење интернета и све већим раздаљинама шири се и географски опсег система плаћања, што представља већи ризик у погледу прања новца. Прекогранична функционалност може да привуче криминалце који перу новац одређеном пружаоцу услуга, јер може да омогући пружаоцима платних услуга да своје активности врше из јурисдикција где не подлежу ни адекватним прописима у погледу спречавања прања новца ни адекватном надзору, и где могу да буду ван домашаја иностраних кривичних истрага. Ипак, могуће је идентификовати токове новца из једне у другу јурисдикцију, као и трендове. Неке државе (западни део Европе и Северна Америка) су полазишта токова прљавог новца, што би могло да укаже на то да су жртве сајбер напада лоциране у тим регионима. Друге државе су „одредишта“ токова прљавог новца, мада се у овој фази не може одредити да ли су оне крајња дестинација новца. Подизање готовинског новца, у комбинацији са употребом мазги за пренос новца како би се уклонили трагови и сакрили токови новца, ометају јасно одређивање крајњег одредишта новца. Постоји однос између дестинација токова новца и порекла сајбер криминалаца, што наводи на закључак да сајбер криминалци често шаљу новац својој породици и пријатељима у својим земљама порекла. За разлику од класичних активности прања новца коришћењем банкарског система, прање новца путем интернета се ослања на различите врсте активности и на пружаоце финансијских услуга, од банковних трансфера, подизања и улагања готовинских средстава, употребе е-новца, па до мазги за пренос новца и служби које врше дознаке новца. Све то полицији и правосудним органима чини откривање и праћење токова прљавог новца много тежим и компликованијим.

3.5. Остали ризици

Остали ризици су: 1. релативна лакоћа оснивања финансијског система на интернету, уз ниске трошкове пословања, могли би водити нејасном власничком профилу, 2. велика брзина обављања активности, укључујући међународне трансфере, могла би да олакша активности прања новца, 2. ниска цена пословања би могла да омогући ниске трошкове прања новца и охрабри потенцијалне криминалце у намери да

озаконе противзаконито стечена средства, 4. лако претварање у прави новац и готовину у великом броју земаља могли би да повећају опасност од прања новца.

4. ТИПОЛОГИЈЕ ПРАЊА НОВЦА ПУТЕМ ИНТЕРНЕТА

Циљ типологија прања новца је едукативни: треба да покажу обвезницима, од банака, мењачница и других представника финансијског сектора, па до посредника у промету непокретности, рачуновођа, ревизора и адвоката, који су све могућности да се опере новац уочене у различитим секторима, где су то сектори којима се свако од њих бави рањиви и на које облике на изглед легалног пословања треба највише да обрате пажњу. Постоје два врло велика и честа проблема: изазови у истрагама који се повезују са идентификацијом учиниоца на интернету и мноштво изазова који се повезују са коришћењем виртуелних валута.

4.1. Коришћење интернет банкарства

Ово се посебно односи на типологије електронских трансфера, преузимања рачуна у банкама и међународних трансфера. Захтеви које законска регулатива поставља пред финансијске институције у смислу мера праћења и познавања странке, вођења евиденција, и сл. су примењиви али у покушају да заобиђу ове контроле, криминалци се ослањају на чињеницу да се интернет банкарство не обавља лично.[6] Постоје три главна трага која треба пратити приликом вођења истраге у таквим предметима: 1. начин на који је банкарски рачун компромитован, 2. информације о пријављивању у вези са компромитованим рачуном у банци, 3. рачун у банци коришћен за трансфер новца са компромитованог рачуна. Да би се бориле финансијске институције често инсталирају аутоматизовани софтвер за праћење трансакција, чија је функција да открије трансакције које одступају од профила трансакција које се обично обављају на датом рачуну. Поред тога, чак и ако је банкарски рачун неког клијента на интернету компромитован, то неће увек бити очигледно на основу IP адресе која се користи за пријављивање, јер ће криминалцу омогућити да се на рачун клијента пријави са IP адресе клијентовог рачунара, и тако спречи активирање упозорења због пријављивања са неуобичајене IP адресе. Повезивање осумњиченог са том IP адресом представља посебан изазов.

4.2. Коришћење других (нефинансијских) услуга на интернету

Друге (небанкарске) финансијске услуге на интернету су: коришћење система плаћања на интернету, куповина преко интернета и коришћење платформи за коцкање, односно трговину путем интернета. То криминалцима даје могућност експлоатације оваквих врста услуга. Ово се најчешће дешава приликом коришћења платних картица за“пуњење” рачуна код пружаоца финансијских услуга путем интернета. Када се средства са платне картице пренесу пружаоцу услуге, природа даљих интеракција између корисника и пружаоца финансијских услуга путем интернета биће непрозирна за традиционални финансијски систем. Стога се препоручује да услуге плаћања преко интернета подлежу обавези усаглашености са законом и надзором.[7] Главни изазови који се појављују односе се на чињеницу да се тражене евиденције обично налазе у другој јурисдикцији. Слични проблеми се појављују код употребе платформи које олакшавају куповину путем интернета. Куповина роба или услуга преко интернета и њихово отпремање криминалцу или мазги за пренос новца представља добар начин да се украдени лични подаци за плаћање претворе у вредност у стварном свету. У тим случајевима, истрага се у потпуности ослања на евиденције платформи за куповину, као и на њихову способност да препознају сумњиву активности. Платформе за коцкање

путем интернета доносе изазове који углавном проистичу из недоследности у регулисању тих субјеката широм света. У оквиру ЕУ неке чланице су у скоријем законодавству одлучиле да дозволе или забране коцкање путем интернета, док га друге дозвољавају или забрањују "пасивно", тако што и даље примењују законодавство које је, често много година раније, усвојено за класично коцкање. Од 20 држава чланица које дозвољавају коцкање преко интернета, 13 имају либерализовано тржиште, 6 имају државне монополе, а једна је издала дозволу за један приватни монопол.[8]

4.3. Коришћење услуга комуникација на интернету

Интернет је, пре свега, платформа за комуникацију и криминалци користе услуге комуникације за омогућавање својих активности. У контексту токова новца који потиче од криминала, посебно на интернету, услуге комуникације путем интернета омогућују им да регрутују мазге, да с њима комуницирају и да њима управљају. Услуге као што је електронска пошта, комуникациони сервис IRC (енг.: Internet relay chat), размена тренутних порука и телефонске услуге које су доступне на интернету криминалци могу користити за организовање својих активности. Техничке тешкоће могу се појавити и код идентификације лица која учествују у комуникацији и код утврђивања садржаја комуникације. Последњих година, тренд међу пружаоцима интернет услуга је све веће фокусирање на гаранције приватности њихових корисника. Ово се показало у многим случајевима, као што је веће коришћење шифровања. Шифровање се, широко гледано, спроводи на три различита начина.[9] Шифровање преноса података једна је од основних безбедносних контрола која олакшава савремени свет електронске трговине и електронског банкарства, тако што онемогућава нападаче да пресретну комуникацију између странке и банке или интернет сајта за електронску трговину.

4.4. Непробојни хостинг

У условима коришћења већине пружалаца услуга интернета и веб хостинга забрањују се нелегалне активности на њиховим мрежама или сервисима. Они ће, зато, обично сарађивати са захтевима за давање информација и захтевима за обарање нелегалних домена или интернет сајтова које упућују органи задужени за спровођење закона. Непробојни хостинг, с друге стране, је назив који се даје пружаоцима хостинг услуга који не сарађују са захтевима за давање информација или за рушење интернет сајтова које упућују органи задужени за спровођење закона. У већини случајева компаније за непробојни хостинг покушаће да се бране тиме што немају законску одговорност за криминалне радње које изврше њихови клијенти користећи њихову инфраструктуру. Ове услуге се често користе за растурање нелегалних материјала, израду нежељене електронске поште, као сервери за команду и контролу малициозног софтвера и за друге облике криминалне инфраструктуре. Законодавства неких земаља подржавају блокирање садржаја за који се зна да је нелегалан од стране националних интернет провајдера, коришћењем различитих техника за техничко филтрирање.[10] Информације о корисницима и услугама које компаније за непробојни хостинг обезбеђују властима нису од велике користи за истрагу због тога што су подаци о тим лицима најчешће лажни. Међутим, метода плаћања за изнајмљене услуге могла би бити важан траг који би могао да помогне приликом утврђивања извора криминалне активности. На законодавној страни такође постоје тешкоће код утврђивања надлежности за извршене нелегалне активности, пошто може постојати више коришћених извора, одредишта или других координационих места. У земљама где постоји непробојни хостинг, у истрази се може користити тајно праћење. Ово ће помоћи приликом прикупљања информација о извору, одредишту и природи криминалне радње.

4.5. Подземна економија

Подземна економија је име које се даје услугама које користе криминалци да би размењивали услуге и информације једни с другима. Постоји много примера подземних форума, као што је Silk Road и Dark Market. По својој организацији, подземна економија је структурирана за вршење кривичних дела. Често се користи пословни модел под називом "Crime as a service"(криминал као услуга). Подземни форуми који су углавном посвећени преварама са кредитним картицама и продаји украдених података са кредитних картица често се називају "carding форуми". У већини случајева ови форуми су отворени само за одређене "клијенте" на основу лозинки или других мера обезбеђења. Истраге које се односе на ове врсте форума обично су веома дуге и сложене и код њих се службе за прикривене иследнике често полако инфилтрирају на форуме и прелазе на позиције од ауторитета, одакле ће добити приступ информацијама које ће омогућити оптуживање администратора и оператера форума. То што су потребне тако сложене истраге значи да у већини истрага неће бити могуће убацити се у неки подземни форум, како би се прикупили докази за истрагу о некој појединачној криминалној радњи или прању новца путем интернета. Такође, из перспективе истраге, важно је имати одговарајуће прописе који инкриминишу такве нелегалне активности и дозвољавају вођење тајних операција и коришћење прикупљених доказа на суду. Ова истрага је мешавина класичних доказних радњи и техника које се спроводе на интернету. У случајевима када су власници или оператери неког познатог подземног форума присутни у националној јурисдикцији, или када се хост тог подземног форума налази у оквиру националне јурисдикције, одговарајуће материјалне одредбе националног законодавства могу се користити као основа за кривични поступак у таквим предметима. Релевантне одредбе ће зависити од специфичности тог предмета али би могле да буду еквивалентне, на пример, члану 6. Будимпештанске конвенције.

5. ЗАКЉУЧАК

Постоји јасна потреба за обављањем истраживања прања новца и високотехнолошког криминалитета, посматрајући природу и обим, извршиоце и помагаче који се користе, начине на који раде, инфраструктуре и службе које нападају, технологије које су тек у развоју и ризике које иду уз њих, као и најновије претње. Испуњавање постојећих рупа сталним истраживачким радом би помогло у развијању одговарајућих политика и мера спречавања и умањивања обима прања новца и високотехнолошког криминалитета у погледу опасности које су препознате. Резултат би био и повећана спознаја представника надлежних институција и приватног сектора о инструментима, технологијама и активностима високотехнолошког криминалитета, како би се препознали они који ће вероватно бити мете криминалаца у области прања новца, чиме би се ојачали капацитети за откривање, у подршци активностима против криминалаца и прања новца. Област управљања ризицима у приватном сектору требало би да буде проширена да обухвати и ризике повезане са интернетом. Значајна је и неопходност ажурирања домаћих законских оквира, како би се на одговарајући начин покрила област високотехнолошког криминалитета, прања новца и мера процесног права како би се омогућило чување, тражење и заплена електронских доказних материјала као и међународна сарадња, у складу са Будимпештанском конвенцијом о високотехнолошком криминалу као и усмерити пажњу на примену измењених препорука FATF-а које су овде непосредно релевантне, посебно оних у вези са проценом ризика, новим технологијама, преносима новца или еквивалентних вредности, телеграфским трансферима, итд. Потребно је успоставити: јасне механизме

и стимулације за јавно пријављивање и процене трендова и претњи, анализе активности криминалаца и токова новца и прања новца, покретање мера органа кривичноправног система и финансијских обавештајних јединица за истраживање и касније процесуирање таквих кривичних дела, успостављање смерница за финансијске и нефинансијске институције у виду обавезаних прописа у области борбе против прања новца и финансирања тероризма, да пријављују када сумњају или имају разуман основ за сумњу да одређени новац представља корист стечену извршењем кривичног дела, оснивање специјализованих јединица и тужилаштава за високотехнолошки криминал, сарадњу између различитих органа у борби против високотехнолошког криминалитета, као и међународна сарадња између држава као кључног фактора у борби против високотехнолошког криминалитета.

6. ЛИТЕРАТУРА

[1] Закон о потврђивању Конвенције о високотехнолошком криминалу („Сл. Гласник РС“, бр. 19/2009)

[2] FATF (2008): Terrorist Financing. Преузето: 25. новембра 2021, са: http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf

[3] Драгојловић, Ј. (2015). Спречавање прања новца у ери глобализације. Култура полиса 12 (посебно издање), стр. 144.

[4] Закон о спречавању прања новца и финансирању тероризма („Службени гласник РС”, бр. 113/2017, 91/2019 и 153/2020)

[5] „FATF-GAFI - Money Laundering Using New Payment Methods“, стр. 18, X 2006. год.

[6] FATF Report, Money Laundering Using New Payment Methods. Преузето 27. новембра 2021. са: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf

[7] FATF Report, Money Laundering Using New Payment Methods. Преузето 27. новембра 2021. са: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf

[8] EU Parliament Study by the Policy Department, Economic and Scientific Policy, titled “Online Gambling, focusing on integrity and a code of conduct for gambling” IP/A/IMCO/FWC/2006-186/C1/SC2.Преузето 29. новембар 2021. са: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2008/408575/IPOL-IMCO_ET(2008)408575_EN.pdf

[9] EU Parliament Study by the Policy Department, Economic and Scientific Policy, titled “Online Gambling, focusing on integrity and a code of conduct for gambling” IP/A/IMCO/FWC/2006-186/C1/SC2. Преузето 30. новембра 2021. са: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2008/408575/IPOL-IMCO_ET(2008)408575_EN.pdf.

[10] T-CY(2006)04 Strengthening Co-operation between law enforcement and the private sector, examples of how the private sector has blocked child pornographic sites(T-CY(2006). Преузето 30. новембра 2021. са: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e6ed1