



iPROCEEDS

Projekt për luftimin e të ardhurave nga krimi në
Internet në Evropën Juglindore dhe në Turqi

www.coe.int/cybercrime

Versioni i datës 21 dhjetor 2017

Kurs trajnimi për gjyqtarë dhe prokurorë

Kurs i avancuar për bastisjen, sekuestrumin dhe konfiskimin e të ardhurave nga krimi kibernetik

Doracak trajnimi për punë të pavarur

Funded
by the European Union
and the Council of Europe



Implemented
by the Council of Europe

Kontakti:

Alexander Seger
Divizioni i Krimit Kibernetik
Drejtoria e Përgjithshme për të Drejtat e
Njeriut dhe Sundim të Ligjit
Këshilli i Evropës
Strasburg, Francë

Tel: +33-3-9021-4506
Faksi: +33-3-9021-5650
Email: alexander.seger@coe.int

Mohim i përgjegjësisë:

Ky raport teknik nuk pasqyron
doemos qëndrimet zyrtare të Këshillit
të Evropës ose të donatorëve që
financojnë këtë projekt.

Përmbajtja

1 Hyrje.....	6
1.1 Qëllimi i kursit	8
1.2 Grupi i synuar i studentëve	8
1.3 Tabela e përmbajtjes.....	9
1.3.1 Sfidat e hetimeve elektronike (online).....	9
1.3.2 Hetimet ndërkufitare.....	9
1.3.3 Valutat virtuale	9
1.3.4 Punë praktike/raste studimore	9
2 Sfidat e hetimeve elektronike (online).....	11
2.1 Tipologjitë e pastrimit të parave online	11
2.1.1 Shfrytëzimi i shërbimeve bankare përmes internetit.....	11
2.1.2 Shfrytëzimi i shërbimeve të tjera financiare në internet.....	12
2.1.3 Shfrytëzimi i shërbimeve të komunikimit përmes internetit.....	14
2.1.4 Hostingu i padepërtueshëm	16
2.1.5 Ekonomia e nëntokës.....	17
2.2 Identifikimi i keqbërësve.....	18
2.2.1 Transferimi i adresës së rrjetit (NAT)	19
2.2.2 Transferimi i adresës së rrjetit përmes sistemeve të besueshme (Carrier Grade Network Address Translation - CGN)	20
2.2.3 Shfrytëzimi i anonimëve.....	21
2.2.4 Botnets (Rrjeti i kompjuterëve të infektuar)/viruset/kontrolli nga largësia i një kompjuteri	24
2.2.5 Shfrytëzimi i WiFi të hapura, publike ose të vjedhura	25
2.2.6 Identifikimi i pronarit të një adrese të IP-së.....	26
2.3 Angazhimi me ISPs	27
2.3.1 Lloji i të dhënave të kërkuara.....	27
2.3.2 Direktiva e BE-së për ruajtje të të dhënave është shpallur e pavlefshme me vendim të CJEU	29
2.3.3 ISP-të kombëtare	31
2.4 Provajderët e Shërbimeve Shumëkombëshe.....	33
2.4.1 Juridiksioni	33
2.4.2 Qëndrimi i përgjithshëm	34
2.4.3 Kërkesat për ruajtje.....	34
2.4.4 Kërkesat emergjente	34
2.4.5 Shtrirja e kërkesës	34
2.4.6 Njoftimi i subjektit të kërkesës	35
3 Hetimet financiare	37
3.1 Hyrje.....	37

3.2	Hetimet financiare dhe të ardhurat nga krimi kibernetik.....	37
3.2.1	Elementet e hetimeve financiare	38
3.2.2	Aspekte të hetimeve financiare të krimeve kibernetike	38
3.2.3	Hetimet financiare në Bashkimin Evropian	39
4	Bashkëpunimi ndërkufitar.....	42
4.1	Përmbledhje.....	42
4.1.1	Rrjetet dhe organizatat relevante për këmbim të informatave dhe ndihma e ndërsjellë juridike	43
4.1.2	Mjetet Ligjore Ndërkombëtare	44
4.1.3	Dispozitat e Bashkëpunimit Ndërkombëtar.....	47
4.2	Vlerësimi i zbatimit të dispozitave për bashkëpunim ndërkombëtar	49
4.2.1	Vlerësimet përkitazi me targetimin e të ardhurave nga krimi.....	50
4.2.2	Vlerësimet që lidhen me krime kibernetike	52
4.3	Përdorimi i shabllonëve dhe formularëve për Ndihmë të ndërsjellë juridike.....	60
5	Valutat virtuale.....	62
5.1	Përmbledhje e kursit bazik.....	62
5.2	Hyrje në valutat virtuale	63
5.2.1	Terminologji më e zgjeruar e valutave virtuale	63
5.2.2	Pjesëmarrësit në valuta virtuale	65
5.2.3	Bitcoin	66
5.3	Rreziqet e valutave virtuale.....	68
5.4	Sfidat hetimore.....	70
5.4.1	Si të dihet se janë përdorur valutat virtuale	70
5.4.2	Anonimiteti i transaksionit	71
5.4.3	Identifikimi i burimit të fondeve	71
5.4.4	Kthimi në para/realizimi dhe konvertimi i të ardhurave.....	72
5.5	Sfidat e ngrirjes/sekuestrimit	73
5.5.1	Valutat virtuale si të ardhura nga krimi	73
5.5.2	Identifikimi i ekzistencës së valutave virtuale	73
5.5.3	Ngrirja/Marrja e kontrollit të valutave virtuale	73
5.5.4	Menaxhimi i aseteve	74
6	Punë praktike/raste studimore.....	75
6.1	Hulumtim i literaturës.....	75
6.2	Rasti studimor 1: Shqyrtimi i bazës ligjore për veprime	75
6.3	Rasti studimor 2: Marrja parasysh e bashkëveprimit me NJIF/Organet e rendit.....	78
6.4	Rasti studimor 3: Shqyrtimi i bashkëveprimit në raste të krimit kibernetik/pastrimit të parave	81
7	Shtojca: Lista e materialeve relevante për lexim	83
7.1	Këshilli i Evropës	83

7.2	Bashkimi Evropian	84
7.3	Kombet e Bashkuara	86
7.4	Task Forca për Veprim Financiar	86
7.5	Jurisprudenca	86
7.6	Referenca të tjera	87

1 Hyrje

Çështjet e krimeve kibernetike, provave elektronike, të ardhurave nga krimi prekin institucione të ndryshme dhe përfshijnë në veçanti njësitë kundër krimeve kibernetike, njësitë për hetime financiare, njësitë për inteligjencë financiare (NJIF) dhe shërbimet e prokurorisë. Megjithatë, hetimet e krimeve kibernetike rrallë shoqërohen nga hetimet financiare dhe anasjelltas, hetimet e veprave penale financiare ose të tjera rrallë shoqërohen nga hetimet e krimeve kibernetike. Për këtë qëllim, ekziston nevoja për bashkëpunim më efektiv mes të gjitha këtyre institucioneve, që pritet të ketë ndikimin më të madh në kontrollin, sekuestrimin dhe konfiskimin e të ardhurave nga krimi kibernetik.

Rrjedha e parave nga krimi kibernetik dhe nga veprat penale në Internet nuk ndalet brenda kufijve gjeografikë. Andaj, për t'i adresuar këto fenomene në mënyrë gjithëpërfshirëse aktivitetet hetuese duhet të tejkalojnë kufijtë dhe të operojnë me juridiksione të ndryshme. Bashkëpunimi efektiv ndërkombëtar po ashtu është kyç për kontrollin, sekuestrimin dhe konfiskimin e të ardhurave nga krimi kibernetik. Ndërlidhja e masave për gjurmimin e të ardhurave nga krimi me masat kundër pastrimit të parave dhe luftimit të financimit të terrorizmit dhe me hetimet e krimeve kibernetike dhe forenzikën kompjuterike ofrojnë mundësi shtesë. Për shembull, masat për ngrirjen e përkohshme të pasurisë duhet të shoqërohen me kërkesa për një ruajtje të përsheptuar të provave elektronike.¹ Kjo është një nga arsyet pse Rekomandimi 36 i Taskforcës për Veprim Financiar propozon zbatimin e Konventës së Budapestit për luftimin e krimeve kibernetike dhe Konventën e Varshavës të Këshillit të Evropës.

Pasi që shfrytëzimi dhe mbështetja në teknologjinë informative janë bërë përherë e më të përhapura në shoqëri, përqendrimi në sisteme kompjuterike dhe shfrytëzimi i tyre është bërë përherë e më i rëndomtë. Veprat penale që përfshijnë kompjuterët janë rritur në mënyrë rapide si në numër ashtu edhe për nga sofistikimi, porse ka pasur një hendek kohor në zhvillimin e masave efektive për luftimin e tyre. Sjellja e kryerësve para drejtësisë kërkon prova të fajësisë përtej dyshimit të arsyeshëm, porse provat e nxjerra nga pajisjet elektronike janë të paqëndrueshme, shpesh të paprekshme dhe me gjasë edhe nga juridiksionet e tjera. Kjo nënkupton se rëndësia për procedura të rrepta e efektive, në përputhje me ligjin, për identifikimin, mbledhjen dhe ruajtjen e provave elektronike është jetike. Procedurat penale ngërthejnë në vete përherë e më shumë krime kibernetike ose prova elektronike të gjetura në sisteme kompjuterike ose në pajisje për ruajtje të dhënash. Ngjashëm kjo vlen edhe për të ardhura nga veprat penale.

Duke marrë parasysh se shoqëritë në mbarë botën mbështeten në teknologji të informimit dhe komunikimit, gjyqtarët dhe prokurorët duhet të jenë të përgatitur të merren me krime kibernetike dhe prova elektronike. Përderisa në shumë vende autoritetet e zbatimit të ligjit ia kanë dalë të forcojnë kapacitetet e tyre për t'i hetuar krimet kibernetike dhe për të siguruar prova elektronike, përqendrimi në kërkesat për gjyqtarë dhe prokurorë ka qenë më i vogël. Përvojat tregojnë se në shumicën e rasteve, gjyqtarët dhe prokurorët hasin në vështirësi kur ballafaqohen me realitete të reja në botën kibernetike. Andaj kërkohen përpjekje të veçanta për t'u mundësuar gjyqtarëve dhe prokurorëve të ndjekin penalisht dhe t'i gjykojnë krimet kibernetike dhe t'i përdorin provat elektronike përmes trajnimeve, rrjetëzimeve dhe specializimeve.

¹Shih paragrafin 317, Rrjedha e parave të krimit në Internet: metodat, trendët dhe luftimi shumëpalësh, nga Raporti Hulumtues MONEYVAL, mars 2012. Gjendet në: [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)

Këshilli i Evropës ka krijuar një koncept për të mbështetur këto përpjekje përmes Projektit kundër krimeve kibernetike në bashkëpunim me Rrjetin e Lisbonës për institucionet e trajnimeve gjyqësore në bashkëpunim me një grup punues shumëpalësh gjatë vitit 2009.

Qëllimi i konceptit ishte të ndihmoheshin institucionet e trajnimeve gjyqësore për të krijuar programe trajnuese rreth krimeve kibernetike dhe provave elektronike për gjyqtarët dhe prokurorët dhe për t'i integruar ato trajnime në trajnimet e rregullta para dhe gjatë shërbimit.

Objektivat e konceptit të trajnimit për gjyqtarët dhe prokurorët janë:

- Të ndihmohen institucionet trajnuese të mbajnë trajnime para dhe gjatë shërbimit lidhur me krimet kibernetike në përputhje me standardet ndërkombëtare
- Të pajiset numër sa më i madh i gjyqtarëve dhe prokurorëve të ardhshëm dhe aktualë me njohuri për krimet kibernetike dhe provat elektronike.
- Të mbahen trajnime të avancuara për një numër të madh të gjyqtarëve dhe prokurorëve
- Të mbështetet specializimi i vazhdueshëm dhe trajnimi teknik i gjyqtarëve dhe prokurorëve
- T'i kontribuohet rritjes së njohurive përmes krijimit të rrjeteve mes gjyqtarëve dhe prokurorëve
- Të lehtësohet qasje në nisma të ndryshme trajnuese dhe rrjete.

Në këtë kontekst, përmes Projektit të Përbashkët Rajonal të Bashkimit Evropian dhe Këshillit të Evropës kundër Krimeve Kibernetike@IPA (Bashkëpunimi Rajonal në Drejtësinë Penale: Forcimi i kapaciteteve në luftën kundër krimeve kibernetike materiale trajnuese rreth krimeve kibernetike dhe provave elektronike janë përgatitur për t'u përdorur nga institucionet e tilla trajnuese.

Duke marrë në konsideratë suksesin dhe vlerën e dëshmuar gjatë trajnimeve bazike dhe të avancuara për gjyqtarë dhe prokurorë në krime kibernetike dhe prova elektronike, përmes Projektit të Përbashkët të Bashkimit Evropian dhe të Këshillit të Evropës iPROCEEDS² janë përgatitur edhe dy module trajnimi: një modul bazik dhe një i avancuar për hetime, sekuestime dhe konfiskime të të ardhurave nga krimi kibernetik.

Në përgjithësi, aktivitetet e kriminelëve dhe të organizatave kriminale janë të dizajnuara për të krijuar profite. Sipas vlerësimeve të Kombeve të Bashkuara, shuma e përgjithshme e të ardhurave nga krimi në vitin 2009 ishin rreth 2.1 trilion dollarë, ose 3,6% e GDP-së globale, por vetëm një pjesë e vogël e atyre fondeve janë kthyer ndonjëherë³. Përqendrimi edhe në të ardhurat nga krimi gjatë kryerjes së hetimeve financiare paralelisht me hetimet penale mund të nxjerr në shesh prova edhe të veprës penale të pastrimit të parave. Pastrimi i parave u mundëson organizatave kriminale të përfitojnë nga aktivitetet e tyre të paligjshme dhe t'i vazhdojnë operacionet e tyre.

² Projekti i përbashkët i Bashkimit Evropian dhe Këshillit të Evropës "Luftimi i të ardhurave nga krimi në internet në Evropën Juglindore dhe Turqi" - iPROCEEDS synon forcimin e kapaciteteve të autoriteteve në rajonin e IPA-s për të kontrolluar, sekuestruar dhe konfiskuar të ardhurat nga krimet kibernetike dhe për të parandaluar pastrimin e parave në Internet. <http://www.coe.int/en/web/cybercrime/iproceeds>

³Memorandum shpjegues për Propozimin për një Direktivë të BE-së që lufton pastrimin e parave sipas ligjit penal (22.12.2016). Gjetet në: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0826>

Ndikimi financiar i krimeve kibernetike dhe shkalla e të ardhurave të ndërlidhura me to është vështirë të caktohet në shifra në mungesë të të dhënave dhe hulumtimeve të besueshme, por rastet tregojnë se të ardhurat nga krimet kibernetike pastrohen përmes skemave të sofistikuara që ngërthejnë në vete metoda si tradicionale ashtu edhe të reja të pagesës⁴. Megjithatë, hetimet e krimeve kibernetike rrallë shoqërohen nga hetimet financiare dhe anasjelltas, hetimet e veprave penale financiare ose të tjera rrallë shoqërohen nga hetimet e krimeve kibernetike.

Grupet e krimit të organizuar fshehin dhe i investojnë prapë pasuritë e tyre në shtete të tjera jashtë atij ku është krijuar pasuria nga krimi i kryer. Kjo e ndërlikon edhe më tej punën e autoriteteve kompetente për ta luftuar krimin e rëndë dhe të organizuar ndërkufitar. Në frymën e njëjtë, edhe rrjedha e parave nga krimi kibernetik dhe nga veprat penale në Internet nuk ndalet brenda kufijve gjeografikë. Për ta adresuar këtë fenomen në mënyrë gjithëpërfshirëse aktivitetet hetuese duhet të tejkalojnë kufijtë dhe të operojnë me juridiksione të ndryshme. Andaj, bashkëpunimi efektiv ndërkombëtar po ashtu është kyç për kontrollin, sekuestrimin dhe konfiskimin e të ardhurave nga krimi kibernetik.

Koncepti i shënjestrimit të të ardhurave nga krimet kibernetike në këtë kurs trajnimi bashkon qasjet e krimit kibernetik, hetimet financiare dhe të pastrimit të parave me qëllim që të rritet efikasiteti dhe suksesi i hetimeve penale dhe i procedurave penale si nga këndvështrimi i ndjekjes së kriminelëve ashtu edhe i luftimit të të ardhurave nga krimi.

1.1 Qëllimi i kursit

Kursi ka për qëllim të lehtësojë trajnimin e vazhdueshëm të gjyqtarëve ose prokurorëve të interesuar, të cilët kanë mbaruar kursin bazik të hetimeve, sekuestrimeve dhe konfiskimeve të të ardhurave nga krimi kibernetik dhe të cilët dëshirojnë ta vazhdojnë avancimin në këtë fushë. Qëllimi është të rriten njohuritë e gjyqtarëve dhe prokurorëve të interesuar përkitazi me peizazhin ligjor dhe teknik pasi që ato zbatohen për të ardhurat nga krimet elektronike. Kjo arrihet përmes një studimi më të hollësishëm të temave të përzgjedhura të interesit në këtë fushë.

Kursi do të mbulojë më në hollësi temat e përzgjedhura në fushat në vazhdim:

- Sfidat ligjore dhe teknike të hetimeve të cilat përfshijnë në vete edhe rrjedhën e parave nga krimi në internet.
- Çështjet praktike të hetimeve ndërkufitare.
- Shfrytëzimin e valutave virtuale dhe rreziqet që bartin ato.

Kjo përcillet me punë praktike në formë të hulumtimit të literaturës dhe studimit të rasteve që studentët mund t'i shqyrtojnë.

1.2 Grupi i synuar i studentëve

Ky kurs është i dizajnuar për gjyqtarët dhe prokurorët të cilët e kanë kryer kursin bazik për kontrollin, sekuestrimin dhe konfiskimin e të ardhurave nga krimi kibernetik. Pritet që shfrytëzuesit e këtij doracakut të kenë njohuri të mëhershme për:

- Kuptimin e krimeve kibernetike dhe natyrën hetimit të krimeve kibernetike

⁴Rrjedha e parave të krimit në Internet - metodat, trendët dhe luftimi shumëpalësh, Raporti Hulumtues MONEYVAL, mars 2012.

- Natyrën e hetimeve financiare
- Veprën penale të pastrimit të parave dhe rolin e Njesisë për Inteligjencë Financiare (NJIF)
- Njohuri elementare teknike siç është adresa e IP-së.
- Njohuri elementare të karakteristikave të provave elektronike.

Të gjitha këto parakushte mund të plotësohen me ndjekjen e kursit të Këshillit të Evropës "Kurs Bazik për Kontrollin, Sekuestrimin dhe Konfiskimin e të Ardhurave nga Krimi Kibernetik".

1.3 Tabela e përmbajtjes

1.3.1 Sfidat e hetimeve elektronike (online)

Në kursin elementar prezantohen një varg rrjedhash të parave në mënyrë elektronike dhe tipologjitë e pastrimit të parave. Qëllimi i kësaj pjesë është të diskutohen më në hollësi disa sfida hetuese të cilat mund të shfaqen me një përzgjedhje të tipologjive të përshkruara aty. Kjo përfshin diskutime të sfidave hetuese të që lidhen me identifikimin e një keqbërësi online, identifikimin e të ardhurave nga krimet online, si dhe sfidat që lidhen me angazhimin e Provajderëve vendorë, ndërkombëtarë dhe shumëkombëtarë të Shërbimeve të Internetit (ISP).

1.3.2 Hetimet ndërkufitare

Koncepti i shënjestrit të të ardhurave nga krimet kibernetike bashkon qasjet e krimit kibernetik, hetimet financiare dhe të pastrimit të parave me qëllim që të rritet efikasiteti dhe suksesi i hetimeve penale dhe i procedurave penale si nga këndvështrimi i ndjekjes së kriminelëve dhe ashtu edhe i luftimit dhe konfiskimit të të ardhurave nga krimi.

Ndonëse ndihma e ndërsjellë juridike ende konsiderohet si mjeti kryesor për t'i zbatuar urdhrat e gjykatës dhe për të mbledhur prova jashtë vendit, kohëzgjatja e procedurës paraqet një pengesë të rëndësishme. Megjithatë, shfrytëzimi i hetimeve të përbashkëta dhe i ekipeve të përbashkëta hetuese mund t'i adresojë disa sfida të efikasitetit. Bashkëpunimi mes organeve të zbatimit të ligjit (policisë dhe prokurorisë) dhe këmbimi i informacioneve janë të rëndësishëm jetike për rastet ndërkufitare. Rrjetet relevante luajnë rol të rëndësishëm në këtë aspekt.

Për qëllime të këtij kursi të avancuar është e dobishme të vihen në pah disa nga gjetjet e fundit rreth pengesave të cilat janë identifikuar nga organizatat ndërkombëtare për zbatimin e standardeve ndërkombëtare në legjislacionin dhe praktikën vendore, si dhe rekomandimet të cilat do të mund të përdoren si burim i frymëzimit.

1.3.3 Valutat virtuale

Pas terminologjisë elementare rreth valutave virtuale të cilat janë diskutuar në kursin fillestar, ky kurs shtjellon edhe më tej pjesëmarrësit në ekosistemin e valutave virtuale, përfshirë këmbimin e valutave virtuale, shërbimet e kuletës (wallet services), etj. Operacioni i valutës virtuale Bitcoin është i përshkruar dhe përcillet me një shpjegim të rreziqeve dhe sfidave që lidhen me hetimin që përfshin valutat virtuale si dhe menaxhimin e bastisjeve dhe sekuestrimit të pasurisë së tyre.

1.3.4 Punë praktike/raste studimore

Me qëllim që të ndihmohen studentët t'i vënë informatat e shpalosura në këtë kurs në kontekst të legjislacionit të tyre vendor, janë dhënë disa hulumtime udhëzuese të literaturës dhe disa raste studimore për t'u mundësuar studentëve që ata vetë, në kohën e tyre, të hulumtojnë edhe më tej çështjet e ngritura këtu.

2 Sfidat e hetimeve elektronike (online)

2.1 Tipologjitë e pastrimit të parave online

Në kursin elementar prezantohen një varg rrjedhash të parave në mënyrë elektronike dhe tipologjitë e pastrimit të parave. Qëllimi i kësaj pjesë është të diskutohen më në hollësi disa sfida hetuese të cilat mund të shfaqen me një përzgjedhje të tipologjive. Ekzistojnë dy probleme shumë të mëdha dhe shumë të shpeshta të cilat do të diskutohen ndaras në kapitujt e tyre të këtij kursi; sfidat hetuese që lidhen me identifikimin e një keqbërësi online (shih Kapitullin 2.2) dhe sfidat e pafundme që lidhen me shfrytëzimin e valutave virtuale (shih Kapitullin 5).

2.1.1 Shfrytëzimi i shërbimeve bankare përmes internetit

Disa nga tipologjitë e diskutuara në kursin bazik përqendrohen në rastet kur kriminelët kanë qasje në një llogari bankare. Në veçanti kjo lidhet me tipologjitë e transfereve elektronike, marrjen e kontrollit mbi llogari bankare dhe transferet ndërkombëtare. Kriteret rregullative për institucionet financiare, përkitazi me kujdesin e duhur, mbajtjen e regjistrave, etj., kuptohen mirë⁵. Megjithatë, kriminelët mbështeten në natyrën e mjedisit bankar elektronik kur nuk keni nevojë të paraqiteni fizikisht për t'i shmangur këto kontrole⁶. Kur nuk ekziston nevoja për kontakt të drejtpërdrejtë me klientin, është e mundshme që një kriminel, për shembull, të shtirët si klienti legjitim i bankës (p.sh., duke vjedhur ose shfrytëzuar kredencialet elektronike bankare) në një mënyrë që është më e vështirë për institucionin financiar ta identifikojë.

Ekzistojnë tri pista kryesore që duhet ndjekur për hetimin e rasteve të tilla:

- Mënyrën si është komprometuar llogaria bankare (p.sh., sigurimi i detajeve për llogarinë duke u shtirë si pronari i saj (fishingu), infeksioni nga softuerët dashakeqë). Provat për këtë mund të sigurohen nga pronari i llogarisë, i cili sipas të gjitha gjasave është viktimë.
- Informata për qasje (login) në llogarinë e komprometuar bankare. Këto informata mund të sigurohen nga institucionet financiare.
- Llogarinë/llogaritë bankare të shfrytëzuara për transferimin e parave nga llogaria e komprometuar. Këto informata janë në dispozicion të institucionit financiar dhe mund të ndihmojnë në identifikimin e individëve të rekrutuar për të transferuar paratë, (money mules) të përfshirë në gjurmimin e parave për sekuestrimin përfundimtar.

Në pjesën e mbetur të këtij kapitulli do të diskutohen disa probleme të caktuara hetuese të cilat janë ndërlikuar edhe më shumë nga përdorimi i shërbimeve elektronike bankare.

Së pari, është më e vështirë të përcaktohet natyra e marrëdhënies, nëse ka të tillë, mes pronarit të llogarisë bankare dhe të dyshimit. Për shembull:

1. A është pronari i llogarisë bankare i vetëdijshëm për aktivitetin e të dyshimit?

⁵ Standardet ndërkombëtare për luftimin e pastrimit të parave dhe financimin e terrorizmit dhe përhapjes së armëve, Task Forca e Veprimit Financiar (FATF) Rekomandime, 2012. Gjetet në:

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

⁶ Raporti i FATF, Pastrimi i parave duke përdorur metodat e reja të pagesës, tetor 2010. Gjetet në:

<http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf>

2. A ka i dyshimti kontroll të drejtpërdrejtë mbi llogarinë bankare apo a është i dyshimti duke i drejtuar veprimet e pronarit të llogarisë bankare?
3. A është e mundshme të identifikohet personi i cili e ka kryer një transaksion të caktuar në një llogari?

Me këto pyetje dhe shumë të tjera, duhet të jetë e qartë se natyra e mosballafaqimit fizik të mjedisit bankar elektronik e bën më sfidues vërtetimin e fakteve gjatë hetimeve.

Së dyti, shfrytëzimi i shërbimeve elektronike bankare po ashtu paraqet disa sfida për identifikimin e vetë aktivitetit të dyshimtë. Në një filiale, kur një i dyshimtë prezantohet dhe mundohet ta kryejë një transaksion, të paktën ekziston mundësia që një sporteliste në bankë ta identifikojë nëse aktiviteti i kryer është qartazi i dyshimtë. Në mjedisin elektronik procesimi i transaksioneve është kryesisht automatik. Kur kjo kombinohet me strukturimin e fondeve për t'i shmangur kufijtë e raportimit mund të shpie te rreziku i shtuar që transaksionet e dyshimta të mos vërehen. Për ta luftuar këtë, institucionet financiare shpesh shfrytëzojnë softuerë automatikë për monitorim të transaksioneve, funksioni i të cilëve është të zbulojnë transaksionet që deviojnë nga profili i transaksioneve të rëndomta të kryera nga një llogari e veçantë.

Disa, por jo të gjithë, softuerët për monitorim të mashtrimeve po ashtu kontrollojnë adresën e IP-së të cilën një llogari bankare elektronike supozohet ta ketë përdorur. Nëse, për shembull, adresa e IP-së nuk është përdorur kurrë më parë nga një llogari bankare, kjo mund të nxisë dyshimin se llogaria bankare elektronike mund të jetë komprometuar. Megjithatë, nga këndvështrimi praktik për institucionet financiare, ekziston një baraspeshë e brishtë mes zbulimit dhe parandalimit të mashtrimit në njërën anë dhe mosndërhyrjes në aktivitetet legjitime bankare të klientëve mobilë globalë në anën tjetër.

Për më tepër, edhe nëse një llogari bankare elektronike e një klienti është komprometuar, kjo nuk do të jetë gjithmonë e qartë nga adresa e IP-së që është shfrytëzuar për kycje (login). Kjo për faktin se në rastet kur kompjuteri personal i klientit është infektuar me ndonjë virus, është e mundshme që kriminelit të ketë kontroll mbi kompjuterin e klientit. Kjo do t'i mundësojë kriminelit që të kyçet në llogarinë e klientit nga adresa e IP së kompjuterit të klientit, duke shmangur kështu ndezjen e alarmit për shkak të kyçjes nga një adresë e pazakontë e IP-së.

Së treti, është çështja e provave shtesë të cilat janë të nevojshme për të demonstruar aktivitetet e të dyshimit dhe nëse ajo provë është në dispozicion. Adresa e IP-së nga e cila kyçet një llogari e caktuar sipas të gjitha gjasave është e regjistruar nga institucioni financiar, por nuk është gjithmonë lehtë e qasshme. Kërkohen përpjekje të mëdha për të identifikuar se cilat adresa të IP-ve janë përdorur për cilat kycje dhe nga cilat llogari. Kjo ndodh për shkak të kompleksitetit të infrastrukturës së shërbimeve bankare elektronike e në veçanti për faktin se kyçjet mund të mos ruhen ose ndërlidhen në një mënyrë që siguron qasje të lehtë në informatat e kërkuara. Për më tepër, nëse dhe kur të identifikohet një adresë e IP-së e cila është përdorur, lidhja e të dyshimit me atë adresë të IP-së është një sfidë e veçantë.

2.1.2 Shfrytëzimi i shërbimeve të tjera financiare në internet

Shërbimet e tjera (jobankare) financiare përmes internetit luajnë rol te disa tipologji të diskutuara në kursin bazik. Në veçanti shfrytëzimi i sistemeve të pagesës përmes internetit, blerjeve përmes internetit dhe shfrytëzimi i platformave online për lojëra të fatit/tregti. Sërish, natyra e mosballafaqimit fizik e raporteve mes shërbimit dhe

shfrytëzuesit të shërbimit paraqet mundësi për kriminelët që t'i shfrytëzojnë këto lloje të shërbimeve.

Fundja, këto shërbime do të kenë nevojë për një lloj forme të bashkëveprimit me sektorin tradicional të shërbimeve financiare. Kjo më së shpeshti ndodh përmes përdorimit të kartelave për pagesë, të cilat shfrytëzohen për ta "mbushur" një llogari me provajderin e shërbimeve financiare në internet. Pasi të jenë bartur fondet nga një pagesë përmes kartelës të ofruesi i shërbimit, natyra e bashkëveprimeve pasuese mes përdoruesit dhe ofruesit të shërbimeve elektronike financiare janë është e turbullt në sistemin financiar tradicional. Andaj, rekomandohet që shërbimet e pagesave elektronike t'u nënshtrohen obligimeve të pajtueshmërisë dhe mbikëqyrjes⁷. Natyra e kësaj rregulloreje mund të ndryshojë nga një juridiksion në tjetrin.

Merrni në konsideratë, për shembull, konceptin e mikropagesave⁸. Nuk do të kishte kuptim financiar që një shërbim elektronik i pagesave menjëherë të ngarkojë çdo mikropagesë në kredit kartë të përdoruesit sepse tarifat për pagesën e kartës do ta shlyenin çdo profit për shërbimet e pagesës në atë transaksion. Në vend të kësaj, shërbimet e pagesës në mënyrë tipike bashkojnë një varg pagesash për një periudhë kohore dhe dorëzojnë një faturë të vetme për të gjitha aktivitetet e përdoruesit brenda një periudhe të caktuar kohore. Andaj shërbimet e pagesave e marrin përsipër një lloj rreziku nga mashtrimet, por pasi që shumica e parave të përfshira në pagesa individuale është zakonisht shumë e vogël, edhe humbjet e përgjithshme priten të jenë të vogla.

Një model i mikropagesës nganjëherë ofrohet edhe nga operatorët e telefonisë mobile. Në këto raste, përdoruesi i bën mikropagesat duke përdorur telefonin e vet ose numrin e telefonit dhe se tarifat i ngarkohen përdoruesit në faturën e radhës të telefonit mobil.

Në këto raste, më e rëndësishmja për një hetues është të qartësohet natyra e aktivitetit të paligjshëm (mashtrim, qasje e paautorizuar), llojet e të dhënave të cilat mund të grumbullohen dhe nga cilat burime me qëllim që të dëshmohet aktiviteti penal dhe të gjurmohet rrjedha e parave.

Në shumicën e rasteve, viktimat njoftohen në fazë të mëvonshme rreth mashtrimeve që përfshijnë llogaritë e tyre bankare ose kartelat bankare. Sidoqoftë, ofruesit e shërbimit të pagesave janë në gjendje të identifikojnë aktivitetet e paligjshme dhe të ruajnë të dhënat, të cilat më vonë mund t'u jepen hetuesve.

Sfidat kryesore që dalin nga përdorimi i shërbimeve për pagesa elektronike lidhen me faktin se të dhënat e kërkuara zakonisht ndodhen në një juridiksion tjetër. Përfshirja e ofruesve të shërbimeve shumëkombëshe dhe e procesit të ndihmës së ndërsjellë juridike mund ta ngadalësojnë dukshëm dhe ta shtojnë kompleksitetin e një hetimi.

Probleme të ngjashme shfaqen me përdorimin e platformave të cilat e mundësojnë blerjen përmes internetit. Siç është diskutuar në kursin bazik, blerja e mallrave ose shërbimeve përmes internetit, të cilat pastaj dërgohen te kriminelin ose personin i kontraktuar, është mënyrë e mirë e konvertimit të kredencialeve të vjedhura për pagesë në vlerë të botës reale. Në këto raste, hetimi mbështetet plotësisht në regjistrat e të dhënave të platformës blerëse dhe në mundësinë e tyre për t'i identifikuar aktivitetet e dyshimta. Sërish, shumica e hetimeve do ta kuptojnë se shumica e platformave për blerje elektronike e kanë selinë

⁷ Raporti i FATF, Pastrimi i parave duke përdorur metodat e reja të pagesës, tetor 2010. Gjetet në: <http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf>

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

në një juridiksion tjetër. Mbledhja e provave nga këto organizata ka si kriter dërgimin e një kërkesë për ndihmë juridike të ndërsjellë te juridiksioni në fjalë.

Platformat e lojërave elektronike të fatit po ashtu paraqesin disa sfida unike të cilat kryesisht shfaqen nga rregullimi jokonsistent i këtyre entiteteve nëpër botë. Për shembull, në disa juridiksione lojërat elektronike të fatit janë ilegale, kështu që bashkëpunimi me operatorin e një kompanie për lojëra elektronike të fatit në këto raste mund të nënkuptojë njohjen e këtyre entiteteve dhe kështu mund të paraqesë sfida ligjore. Brenda BE-së, për shembull, 20 shtete anëtare i lejojnë lojërat elektronike të fatit dhe shtatë nuk i lejojnë. Sipas legjislacionit aktual, disa kanë vendosur t'i lejojnë ose t'i ndalojnë lojërat elektronike të fatit, ndërsa të tjerat i lejojnë ose i ndalojnë në mënyrë "pasive" duke vazhduar ta zbatojnë legjislacionin e hartuar, shpesh shumë vite më parë, për lojërat konvencionale të fatit. Nga njëzet Shtetet Anëtare të cilat i lejojnë lojërat elektronike, trembëdhjetë operojnë në një treg të liberalizuar, gjashtë operojnë monopole në pronësi të shtetit dhe një ka një monopol të licencuar privat⁹.

2.1.3 Shfrytëzimi i shërbimeve të komunikimit përmes internetit

Interneti është përfundimisht një platformë komunikimi dhe kriminelët i përdorin shërbimet e komunikimit për të mundësuar aktivitetet e tyre. Brenda kontekstit të rrjedhës së parave nga krimi në internet në veçanti, shërbimet e komunikimit në internet mundësojnë rekrutimin e personave për transferim të parave, komunikim dhe menaxhim. Shërbimet siç janë email, bisedat përmes internetit, dërgimi i porosive dhe shërbimet telefonike të cilat janë në dispozicion online mund të shfrytëzohen nga kriminelët për të organizuar aktivitetet e tyre.

Vështirësitë teknike mund të shfaqen si gjatë identifikimit të palëve komunikuese ashtu edhe për identifikimin e thelbit të komunikimit. Çështja e identifikimit të të dyshimtëve në internet është diskutuar në hollësi në Kapitullin 2.2.

Trendi i viteve të fundit ka shkuar drejt një përqendrimi të shtuar të ofruesve të shërbimeve të internetit në sigurimin e privatësisë për klientët e tyre. Kjo është manifestuar në shumë raste siç është përdorimi i shtuar i enkriptimit. Enkriptimi shfrytëzohet kryesisht në tri mënyra¹⁰:

- **Enkriptimi i gjithë diskut apo pajisjes:** Në rastin e një laptopi ose kompjuteri personal, teknologjitë për të enkriptuar gjithë përmbajtjen e pajisjes për ruajtje të informatave (hard drive) kanë ekzistuar që një kohë. Po ashtu ka qenë e mundur që një kohë që të enkriptohen edhe të dhënat e pajisjes së telefonit siç janë telefonat e mençur. Rreth vitit 2014 kompanitë e teknologjisë si Apple dhe Google kanë filluar ta mundësojnë enkriptimin e pajisjes thuajse në mënyrë automatike në telefonat e tyre të mençur. Dekriptimi apo qasja në pajisje zakonisht kërkon një frazë kalimi apo PIN. Kërkesa legjitime për një enkriptim të tillë është të mbrohen të dhënat personale të pronarit të telefonit të mençur nga humbja ose vjedhja e pajisjes.

⁹Studim nga Departamenti i Politikave, nga Politikat Ekonomike dhe Shkencore i Parlamentit të BE-së, me titull "Lojërat elektronike të fatit, me përqendrim në integritet dhe një kod të sjelljes për lojërat e fatit". IP/A/IMCO/FWC/2006-186/C1/SC2. Gjetet në: [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)

¹⁰Enkriptimi çështje e të drejtave të njeriut, Raport nga Amnesty International, mars 2016. Gjetet në: http://www.amnestyusa.org/sites/default/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf

- **Enkriptimi nga një skaj në tjetrin (end-to-end):** Kjo shprehje vlen për enkriptimin e porosive të dërguara përmes një platforme të porosive në atë mënyrë që ato të jenë të lexueshme vetëm nga dërguesi dhe pranuesi i porosive. Shumë shërbime të porosive, përfshirë iMessage, WhatsApp dhe Facebook Messenger ofrojnë variacione të enkriptimit nga një skaj në tjetrin (end-to-end) për mesazhe. Nëse marrim iMessage si shembull, përdorimi i enkriptimit nga një skaj në tjetrin nënkupton se edhe Apple, ofruesit e shërbimit, nuk kanë qasje në përmbajtjen e porosive.
- **Enkriptimi për bartje të dhënash:** Kjo formë e enkriptimit i referohet enkriptimit të të dhënave për bartje mes dy palëve. Më së shpeshti këto ditë përdoret për t'iu referuar enkriptimit të trafikut nëpër uebsajte. Enkriptimi për bartje të dhënash është njëri nga kontrollet më themelore të sigurisë të pajisjeve të botës moderne e-commerce dhe e-banking, duke ia pamundësuar çfarëdo sulmuesi që të jetë në gjendje ta përgjojë komunikimin mes një klienti dhe një banke ose një uebsajti e-commerce.

Në rastet që përfshijnë përdorimin e enkriptimit për bartje të dhënash, masat e veçanta hetuese, siç është përgjimi i komunikimeve ende mund të jenë teknikisht të mundshme, me bashkëpunimin e palëve relevante siç është pronari i uebsajtit dhe/ose Ofruesi i Shërbimeve të Internetit. Sigurimi i qasjes në një pajisje të enkriptuar ose në një komunikim që është enkriptuar nga një skaj në tjetrin është më sfidues dhe shpesh do të kërkojë qasje në pajisjen ose kompjuterin personal të të dyshimit.

RAST STUDIMOR: APPLE KUNDËR. FBI¹¹

FBI kërkonte të hapej një iPhone 5C i përdorur nga njëri nga gjuajtësit në një sulm në San Bernardino, Kaliforni, që la 14 të vrarë në dhjetor të vitit 2015.

Më 16 shkurt 2016, si përgjigje ndaj një kërkesë nga Departamenti Amerikan i Drejtësisë, një gjyqtar federal urdhëroi Apple ta krijojë një version të zakonshëm të sistemit të tij operativ iOS që do t'u mundësonte hetuesve në atë rast t'u shmangeshin karakteristikave të sigurisë së telefonit. Kryeshefi ekzekutiv i Apple, Tim Cook, u përgjigj në një letër të hapur, në të cilën deklaronte se kërkesat e qeverisë përbënin "shkelje të privatësisë" me pasoja të "frikshme". Cook tha:

"Kur FBI ka kërkuar për diçka që kishim në posedim, ne e kemi siguruar. Apple u është bindur fletëthirrjeve të vlefshme dhe mandateve të bastisjes, siç i kemi pasur në rastin San Bernardino. Po ashtu kemi vënë në dispozicion inxhinierët e Apple për ta këshilluar FBI dhe kemi ofruar idetë tona më të mira në një varg të opsioneve hetuese që ata i kishin në dispozicion...Por tash, Qeveria e SHBA-ve na ka kërkuar diçka që nuk e kemi dhe diçka që e konsiderojmë shumë të rrezikshme që ta krijojmë. Ata kanë kërkuar prej nesh të ndërtojmë një derë të pasme në iPhone."

Apple u ankua kundër urdhrit të gjykatës dhe një seancë dëgjimore në gjykatë u caktua për 22 mars 2016. Ekspertë të shumtë të pavarur të teknologjisë, profesorë të juridikut, kompani të teknologjisë dhe organizata të të drejtave të njeriut kanë mbështetur qëndrimin e Apple në këtë çështje. Këndvështrimi shumë i mbështetur mes atyre që kundërshtojnë kërkesën e FBI, përfshirë edhe Amnesty International, ishte se nëse Apple

¹¹ Ibid.

detyrohej ta ndryshonte softuerin për ta hapur këtë telefon, kjo do të përbënte një precedent që do t'i mundësonte Qeverisë së SHBA-ve - e mundësisht edhe qeverive të tjera - për t'i detyruar kompanitë e teknologjisë t'i zbusin ose ndryshe t'i shmangen enkriptimeve duke siguruar një 'derë të pasme' për inteligjencën dhe agjencitë e tjera të sigurisë.

Në përgjigjen e tij në këtë rast, Komisioneri i Lartë i KB për të Drejta të Njeriut deklaroi: "Një rast i suksesshëm kundër Apple në SHBA do të përbëjë një precedent që mund ta bëjë të pamundur për Apple ose për cilëndo kompani tjetër të madhe të TI ta mbrojë me sukses privatësinë e klientëve kudo në botë --- me mundësi të shërbejë si dhuratë për regjimet autoritare si dhe për hakerët kriminelë. Po ashtu ka pasur një varg përpjekjesh të bashkërenduara nga autoritetet në shtete të tjera për t'i detyruar kompanitë e TI dhe komunikimeve si Google dhe Blackberry për t'i ekspozuar klientët e tyre ndaj përgjimeve masive."

Më 28 mars, FBI deklaroi se e kishte hapur iPhone me ndihmën e një pale të tretë dhe Departamenti i Drejtësisë e tërhoqi rastin.¹²

2.1.4 Hostingu i padepërtueshëm

Kushtet e shërbimit për shumicën e shërbimeve të internetit dhe të hostingut për uebfaqe nuk lejojnë aktivitete të paligjshme në rrjetet ose shërbimet e tyre. Andaj ata zakonisht bashkëpunojnë me organet e zbatimit të ligjit për kërkesa për informata dhe për kërkesa për mbyllje të domeneve dhe uebsajteve të paligjshme.

Hostingu i padepërtueshëm, në anën tjetër, është emri që u jepet shërbimeve të hostingut të cilat nuk bashkëpunojnë me kërkesat e organeve të rendit për informata ose për mbyllje të uebsajteve. Shpesh këto shërbime gjeografikisht ndodhen në vende të tjera (të ndërlidhura me vendet ku zhvillohen hetimet). Në shumicën e rasteve, kompanitë e hostingut të padepërtueshëm do të përpiqen ta mbrojnë veten duke mos pasur përgjegjësi ligjore për aktivitetet penale të kryera nga klientët e tyre që përdorin infrastrukturën e tyre.

Këto shërbime shpesh përdoren për të shpërndarë materiale të paligjshme, për të krijuar emaile spam si serverë për të komanduar dhe kontrolluar softuerët infektues dhe format e tjera të infrastrukturës kriminale^{13, 14, 15}.

Uebsajtet mashtruese të cilat përqendrohen në shërbimet elektronike bankare (dhe të tjera) shpesh i përdorin hostingjet e padepërtueshme për të krijuar uebsajte të cilat duken të ngjashme me uebsajtet legjitime. Këto shpesh mbyllen, ose bllokohen, në bazë të shfrytëzimit të paautorizuar të shenjës dalluese (trademark) të institucioneve financiare. Uebsajtet të cilat nuk përdorin shenjën dalluese të ndonjë organizate legjitime është më e vështirë të mbyllen.

¹² FBI deklaroi se e ka deshifruar iPhone e terroristit pa ndihmën e Apple, CNN, 29 mars 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

Legjislacioni në disa vende mbështet bllokimin nga ISP-të e shtetit, duke përdorur teknika të ndryshme të filtrimeve teknike për përmbajtjen që njihet si e paligjshme¹⁶.

Informatat e siguruara nga kompanitë e hostingut të padepërtueshëm për përdoruesit dhe shërbimet e tyre nuk ndihmojnë shumë për hetime për faktin se detajet e këtyre personave të shumtën e herëve janë të rreme. Megjithatë, metoda e pagesës për shërbimet me qira mund të jenë një pistë e rëndësishme që mund të ndihmojë në identifikimin e burimit të një aktiviteti kriminal.

Për nga aspekti legjislativ ka po ashtu vështirësi për ta vërtetuar juridiksionin e aktiviteteve të paligjshme të kryera pasi që mund të ketë më shumë burime, destinacione ose vende/entitete koordinuese të përfshira.

Në vendet ku ka hosting të padepërtueshëm përgjimet mund të shfrytëzohen gjatë një hetimi. Kjo do të ndihmojë në mbledhjen e informacioneve rreth burimit, destinacionit dhe natyrës së aktivitetit kriminal.

2.1.5 Ekonomia e nëntokës

Ekonomia e nëntokës është termi me të cilin njihen shërbimet e shfrytëzuara nga kriminelët për t'i tregtuar shërbimet dhe informatat mes tyre. Ka pasur shumë shembuj të forumeve të nëntokës, siç është ai i Rugës së Mëndafshit dhe Tregut të Zi (silk road and dark market).¹⁷

Ekonomia e nëntokës është e strukturuar në mënyrë organizative për të kryer krime. Ata shpesh e përdorin modelin afarist të quajtur Crime-as-a-service (Krimi si shërbim).

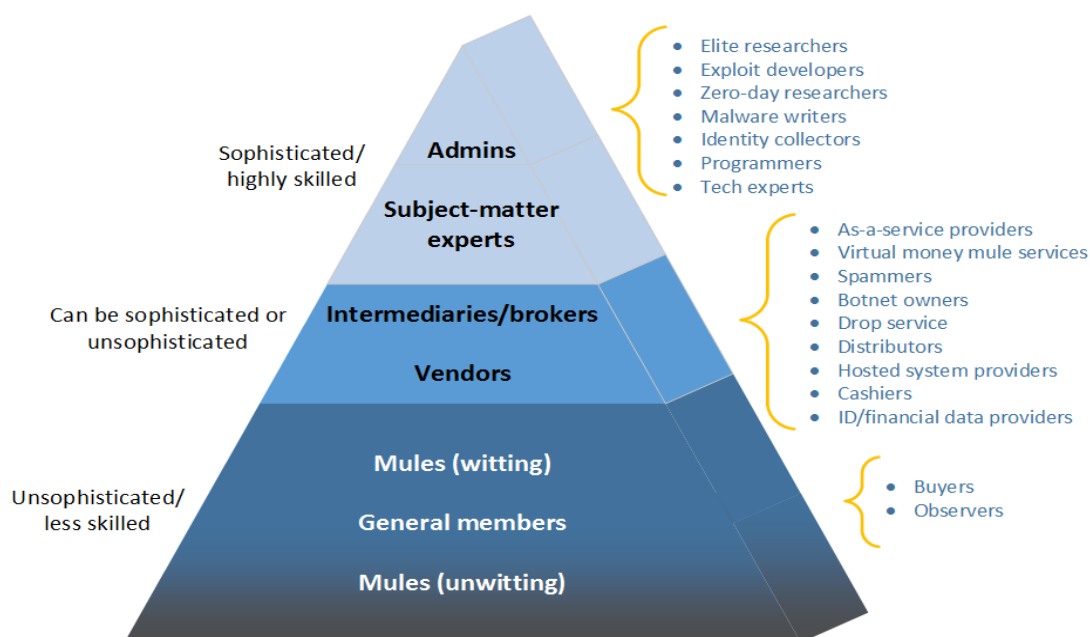


Figura 1: Pjesëmarrësit e Modelit Afarist Kriminal në Darkweb

¹⁶ T-CY(2006)04 Forcimi i bashkëpunimit mes organeve të rendit dhe sektorit privat, shembuj si sektori privat ka bllokuar sajte të pornografisë së fëmijëve, shkurt 2006. Gjendet në: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e6ed1>

¹⁷ Për më shumë informata rreth tregjeve Darknet, shih: <https://www.deepdotweb.com/>

Trajnimi nga Picture Empact

Forumet e nëntokës të cilat kryesisht u dedikohen mashtrimeve rreth kredit kartelave dhe shitjes së të dhënave nga kredit kartelat e vjedhura shpesh njihen si forume të kartelave.

Në shumicën e rasteve këto forume janë të hapura vetëm për "klientë" të kufizuar në bazë të fjalëkalimeve ose masave të sigurisë.

Hetimet e këtyre llojeve të forumeve janë shpesh të gjata dhe komplekse, me agjencitë sekrete që shpesh mundohen që gradualisht të infiltrohen në forume dhe të depërtojnë në pozita me pushtet prej ku do sigurojnë qasje në informata të cilat do mundësojnë ngritjen e akuzave kundër administratorëve dhe operatorëve të forumit. Fakti se kërkohen hetime të tilla komplekse nënkupton se për shumicën e hetimeve nuk do të jetë e mundshme të infiltrohen në një forum të nëntokës për të mbledhur prova për një akt të caktuar kriminal kibernetik ose për një hetim të pastrimit të parave.

Po ashtu, nga këndvështrimi i hetimeve, është e rëndësishme të ketë legjislacion relevant të miratuar që i inkriminon këto aktivitete të paligjshme, që lejon kryerjen e aktiviteteve zbuluese dhe që i konsideron provat e mbledhura të pranuar në gjykatë. Hetimi është një përzjerje e teknikave klasike të hetimeve dhe teknikave online.

Në rastet kur pronarët ose operatorët e një forumi të nëntokës janë të pranishëm brenda legjislacionit shtetëror, ose ku forumi i nëntokës mbahet brenda juridiksionit shtetëror, dispozitat relevante reale në legjislacionin shtetëror do të mund të përdoren si bazë për procedurë penale në këto raste. Dispozitat relevante do të varen nga veçantitë e rastit, por mund edhe të jenë ekuivalente me, për shembull, Nenin 6 të Konventës së Budapestit.

PYETJE PËR VETËREFLEKTIM

1. Cilat kushte duhet të plotësohen para se të autorizohet monitorimi i llogarisë bankare të një të dyshimti?
2. Çfarë baraspeshe është e nevojshme për të mbrojtur interesat e një pale të tretë që ka mundësi të jetë e pafajshme të cilës i është komprometuar llogaria bankare?
3. Cilat dispozita ekzistojnë në legjislacionin tuaj për ta detyruar një të dyshimtë që ta dekriptojë një pajisje ose një dosje të enkriptuar?
4. Cilat masa janë në dispozicion në legjislacionin tuaj shtetëror për ta detyruar një Ofrues të Shërbimeve të Internetit për t'i bllokuar ose filtruar përmbajtjet e paligjshme?

2.2 Identifikimi i keqbërësve

Kujtoni nga kursi bazik se karakteristika kryesore që është përdorur për identifikimin e një të dyshimti në internet është adresa e tyre e IP-së.

Qëllimi i këtij kapitulli është të përshkruhen më në hollësi disa nga sfidat praktike të cilat mund të paraqiten gjatë përpjekjes për ta lidhur një adresë të IP-së me një person. Me fjalë të tjera, në rastet kur ju mund ta lidhni një aktivitet kriminal kibernetik me një adresë të caktuar të IP-së dhe po mundoheni ta identifikoni personin e vërtetë i cili ka pasur kontroll mbi atë adresë të IP-së në kohën kur është kryer aktiviteti kriminal.

Natyrisht se mund të shfaqet edhe pyetja anasjelltas, kur ju e keni një të dyshimtë real dhe mundoheni ta identifikoni adresën e IP-së të përdorur online nga ky person. Në shumë aspekte kjo situatë është më e lehtë për t'u trajtuar dhe këtu mund të përdoren teknikat tradicionale të hetimeve (siç janë masat e veçanta hetuese).

2.2.1 Transferimi i adresës së rrjetit (NAT)

Për të komunikuar në internet kërkohet adresa e IP-së e burimit dhe destinacionit. Në të kaluarën (para futjes në përdorim të NAT), çdo kompjuter duhej të kishte adresën unike të IP-së. Problemi me të është se adresat e IP-së janë ndarë në mënyrë të paefektshme dhe si të tilla janë duke u harxhuar. Zgjidhja afatgjate e mungesës së adresave të IP-së është futja në përdorim e një versioni të IP-së, versionit 6 të IP-së, i cili ka numër shumë më të madh të adresave të IP-së në dispozicion. Ndërkohë, përdoren disa teknika për ta zgjatur jetën e versionit 4 të IP-së, një prej të cilave është NAT.

Ekzistojnë disa shtrirje të caktuara të adresave të IP-së të cilat janë të rezervuara. Me fjalë të tjera, ato nuk janë menduar të përdoren në internet. Por janë menduar të përdoren në rrjete private, siç janë hapësirat e zyrave të brendshme. Hapësirat e rezervuara janë:

1. 10.0.0.0 – 10.255.255.255
 - a. Me fjalë të tjera, çdo adresë e IP-së që fillon me "10"
2. 192.168.0.0 – 192.168.255.255
 - a. Me fjalë të tjera, çdo adresë e IP-së që fillon me "192,168"
3. 172.16.0.0 – 172.31.255.255
 - a. Me fjalë të tjera, çdo adresë e IP-së që fillon me "172" dhe përcillet nga një numër mes "16" dhe "31".
 - b. Kjo hapësirë e rezervuar përdoret më pak se dy të tjerat.

Përdorimi më i shpeshtë i NAT përfshin një organizatë e cila i ndan adresat e IP-së nga njëra prej këtyre hapësirave të të gjithë kompjuterët e tyre në zyrë. Pastaj, kur njëri nga kompjuterët personal në rrjetin e tyre dëshiron të komunikojë me një adresë të IP-së në internet, ruteri i tyre e zëvendëson adresën e IP-së së brendshme me një nga hapësirat e vogla të një adrese të vërtetë të IP-së, internetit. Në shumicën e rasteve, rezultati i këtij procesi është se të gjitha të dhënat e IP-së nga të gjithë kompjuterët personalë në rrjetin e zyrës duken te pjesa tjetër e internetit sikur të vinin nga një adresë e vetme e IP-së.

Shfrytëzimi i NAT është po ashtu shumë i rëndomtë, thuajse gjendet kudo në fakt, në konfiguracionet e internetit broadband nëpër shtëpi. Kjo nënkupton se një përdorues në shtëpi mund të përdorë pajisje të shumta në rrjetin e tyre shtëpiak porse Provajderi i Shërbimit të Internetit ka nevojë që lidhjes së tyre t'ia ndajë vetëm një adresë të vetme të IP-së.

Shumë përshkrime të shkëlqyeshme si funksionon NAT mund të gjenden në internet^{18, 19, 20}. Lexuesit e interesuar inkurajohen të shqyrtojnë disa nga këto referencat për më shumë informacione nëse kërkohet.

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

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

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

Ia vlen të merren në konsideratë implikimet e shfrytëzimit të NAT në hetimet elektronike. Mund të jetë e mundshme të identifikohet adresa e IP-së publike në përdorim gjatë një aktiviteti të caktuar kriminal por nëse NAT është në përdorim, kjo adresë e IP-së mund ta paraqesë edhe aktivitetin elektronik të shumë përdoruesve të pavarur. Andaj kërkohet një hap shtesë hetues për ta përcaktuar lidhjen mes aktivitetit elektronik dhe një përdoruesi individual të kompjuterit personal duke e përdorur një adresë të rezervuar të IP-së pas ruterit të NAT.

Ekziston një mundësi e largët që një organizatë e cila përdor NAT të mund të ketë shënime (logs) të trafikut hyrës dhe dalës që mund të përdoren për ta përcaktuar se cila adresë e IP-së ishte përgjegjëse për krijimin e një pjese të caktuar të trafikut, që mund të jetë objekt i hetimit. Megjithatë, kjo ka pak mundësi të ndodhë. Veç kësaj, në rastet e përdoruesve të zyrave të vogla ose në shtëpi, përdorimi i pajisjeve dhe shërbimeve standarde të ofruara nga ISP-të e tyre, këto shënime nuk sigurohen.

Andaj hetimet duhet ta përdorin një mekanizëm alternativ për ta lidhur adresë e IP-së së të dyshimit me një kompjuter të caktuar. Mund të ekzistojnë karakteristika të caktuara të trafikut që mundësojnë identifikimin e adresës së IP-së së brendshme. Për shembull, aplikacione të caktuara përfshijnë adresën e IP-së së kompjuterit që e gjeneron trafikun brenda vetë trafikut. Si alternativë, mund të ketë tri karakteristika të tjera dalluese, përveç adresës së IP-së të cilat mund të përdoren. Këto mund të përfshijnë emrat e përdoruesve, adresat e emailit, informatat teknike rreth pajisjes së burimit, e kështu me radhë. Përmes analizave të detajuara nga një ekspert, mund të jetë e mundshme të identifikohet burimi i trafikut në këtë mënyrë.

Nëse aktiviteti kriminal ndodhë në kohë reale, mund të aplikohen masa të veçanta hetuese për ta përgjuar trafikun dalës dhe për ta identifikuar kompjuterin e brendshëm në atë mënyrë. Në raste të tilla mund të kërkohet bashkëpunimi i organizatës për ta identifikuar lokacionin e duhur në rrjetin e tyre për ta instaluar një stacion monitorues. Kjo në mënyrë tipike përfshin bashkëpunimin e stafit të TI/administrimit të sistemit dhe këtu duhet të kihet parasysh se nuk ka kurrfarë mënyre për ta kuptuar paraprakisht nëse i dyshimti nuk është njëri nga stafi i TI/administrimit të sistemit i cili pastaj do të kuptonte për hetimin.

Si përmbledhje, NAT paraqet sfidë kur është fjala për lidhjen e një adrese të caktuar të IP-së me aktivitetin e një përdoruesi real. Informata shtesë (përveç adresës së IP-së) të mbledhura nga analiza e aktivitetit elektronik ose, si alternativë, masa të tjera hetuese, do të jenë zakonisht të nevojshme për ta kompletuar hetimin dhe për ta identifikuar të dyshimtin.

2.2.2 Transferimi i adresës së rrjetit përmes sistemeve të besueshme (Carrier Grade Network Address Translation - CGN)

Sfida të reja shfaqen gjatë përdorimit të carrier grade NAT ose CGN. CGN është një teknikë përmes së cilës një ISP mund ta shfrytëzojë NAT për të shndërruar një numër të adresave të abonuar të IP-së në një numër më të vogël të adresave reale të IP-së së internetit.

Në këto raste, CGN nënkupton se, përveç NAT që mund të ndodhë përderisa trafiku lëviz nga një zyrë e vogël ose nga një shtëpi në rrjetin e ISP-së, një NAT i dytë mund të ndodhë brenda rrjetit të ISP-së para se të përcillet në internet^{21, 22}.

²¹ Për informata mbi historikun, linqe të tjera mund të gjenden në:

https://en.wikipedia.org/wiki/Carrier-grade_NAT.

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

CGN dallon nga një NAT i "thjeshtë" që është përshkruar në kapitullin paraprak pasi që jo vetëm që adresa e IP-së së brendshme (private) zëvendësohet me një adresë publike (të jashtme) të IP-së, por edhe numri i portit privat (të brendshëm) TCP/IP zëvendësohet me një numër të portit publik (të jashtëm). Në thelb, CGN lokalizon TCP ose sesionet e UDP nga një hapësirë e adresës së brendshme në një hapësirë të adresës së jashtme. Kjo teknikë i lejon CGN që të tejkalojë disa nga çështjet e shkallëzuara me një NAT të "thjeshtë" por paraqet një problem nga këndvështrimi i hetimeve, respektivisht se në pjesën dërmuese të rasteve, organizatat do ta regjistrojnë adresën e IP-së nga e cila i marrin lidhjet por nuk e regjistrojnë numrin e logut hyrës. Pasi që CGN mundëson që mijëra përdorues ta përdorin adresën e njëjtë publike të IP-së, vetëm adresa e IP-së nduk do të jetë e mundshme për lidhur aktivitetin me një përdorues të veçantë.

Andaj, nëse supozojmë se numri i portit nuk është në dispozicion; ka nevojë për informata shtesë (përveç adresës së IP-së) të mbledhura nga analiza e aktivitetit online për ta identifikuar të dyshimtin.

Europoli, në Vlerësimin e Kërcënimit nga Krimi i Organizuar në Internet, të vitit 2016, i bëjnë disa rekomandime për t'i adresuar sfidat e ngritura nga CGN, si në vazhdim²³:

- Me qëllim që të jeni në gjendje ta gjurmoni një përdorues të fundit të një adrese të IP-së në një rrjet që përdor CGN, organet e rendit duhet të kërkojnë informata shtesë nga ofruesit e shërbimeve përmes procesit ligjor:
- Burimin dhe destinacionin e adresës së IP-së
- Numrin e portit burimor
- Kohën e saktë të konektimit (brenda një sekonde).
- Megjithatë, mungesa e kriterëve të harmonizuara për standardet e ruajtjes së të dhënave në Evropë nënkupton se ofruesit e shërbimit të përmbajtjes, të shërbimit të internetit dhe hostingut të të dhënave nuk kanë obligim ligjor për t'i ruajtur këto lloje të të dhënave, do të thotë se edhe një kërkesë më e elaboruar nga një agjenci e zbatimit të ligjit nuk do të siguronte informata të përdorueshme nga provajderi.
- Ka nevojë për ndryshime rregullative/legjislative për t'u siguruar se ofruesit e shërbimeve të përmbajtjes të ruajnë të dhënat e nevojshme shtesë (portin burimor) të cilat i kërkojnë organet e rendit për t'i identifikuar përdoruesit e fundit.
- Si alternativë, mund të zhvillohen zgjidhje praktike përmes bashkëpunimit mes ofruesve të shërbimeve elektronike dhe organeve të rendit. Disa ofrues të shërbimeve elektronike në Evropë i ruajnë informatat relevante (portin burimor). Një portal mbarëevropian do të mund ta ruante një listë të përditësuar të atyre ofruesve dhe një listë të pikave kontaktuese ose adresave në rast se një hetim ndalohej nga CGN.

2.2.3 Shfrytëzimi i anonimesëve

Anonimusi është një instrument që përpiket që ta bëjë një aktivitet në internet të pagjurmueshëm. Ai vepron si një ndërmjetësues mes një kompjuteri personal dhe pjesës tjetër të internetit dhe qaset në internet në emër të përdoruesit duke fshehur informatat identifikuese të përdoruesit.

²³ Vlerësimi i Kërcënimit nga Krimi i Organizuar në Internet (IOCTA), Europol, 2016 Gjendet në: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016> and 2017 at : <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>

Anonimusët ndahen në dy kategori kryesore;

- **Anonimusët e protokolleve specifike:** Këta punojnë me një protokoll të veçantë. Shembull i kësaj do të ishte një ridërgues anonim i emailave ose një uebproksi anonim.
- **Anonimusët e pavarur të protokolleve:** Këta punojnë duke krijuar një tunel të IP-së përmes të cilit përcillet i tërë trafiku i përdoruesit. Nga këndvështrimi i përdoruesit pranues, trafiku i IP-së duket sikur vjen nga dikush tjetër e jo nga dërguesi origjinal. Shembull i kësaj do të ishte Tor (më herët njihesh si "Ruteri gepë").

Disa shembuj diskutohen në rastet e mëposhtme studimore.

Në hetimet ku përdoret një anonimus dhe kur një ofrues i shërbimit nuk është i gatshëm ose nuk është në gjendje të ofrojë mbështetje për hetimin, mund të ketë nevojë për masa hetuese alternative (jo-teknike) për të arritur përparim.

RAST STUDIMOR: RIDËRGUESI ANONIM I EMAILEVE

Qëllimi i një ridërguesi anonim i emailave është të pranohen porositë, të heqë informatat identifikuese dhe pastaj t'i përcjellë ato te pranuesi i synuar në atë mënyrë që pranuesi nuk mund ta dijë se prej kah ka ardhur emaili origjinal.

Ekzistojnë disa mënyra si kjo mund të arrihet:

- **Ridërguesit e emailave me pseudonime;** heqin adresën e dërguesit, i caktojnë një pseudonim dërguesit dhe e dërgojnë porosinë te pranuesi i synuar. Pranuesi do të jetë në gjendje të përgjigjet duke dërguar një email te personi me pseudonim, të cilin ridërguesi i emailit do t'ia kthejë dërguesit origjinal.
- **Ridërguesit e emailave Cypherpunk (a.k.a. Type I):** Dërgon porosinë te pranuesi duke hequr adresën e dërguesit. Pranuesi nuk mund të përgjigjet në emailin e dërguar përmes këtij lloji të ridërguesit të emailit. Zakonisht dërguesi i porosisë do të dorëzojë porosinë te ridërguesi në formë të enkriptuar. Ridërguesi e dekripton atë dhe e dërgon te pranuesi. Këto lloje të ridërguesve të emailave nuk mbajnë regjistra të transaksioneve.
- **Ridërguesit e emailave Mixmaster (a.k.a. Type II):** Dërguesi e përgatit një email dhe e dërgon te ridërguesi. Porosia përcillet shumë herë përmes një rrjeti nga një ridërgues te një tjetër deri sa ai të arrijë te pranuesi. Pranuesi nuk mund të përgjigjet në email, përveçse nëse jepet një adresë në përmbajtjen e emailit. Duhet të instalohet një softuer i veçantë në kompjuterin personal të përdoruesit për ta shfrytëzuar ridërguesin Mixmaster.
- **Ridërguesit e emailave Mixminion (a.k.a. Type III):** Këto janë të ngjashme me ridërguesit Mixmaster por disa çështje teknike duhet të adresohen. Në veçanti, është e mundur që pranuesi të përgjigjet përmes rrjetit të ridërguesve, pa e ditur se kush ishte dërguesi.

Është e mundur të lidhen shumë ridërgues së bashku në mënyrë që as ata të

mos e dinë se kush e ka dërguar porosinë. Po ashtu është e mundshme që një interface e bazuar në ueb të mund të përdoret, në vend se të përdoret një aplikacion standard ose i rëndomtë i emailit i instaluar në kompjuterin personal të përdoruesit.

RAST STUDIMOR: UEBPROKSI ANONIMUS

Një server i proksit anonim mundohet t'i bëjë anonime aktivitetet e vizitave të uebfaqeve të përdoruesit në internet. Në mënyrë tipike, një proksi anonim do të pranojë kërkesat nga përdoruesit dhe do t'i përcjellë ato. Nga këndvështrimi i uebserverit që pranon kërkesën, kërkesa duket sikur vjen nga një proksi anonim. Përveçse nëse proksi anonim i ka të dhënat në dispozicion për ta lidhur kërkesën e dërguar me një burim të caktuar të adresave të IP-së, kjo nuk do të jetë e mundshme nga analizat e të dhënave të IP-së.

Përdorimi i një uebproksi mbështetet thajse nga çdo brauzer standard, sepse ekzistojnë shumë arsye legjitime pse përdoruesit mund të dëshirojnë ta konfigurojnë një proksi²⁴. Përdorimi i këtyre shërbimeve zakonisht kërkon pak më shumë se konfigurimin e një numri të vogël të opsioneve në softuerin e brauzerit standard.

Megjithatë, përmbajtja e trafikut në ueb ende mund të përmbajë detaje të cilat do të mund të ndihmonin të identifikohet një i dyshimtë. Për shembull, nëse një i dyshimtë futet në një uebsajt përmes një proksi anonim, adresa e IP-së nga e cila ata futen mund të mos jetë në dispozicion, por analizat e trafikut në ueb mund ta zbulojnë emrin e përdoruesit dhe/ose fjalëkalimin e përdorur.

RAST STUDIMOR: TOR (MË HERËT NJIHEJ SI "RUTERI QEPË")

Tor është një instrument softueri që drejton trafikun në internet përmes një rrjeti të kompjuterëve, në pronësi të vullnetarëve dhe që operohet pa pagesë, i përbërë nga disa mijëra ritransmetues (relay). Qëllimi i kësaj është të bëhet e vështirë për aktivitetet në internet që ato të gjurmohen deri te përdoruesi origjinal.

Linja (routing) mundësohet nga shtresa të shumëfishta të enkriptimit dhe pastaj përcillet trafiku përmes ritransmetuesve të shumtë dhe të zgjedhur rastësisht.

²⁴Për shembull, një organizatë mund të dëshirojë t'ua pamundësojë punonjësve t'i shikojnë disa uebsajte gjatë orëve të punës. Në raste të tilla, një proksi mund të konfigurohet në kompjuterët e punonjësve dhe kështu bllokohet qasja e drejtpërdrejtë në internet përmes një firewall. Të gjitha kërkesat për ueb duhet të kalojnë nëpër proksi dhe pastaj proksi është në gjendje të bllokojë ose të lejojë kërkesat sipas një politike të përcaktuar të organizatës.

Çdo relay dekripton një nivel të enkriptimit, që zbulon vetëm shtresën e radhës të ritransmetuesit dhe i kalon pjesën e mbetur të të dhënave të enkriptuara në të. Ritransmetuesi i fundit dekripton të dhënat e enkriptuara më të thella dhe i dërgon ato te destinacioni i synuar pa zbuluar ose pa u ditur, adresa e IP-së burimore. Rutingu i komunikimit është pjesërisht i fshehur nga çdo kërcim nga një segment në tjetrin në rrjetin Tor, do të thotë se nuk ka asnjë moment të vetëm kur shokët komunikues mund ta gjurmojnë në mënyrë që bazohet ose identifikohet me burimin dhe destinacionin e komunikimit.

Një përdorues i rrjetit Tor instalon një softuer special në kompjuterin e tij i cili do t'i përgjojë disa ose të gjitha trafikut e rrjetit dalës dhe t'i përcjellë ato te rrjeti Tor, në vend se t'i dërgojë drejtpërdrejt te destinacioni i synuar. Pasi që trafiku të jetë brenda rrjetit Tor, ai e dërgon atë nga një ruter në tjetrin derisa të arrihet ruteri i fundit në rrjet (ku bëhet dekriptimi i fundit dhe ku zbulohet trafiku origjinal). Ky ruter njihet si pika dalëse. Nga këndvështrimi i destinacionit, trafiku duket se buron nga pika dalëse.

Nga përshkrimi i mësipërm, mund të duket se rrjeti Tor lejon vetëm anonimizimin e komunikimit të inicuar nga klienti. Megjithatë, Tor po ashtu mbështet drejtimin e serverëve përmes rrjetit Tor në një mënyrë që adresa e IP-së nuk është e dukshme për përdoruesit e atij serveri. Për ta arritur këtë, adresa speciale u jepen serverëve, të njohura si adresa qepë, pastaj në to mund të ketë qasje përmes rrjetit Tor në mënyrë që nuk e tregon lokacionin e serverit²⁵. Një shërbim i fshehtë e reklamon ekzistencën e tij, pastaj rrjeti Tor i cakton "pikat e takimit" (rendeyvous points) në një mënyrë të decentralizuar që lejon konektimet mes shërbimeve të fshehta dhe përdoruesve pa e ditur identitetin e tjetrit.

Përderisa identifikimi i drejtpërdrejtë i adresës së IP-së së një të dyshimti që përdor rrjetin Tor është thuajse i pamundur, ekzistojnë teknika të specializuara për të identifikuar informata të tjera të cilat mund ta ndihmojnë hetimin. Për shembull, është e mundshme që një keqkonfigurim i serverit mund të zbulojë informacione rreth burimit të vërtetë të shërbimit të fshehtë. Faqet e gabuara (error) të gjeneruara nga shumë uebserversë të rëndomtë (p.sh., porositë e gabuara që i prezantohen një përdoruesi kurdo që kërkesa e tyre shkaktin një gabim) përfshijnë adresën e IP-së së serverit, do të thotë se duke krijuar një kusht gabimi në server mund të jetë e mundshme të zbulohet adresa e IP-së.

2.2.4 Botnets (Rrjeti i kompjuterëve të infektuar)/viruset/kontrolli nga largësia i një kompjuteri

Kur kompjuteri i një personi infektohet me një virus, është e mundshme që softueri të mund të instalohe në kompjuter që i mundëson një të dyshimti ta kontrollojë kompjuterin dhe përdorimin e tij për kryerjen e aktiviteteve kriminale. Mes mundësive të tjera, i dyshimti mund të instalojë një proksi në kompjuterin e komprometuar dhe ta përcjellë gjithë trafikun e tyre përmes këtij proksi.

²⁵Për më shumë hollësi rreth operimit të shërbimeve të fshehta vizitoni:
<https://www.torproject.org/docs/hidden-services.html>

Në këto raste, trafiku në internet që ndërlidhet me aktivitetin kriminal do të duket sikur vjen nga adresa e IP-së e një pale të pafajshme. Megjithatë, masat teknike janë të mundshme të cilat mund të mundësojnë identifikimin e burimit të vërtetë të trafikut. Për shembull, duke monitoruar trafikun e IP-së drejt dhe nga kompjuteri i komprometuar, mund të jetë e mundshme të identifikohet adresa e IP-së së të dyshimit që e kontrollon kompjuterin. Kjo më së shumti ka mundësi të ndodhë në rastet kur një kriminel ka komprometuar një numër të vogël të kompjuterëve dhe komunikon individualisht me ta.

Megjithatë, kompleksiteti i infrastrukturës së komandës dhe kontrollit (C&C) të cilët kriminelët e shfrytëzojnë për t'i operuar rrjetet e kompjuterëve të komprometuar (nganjëherë të njohur si botnetë) nuk duhet të nënvlerësohet. Shumë teknika përdoren nga operatorët e botnetit për të fshehur aktivitetin e tyre^{26,27} dhe për ta mundësuar trafikun e tyre të kontrollit të kalojë nëpër firewalls²⁸.

Analizat e kompjuterit personal të përdoruesit mund ta zbulojnë praninë e virusit, që e mbështesin supozimin se kompjuteri mund të jetë kontrolluar nga një palë e tretë nga largësia. Megjithatë, nuk mund të përjashtohet mundësia që një i dyshimtë mund ta infekttojë kompjuterin e vet me qëllim me ndonjë virus, me qëllim që të mbështetet gjatë mbrojtjes së tij se nuk ka qenë përgjegjës për veprimet e kryera në ose përmes kompjuterit të tij. Andaj, sfida e "vënies së të dyshimitit para testaturës" mund të kërkojë masa të tjera joteknike siç është vëzhgimi për ta përcaktuar me një shkallë të sigurisë se cili person i ka kryer cilat veprime, ose në mënyrë ekuivalente, për ta përjashtuar një person të caktuar si i dyshimtë se i ka kryer veprimet kriminale.

Hetuesit po ashtu përballen me sfidën që ka të bëjë me mënyrën për alarmimin e përdoruesit për infektimin dhe instrumentet e dhura që duhet të përdoren për ta larguar virusin. Momenti kur përdoruesit duhet të njoftohen për infektimin e kompjuterit të tyre është i rëndësishëm dhe duhet të vendoset varësisht nga statusi i hetimeve. Largimi i softuerit keqdashës nga pajisjet e infektuara duhet të bëhet në mënyrë që shmang qasjen e paligjshme ose përgjimin e komunikimit pa pëlqimin/autorizimin e duhur.

2.2.5 Shfrytëzimi i WiFi të hapura, publike ose të vjedhura

Rrjetet e hapura të WiFi janë të krijuara në mënyrë specifike për t'i mundësuar çdokujt që të lidhet me to dhe ta shfrytëzojë internetin. Rrjetet e hapura të WiFi paraqesin rrezik për përdorim kriminal të lidhjes së internetit në mënyrë që mund të jetë e pamundshme të lidhet aktiviteti i tyre me ndokënd tjetër përveç burimit të WiFi të hapur. Disa por jo të gjitha rrjetet e WiFi të hapura kërkojnë regjistrim dhe/ose i regjistrojnë kycjet.

Një problem i ngjashëm shfaqet në rastet kur është e mundshme që një sulmues ta qëllojë ose thyej fjalëkalimin e WiFi të një rrjeti të mbyllur të WiFi. Një skenar që është përmendur shpesh lidhur me shfrytëzimin e pikave të qasjes në WiFi të hakuar dhe/ose vjedhur është se një sulmues parkon veturën jashtë një ndërtese të zyrave dhe e shfrytëzon WiFi-në e tyre për ta kryer aktivitetin kriminal. Në raste të tilla, ka fare pak gjasa që mund të ketë ndonjë të dhënë identifikuese nga lidhja në rrjetin e WiFi (sidomos kur është fjala për bizneset e vogla), andaj nuk ka mënyrë për ta vazhduar hetimin për ta lokalizuar të dyshimin. Është e mundshme që një i dyshimtë të mund ta shfrytëzojë

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/

lokacionin e njëjtë në shumë raste, me ç'rast vëzhgimi i vendit mund të shpie te identifikimi i të dyshimitit.

Një problem i ndërlidhur shfaqet për faktin se ka shumë lokacione prej ku mund të ketë qasje në internet në një mënyrë relativisht anonime, siç janë bibliotekat, universitetet ose internet-kafetë.

Karakteristika përkufizuese e këtij problemi është mundësia që një i dyshimtë të ketë qasje thuajse krejtësisht anonime në internet përmes shfrytëzimit të lidhjeve të internetit dhe në disa raste, edhe të kompjuterëve, të cilët janë në pronësi të palës të tretë.

Ngjashëm me argumentin e bërë në fund të kapitullit paraprak, analiza e rrjetit të personit mund ta zbulojë praninë e një rrjeti të hapur të WiFi, që mbështet supozimin se WiFi mund të jetë përdorur nga një palë e tretë. Megjithatë, nuk mund të përjashtohet mundësia që një i dyshimtë mund ta lërë WiFi-në e vet hapur me paramendim, me qëllim që të mbështetet gjatë mbrojtjes së tij se nuk ka qenë përgjegjës për veprimet e kryera përmes WiFi-së. Sërish, mund të kërkohej masa të mëtejme jo-teknike siç është vëzhgimi për ta përcaktuar me një shkallë të sigurisë se cili person i ka kryer cilat veprime, ose në mënyrë ekuivalente, për ta përjashtuar një person të caktuar që t'i ketë kryer aktet kriminale.

Përgjimi i internetit është një teknikë tjetër e cila mund të shfrytëzohet për ta vërtetuar përfshirjen e individëve të ndryshëm në aktivitete kriminale.

2.2.6 Identifikimi i pronarit të një adrese të IP-së

WHOIS është një shërbim pa pagesë që ofron informata rreth pronarit të emrit të një domeni, përfshirë emrin, mbiemrin dhe referenca për kontaktin.

Sipas ICANN²⁹, administratori i emrit të domenit worldwide, "shërbimi WHOIS është pa pagesë, regjistër në dispozicion publik që përmban kontakte dhe informata teknike të regjistruarve të emrit të domeneve. Kushdo që dëshiron ta dijë se kush është prapa një emri të një domeni të uebsajtit mund ta bëjë një kërkesë për atë informatë përmes WHOIS.

Të dhënat mblidhen dhe vihen në dispozicion nga regjistrat dhe regjistruarit sipas kushteve të marrëveshjes me ICANN. WHOIS nuk është një bazë e vetme e të dhënave e menaxhuar nga qendra. Aty më tepër mbahen të dhënat në lokacione të shpërndara dhe administrohen nga regjistrat dhe regjistruarit të shumfishtë. Ata i caktojnë vetë konventat e tyre për shërbimin WHOIS, që është në përputhje me kriteret minimale të përcaktuara në kontratat e tyre me ICANN".

WHOIS përdoret për të gjetur se kujt i është caktuar një adresë e IP-së. Problemi është se informatat nga baza e të dhënave WHOIS nuk është gjithmonë e saktë. Regjistruarit u kërkohej që në baza periodike të komunikojnë me ata që janë regjistruar me ta por ata nuk kanë ndonjë përgjegjësi për ta vërtetuar saktësinë e të dhënave që të regjistruarit i ofrojnë. Ky është problem sidomos gjatë përpjekjes për ta identifikuar se kush është pronari i një emri të caktuar të një domeni.

²⁹Korporata e internetit për caktimin e emrave dhe numrave, organizata ndërkombëtare përgjegjëse për përcaktimin e politikave dhe kontratave të ndërlidhura me regjistrat dhe regjistruarit.

Në rastin e adresave të IP-së, është identifikuar edhe një problem tjetër sistematik, që është nën-ndarja e adresave të IP-së.³⁰ Problemi shfaqet nëse një ofrues, të cilit i janë caktuar një varg të adresave të IP-së, pastaj i cakton disa nga këto adresa të IP-së te një nën-ofrues por nuk mban informata të sakta ose të përditësuara se kush është duke i shfrytëzuar ato adresa të IP-së. Veçanërisht, provajderi mund të mos i raportojë gjithmonë këtë nën-caktim te regjistri i bazës së të dhënave WHOIS, që do të thotë se baza e të dhënave WHOIS nuk do të përmbajë informata të sakta rreth kontrolluesit të fundit të adresës së IP-së në fjalë.

Të dhënat nga WHOIS mund të konsiderohen si një formë specifike e të dhënave rreth informatave të abonuesit, të cilat janë në dispozicion publik në internet me qasje të pakufishme. Megjithatë, me hyrjen në fuqi të Rregullores së BE-së për Mbrojtjen e Përgjithshme të të Dhënave (GDPR) më 25 maj 2018, qasja në WHOIS do të ndryshojë për ta siguruar përputhshmërinë me GDPR.³¹

PYETJE PËR VETËREFLEKTIM

1. A mundet një urdhër për monitorim të adresës së IP-së të formulohet në atë mënyrë që nuk i prek të drejtat e palëve të treta të pafajshme?
2. Si të jetë e mundshme të vërtetohet nëse aktiviteti që lidhet me një adresë të caktuar të IP-së është kryer nga mbajtësi i asaj adrese të IP-së apo nga lart, për faktin se kompjuteri i tyre ka qenë i infektuar me softuerin dashakeq?
3. Cilat kushte duhet të përmbushen për ta siguruar një urdhër i cili do ta mundësonte identifikimin e adresës së IP-së në përdorim nga një i dyshimtë i botës reale?
4. Cilat kushte duhet të përmbushen që të sigurohet një urdhër i cili do ta mundësonte identifikimin e një mbajtësi real të një adrese të IP-së që është i përfshirë në aktivitet kriminal?

2.3 Angazhimi me ISPs

2.3.1 Lloji i të dhënave të kërkuara

Për qëllime të hetimit penal, mund të ketë nevojë për tri lloje të dhënash:

- Informata për abonuesin
- Të dhëna për trafikun
- Të dhëna për përmbajtjen

Në shumë juridiksione, kriteret për qasje në informata për abonuesin janë të prira të jenë më të ulëta se për të dhënat për trafikun dhe regjimi më i rreptë aplikohet për të dhënat për përmbajtjen. Ky lloj i të dhënave që kërkohen qartazi do të ndikojnë në natyrën e kërkesës që ka nevojë t'i bëhet një provajderi të shërbimeve shumëkombëshe me qëllim që të sigurohet qasja në të dhëna. Disa provajderë të shërbimeve shumëkombëshe, por jo

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

³¹ Për informata të mëtejme rreth qasjes në WHOIS shih: <https://www.icann.org/news/blog/data-protection-privacy-update-seeking-input-on-proposed-interim-model-for-gdpr-compliance>

të gjitha, kanë një formë të bashkëpunimit vullnetar të përshpejtuar përmes të cilit mund të sigurohen informatat për abonuesin, në pritje të pranimit të procesit zyrtar ligjor.

2.3.1.1 Informata për abonuesin

Informata për abonuesin është informata më së shpeshti e kërkuar në hetimet vendore dhe penale dhe, pa këtë informatë, është shpesh e pamundur të vazhdohet hetimit³². Termi informata për abonuesin përkufizohet në Nenin 18,3 të Konventës së Budapestit si:

"Për qëllime të këtij neni, termi "informata për abonuesin" nënkupton çdo informatë që mbahet në formë të të dhënave kompjuterike ose çfarëdo forme tjetër nga një provajder i shërbimit, që lidhet me abonuesin e shërbimeve të tyre, me përjashtim të të dhënave për trafikun dhe përmbajtjen dhe përmes të cilave mund të vërtetohet:

- a. Lloji i shërbimit të komunikimit të përdorur, dispozitat teknike të marra atje dhe periudha e shërbimit;*
- b. Identiteti i abonuesit, adresa postale ose gjeografike, numri i telefonit dhe qasja tjetër, informata rreth faturimit dhe pagesës, që sigurohen në bazë të marrëveshjes ose aranzhimit për shërbim;*
- c. Çdo informatë tjetër rreth vendit të instalimit të pajisjeve të komunikimit, që sigurohen në bazë të marrëveshjes ose aranzhimit të shërbimit."*

Informatat për abonuesin ka mundësi të mbahen nga provajderët e shërbimit ndonëse informatat mund të jenë të ruajtura në serverë që ndodhen në juridiksione të tjera. Kështu që mund të mos jetë gjithmonë e qartë kujt t'i adresohet një kërkesë për informata për abonuesin.

2.3.1.2 Të dhënat për trafikun

Dosjet e regjistrimit që shënojnë aktivitetet e sistemit operativ të një kompjuteri ose të softuerit tjetër ose të komunikimit mes kompjuterëve janë jetike për rastet e krimeve kibernetike dhe mund të jenë po aq të rëndësishme në rastet që kanë të bëjnë me të ardhurat nga krimi kibernetik. Termi "të dhënat për trafikun" përkufizohet në Nenin 1.d të Konventës së Budapestit si:

"Të dhënat për trafikun nënkuptojnë të dhënat kompjuterike të një komunikimi përmes një sistemi kompjuterik, të gjeneruar nga një sistem kompjuterik që ka formuar një pjesë të zinxhirit të komunikimit, që tregon origjinën e komunikimit, destinacionin, rrugën, kohën, datën, madhësinë, kohëzgjatjen, ose lloje të shërbimeve të tjera themelore"

2.3.1.3 Të dhëna për përmbajtjen

Në fund edhe të dhënat për përmbajtjen kërkojnë shpesh në hetime penale. Sipas paragrafit 209 të Raportit Shpjegues të Konventës së Budapestit:

"Të dhëna për përmbajtjen nuk janë të përkufizuara në Konventë por i referohen përmbajtjes së komunikimit; do të thotë kuptimit ose domethënies së komunikimit, ose porosisë ose informatës që bartet përmes komunikimit (përveç të dhënave për trafikun)."

³² Raporti T-CY për rregullat e sigurimit të informatave për abonuesin të miratuar më takimin e 12-të plenar të datës 2-3 dhjetor 2014. Gjendet në: <https://rm.coe.int/16802e7ad1>

Po ashtu duhet të bëhet dallim mes të dhënave për përmbajtjen "e ruajtur" që veçse ndodhet në një sistem kompjuterik dhe të dhënave për përmbajtjen e "ardhshme" të cilat ende nuk janë në dispozicion dhe të cilat kanë nevojë të mbliidhen, për shembull, përmes përgjimit të komunikimit. Përgjimet mund të kryhen me urdhër të gjykatës ose nga policia ose nga një grup i specializuar në mënyrë të drejtpërdrejtë ose me ndihmën e ndonjë provajderi të shërbimeve. Përdorimi i tyre shpesh kufizohet vetëm brenda krimeve të rënda.

2.3.2 Direktiva e BE-së për ruajtje të të dhënave është shpallur e pavlefshme me vendim të CJEU

Siç u përshkrua më lart, identifikimi i kryerësve në botën kibernetike shpesh varet nga qasja në të dhënat e mbajtura nga provajderët privatë të shërbimit të internetit. Lidhja e një adresë të IP-së me një person (abonues të adresës së IP-së, email ose llogari në Facebook) dhe bashkëveprimi i të dyshimit me të dyshimtët e tjerë të mundshëm (të dhënat për trafikun) madje edhe përmbajtja e atij veprimi janë një pjesë jetike për ta zbuluar keqbërësin, të dyshimtët e tjerë dhe për t'i siguruar provat e një krimi.

E tërë kjo është e mundshme vetëm nëse kompania private i ruan të dhënat e nevojshme (të dhënat për abonuesin, të dhënat për trafikun dhe/ose të dhëna për përmbajtjen). Obligimi ligjor për të ruajtur të dhënat për qëllime të zbatimit të ligjit është sfiduar para Gjykatës së Drejtësisë së Bashkimit Evropian (CJEU)³³. Në vendimin e tij në Rastet e Bashkuara C -93/12 dhe C - 594/12 (Të drejtat digjitale Irlanda dhe Seitlinger dhe të tjerët) Direktiva për Ruajtjen e të Dhënave 2006/24/EC³⁴ është shpallur e pavlefshme. Ky vendim ka shpënë te anulimi i legjislacionit relevant shtetëror në disa vende të BE-së, ku ka ekzistuar obligimi për provajderët që të ruajnë të dhënat për trafikun për një periudhë që sillet nga 6 muaj në 2 vjet.

Si rrjedhojë ISP-të nuk janë më të obliguara të ruajnë (mbajnë) të dhënat për trafikun për qëllime të hetimeve të krimeve të rënda për një periudhë kohore që më herët parashihej me legjislacionin shtetëror, por ato i ruajnë të dhënat vetëm për periudhën që është e nevojshme për faturim ose për përdorime të tjera komerciale. Në praktikë, kjo do të thotë rreth 1-3 muaj. BE-ja ende nuk e ka miratuar ndonjë instrument të ri ligjor dhe shumë shtete ende janë në proces të përkufizimit të zgjidhjeve të përshtatshme ligjore për t'i adresuar shqetësimet ligjore. Megjithatë, në dukje është veçanërisht sfiduese të adresohen pritjet e gjykatës për të shmangur mbulimin e përgjithshëm të të gjithë personave, të gjitha mjeteve të komunikimit elektronik dhe të gjitha të dhënave të trafikut pa kurrfarë dallimi, kufizimi ose përjashtimi në emër të qëllimit për t'i luftuar krimet e rënda.

Një nga qasjet e mundshme do të mund të ishte rregullimi i nxjerrjes së urdhrat për ruajtje të të dhënave (për trafikun) pasi të jetë bërë kërkesa juridike për një periudhë të kufizuar kohore.

Pasi që arsyet për këtë zbulje u bazuan në pikëpamjet e gjykatës se direktiva i tejkalonte kufijtë e parimeve të proporcionalitetit, pasi që ajo ndërhynte në mënyrë të rëndë në të drejtat themelore për respektim të jetës private dhe për mbrojtje të të dhënave personale,

³³ Aktgjykimi i Gjykatës për Drejtësi të Bashkimit Evropian në rastet e bashkuara C-293/12 dhe C-594/12. Të drejtat digjitale Irlanda dhe Seitlinger dhe të tjerët. Gjendet në: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>

³⁴ Direktiva 2006/24/EC e datës 15 mars 2006 për ruajtjen të të dhënave të gjeneruara ose të procesuara në lidhje me ofrimin e shërbimeve të komunikimit elektronik në dispozicion publik ose të rrjeteve të komunikimeve publike dhe ndryshimi i Direktivës 2002/58/EC. (E shfuqizuar)

ky vendim mund të ketë ndikim edhe në shtetet joanëtare të BE-së, sidomos nëse legjislacioni shtetëror sfidohet në gjykatat kushtetuese të vendeve ose në raste të ankesave individuale në Gjykatën Evropiane të të Drejtave të Njeriut për shkelje të Nenit 8 të Konventës për të Drejtat e Njeriut.

Andaj, thekset kryesore të vendimit të gjykatës mund të jenë me rëndësi për ligjbërësit shtetërorë. Gjykata ka gjetur se direktiva ndërhyr në mënyrë të rëndë në të drejtat themelore të respektimit të jetës private dhe të mbrojtjes së të dhënave personale. Po ashtu ka të ngjarë të shkaktojë te njerëzit në fjalë përshtypjen se jetët e tyre private janë nën vëzhgim të përhershëm.

Gjykata vuri në pah se direktiva nuk e rregullon përmbajtjen e komunikimeve dhe se ruajtja e të dhënave për qëllime të dërgimit të tyre të autoritetet kompetente të shtetit në thelb e përmbush një qëllim në shërbim të interesit të përgjithshëm, respektivisht luftës kundër krimeve të rënda dhe si rrjedhojë edhe të sigurisë publike. Megjithatë, organet ligjvënëse i kanë tejkaluar kufijtë e caktuar nga respektimi i parimit të proporcionalitetit, duke theksuar se rishikimi i diskrecionit të ligjvënësit duhet të jetë i rreptë.

Ndonëse ruajtja e të dhënave të kërkuara nga direktiva mund të konsiderohet si gjëja e duhur për ta ndjekur qëllimin e vënë prej saj, shtrirja e gjerë e sidomos ndërhyrja e rëndë e direktivës në të drejtat themelore të respektimit të jetës private dhe mbrojtjes së të dhënave personale ka tejkaluar kufijtë e caktuar nga respektimi i parimit të proporcionalitetit, si:

- Shtrirja e saj nuk ishte e kufizuar mjaftueshëm për t'u siguruar që ndërhyrja të kufizohej vetëm brenda asaj që është e domosdoshme,
- Ajo mbulon, në mënyrë të përgjithësuar, të gjithë personat, të gjitha mjetet e komunikimit elektronik dhe të gjitha të dhënat e trafikut pa kurrfarë dallimi, kufizimi ose përjashtimi në emër të qëllimit për t'i luftuar krimet e rënda.
- Nuk ekzistojnë kritere objektive për autoritetet kompetente të shtetit për të pasur qasje në të dhëna andaj mund t'i përdorin ato vetëm për qëllime të parandalimit, zbulimit ose ndjekjes penale të veprave të cilat mund të konsiderohen të jenë aq të rënda sa për ta arsyetuar një ndërhyrje të tillë. Ajo thjesht u referohet 'krimeve të rënda',
- Qasja në të dhëna nuk është lënë të varet nga shqyrtimi paraprak nga një gjykatë ose nga një organ i pavarur administrativ,
- Ajo imponon një periudhë ruajtjeje prej gjashtë muajsh, pa bërë kurrfarë dallimi mes kategorive të të dhënave në bazë të personave në fjalë ose të dobisë së mundshme të të dhënave.
- Periudha caktohet mes një minimumi prej gjashtë muajsh dhe një maksimumi prej 24 muajsh, por nuk ka kritere objektive në bazë të të cilave do të caktohej periudha e kufizuar e ruajtjes brenda asaj që është vërtet e domosdoshme,
- Asaj i mungon kujdesi i mjaftueshëm për të siguruar mbrojtjen efektive të të dhënave nga rreziku i keqpërdorimit,
- Ajo nuk sigurohet për shkatërrimin e pakthyeshëm të të dhënave në fund të periudhës së ruajtjes së tyre.

Për literaturë të mëtejme rreth ndikimit të vendimit, Franziska Boehm dhe Mark D. Cole kanë theksuar disa aspekte të rëndësishme në artikullin e tyre për Ruajtjen e të Dhënave pas Aktgjykimit nga Gjykata e Drejtësisë e Bashkimit Evropian nga data 30 qershor

2014³⁵. Ata kanë theksuar se deklaratimet e Gjykatës jo vetëm që i referohen një rasti të veçantë të Direktivës, por po ashtu i përcaktojnë parimet e përgjithshme për masa të ngjashme për ruajtje të të dhënave. Këto parime mbulojnë pikat në vazhdim:

- Mbledhja, ruajtja dhe transferi i të dhënave secila përbëjnë shkelje të Neneve 7 dhe 8 dhe parashihet që kjo të bëhet vetëm në raste tejet të domosdoshme dhe me një test të proporcionalitetit.
- Gjykata qartazi refuzon ruajtjen e të dhënave të përgjithshme të personave që nuk janë të dyshimtë si dhe periudhën e gjatë dhe të paafatshme të ruajtjes së të dhënave.
- Gjykata i konsideron si problem të ndjeshëm të dhënat të cilat në fillim mbledhen për qëllime të tjera e më vonë përdoren për qëllime të zbatimit të ligjit. Ajo kërkon një lidhje mes kërcënimit ndaj sigurisë publike dhe të dhënave që ruhen për ato qëllime.
- Kjo lidhje e kërkuar ndikon me të madhe në raportet mes akterëve privatë dhe publikë. Organet e rendit lejohen të kenë qasje vetëm në të dhënat e mbledhura për qëllime të tjera në raste të caktuara.
- Gjykata në mënyrë eksplicite kërkon rregulla efektive procedurale siç janë mbikëqyrja e pavarur dhe kontrolli i qasjes.
- Mbledhja dhe shfrytëzimi i të dhënave për qëllime të zbatimit të ligjit përmbajnë në vete rrezikun e stigmatizimit që del nga përfshirja e të dhënave në bazat e të dhënave të organeve të rendit. Ky rrezik duhet të merret në konsideratë kur të rishikohen masat e tjera ekzistuese ose të planifikuara për ruajtje të të dhënave në nivel të organeve të rendit dhe Shteteve Anëtare.

Me qëllim që të adresohen problemet e ngritura nga aktvendimi nga CJEU, më 29 nëntor 2016, MB miratoi aktin për kompetencat hetuese 2016. Mes teknikave të tjera të rëndësishme, ajo përcakton edhe obligimin ndaj ISP-ve që të ruajnë 'të dhënat rreth konektimit' për 12 muaj. Kjo është një formë e ndërhyrjes më të vogël sesa regjistrimi i të gjitha të dhënave të shfletimeve dhe është e dizajnuar për të akomoduar shqetësimet e CJEU rreth ndërhyrjes disproporcionale. Ajo po ashtu krijon kompetenca të reja që mundësojnë, në bazë të urdhrit të gjykatës, monitorimin dhe mbajtjen e shfletimeve nga i dyshimti, etj.

2.3.3 ISP-të kombëtare

Të dhënat të cilat mbahen nga Provajderët e Shërbimit të Internetit (ISP) janë të rëndësishme për identifikimin e keqbërësve dhe bashkëpunëtorëve të tyre, lidhjeve të tyre në kohë dhe hapësirë dhe për provat rreth përmbajtjes së komunikimit (përmbajtjes së emailit, postimeve në platforma sociale, siç është Facebook).

Obligimet e ISP-ve rregullohen me dispozita shtetërore për ruajtjen e të dhënave (për trafikun) dhe për kriteret për qasjen dhe përdorimin e këtyre të dhënave për qëllime të hetimeve penale. Të dhënat mund të kategorizohen si të dhëna për abonuesin, të dhëna për trafikun dhe të dhëna për përmbajtjen.

³⁵Ruajtja e të Dhënave pas Aktgjykimit nga Gjykata e Drejtësisë e Bashkimit Evropian, Prof. Dr. Franziska Boehm et al., Munster/Luxembourg, 30 qershor 2014. Gjetet në: http://www.janlabrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf

Të dhënat për abonuesin konsiderohen si më pak të ndjeshme për privatësinë dhe më pak ndërhyrëse se të dhënat për trafikun dhe të dhëna për përmbajtjen. Këto janë të dhënat që kërkohen më së shpeshti në hetimet vendore dhe ndërkombëtare të hetimeve penale që kanë të bëjnë me krime kibernetike dhe prova elektronike. Pa këto informata, shpesh është e pamundshme të vazhdohet me një hetim.

Të dhënat për abonuesin zakonisht mbahen nga ISP private dhe mund të sigurohen nga policia ose prokuroria në bazë të urdhrit të siguruar. Megjithatë, në raste të adresave dinamike të IP-ve, shumë shtete kërkojnë të ketë urdhër të gjykatës, pasi që disa të dhënat për trafikun janë të përfshira. Në shumicën e shteteve kërkohet urdhër i gjykatës për: qasje në të dhënat për trafikun (për çështjen e mbajtjes së të dhënave shih kapitullin paraprak); për urdhër për ruajtje (ruajtjen e të dhënave për trafikun në të ardhmen); për të dhënat për trafikun dhe; për qasje në të dhëna për përmbajtjen e në veçanti për përgjimin e komunikimeve (këto të fundit zakonisht konsiderohen si më ndërhyrëset, andaj u nënshtrohen disa mbrojtjeve, kushteve dhe parimeve më specifike të proporcionalitetit).

Përveç kërkesave ligjore, janë të rëndësishme edhe aranzhimet teknike dhe praktike të transferit të të dhënave mes ISP-ve dhe autoriteteve të rendit, e sidomos në raste të monitorimit të drejtpërdrejtë dhe transmetimit të të dhënave, që mundësojnë përpunimin e shpejtë të të dhënave.

Një fushë tjetër e bashkëpunimit mes autoriteteve të organeve të rendit dhe ISP-ve është çështja e bllokimit dhe mbylljes së faqeve të internetit në raste të veprave penale ose përmbajtjes kriminale. Materialet e pornografisë së fëmijëve përmenden më së shpeshti në këtë kontekst, por edhe format e tjera mund të jenë të rëndësishme, siç janë gjuha e urrejtjes dhe provokimet publike për të kryer vepra terroriste ose shkelje të të drejtave të pronës intelektuale. Ndonëse zakonisht kërkohet një urdhër i gjykatës për masa të tilla, veprimi "vullnetar" i pronarit ose redaktorit të faqes së internetit është duke u promovuar, për arsye të shkeljes së kodit të brendshëm të sjelljes. Ndonëse një qasje e tillë mund të jetë më efikasja, sidomos në raste të shkeljeve prima facie (siç janë materialet pornografike), kjo mund të ngritë disa shqetësime rreth ndërhyrjes së mundshme në lirinë e shprehjes, siç është identifikuar në Studimin e Këshillit të Evropës për filtrimin, bllokimin dhe mbylljen e përmbajtjes së paligjshme në internet në vitin 2016³⁶.

PYETJE PËR VETËREFLEKTIM

1. Çka nënkuptohet me termin "informata për abonuesin"?
2. Çka nënkuptohet me termin "të dhëna për trafikun"?
3. Çka nënkuptohet me termin "të dhëna për përmbajtjen"?
4. Cilat janë implikimet e vendimit nga CJEU për ruajtjen e të dhënave për identifikim të një të dyshimti nga bota reale sipas adresës së IP-së që lidhet me aktivitetin penal?

³⁶Studimi i Këshillit të Evropës për filtrimin, bllokimin dhe mbylljen e përmbajtjes së paligjshme në internet, qershor 2016. Gjetet në: <https://www.coe.int/en/web/cybercrime/-/study-on-filtering-blocking-and-take-down-of-illegal-content-on-the-internet>

2.4 Provajderët e Shërbimeve Shumëkombëshe

Në rastet që kanë të bëjnë me të ardhura nga krimet kibernetike, prova vendimtare mbahen nga organizatat e sektorit privat si Facebook, Google, Microsoft, Twitter, Yahoo! e të tjera. Andaj bashkëpunimi mes autoriteteve kompetente dhe këtyre provajderëve të shërbimeve shumëkombëshe është kyç për të siguruar prova elektronike. Nuk është e mundshme që në një doracak si ky të jepen informata për të gjithë provajderët e ndryshëm të shërbimeve shumëkombëshe për të cilat një lexues i mundshëm mund ketë nevojë; detaje rreth procesit si një provajder i caktuar i shërbimit i trajton kërkesat nga organet e rendit zakonisht mund të gjenden në uebsajtet e tyre. Andaj janë bërë përpjekje për t'i kategorizuar aspektet kyçe të politikave të zbatimit të ligjit për provajderët e shërbimeve shumëkombëshe.

Qëllimi është që të sigurohet një kornizë brenda së cilës të shqyrtohet angazhimi me një provajder të një shërbimi të caktuar në të ardhmen. Së dyti, kjo po ashtu do të ndihmonte në qartësimin e faktorëve të cilët provajderët e shërbimeve shumëkombëshe do t'i marrin në konsideratë kur t'i shqyrtojnë kërkesat e ardhura nga organet e rendit, e kështu edhe faktorët të cilët duhet të merren në konsideratë kur të formulohet një kërkesë e tillë për një provajder të shërbimeve me qëllim që të maksimalizohet mundësia për një rezultat të suksesshëm.

Cloud Evidence Group - CEG (Grupi i Provave Hije) kanë përgatitur një dokument gjithëpërfshirës për çështjen e qasjes nga organet e rendit në të dhënat e mbajtura nga provajderët e shërbimeve shumëkombëshe³⁷. Shumë aspekte interesante do të shtjellohen më në hollësi në Kapitullin **Error! Reference source not found..** Për t'i theksuar disa prej tyre:

- CEG ka ardhur në përfundim se ndihma e ndërsjellë juridike mbetet mjeti kryesor për të sigurua prova elektronike nga juridiksionet e huaja për shfrytëzim të tyre në procedurat penale vendore. Kjo është veçanërisht e vërtetë për të dhëna për përmbajtjen.
- Qasja në të dhënat për abonuesin janë më pak ndërhyrëse dhe duhet të lehtësohet. Neni 18 për sigurimin e urdhrit vendor duhet të shfrytëzohet edhe për ISP-të shumëkombëshe që veprojnë në territorin e një shteti - një Udhërrëfyes draft nr. 10 sigurimin e urdhreve për informata të abonuesve është përgatitur.
- Bashkëpunimi i drejtpërdrejtë i ISP-ve nga SHBA-të me autoritetet e huaja të rendit janë pranuar duke marrë në konsideratë po ashtu edhe rritjen e kërkesave për ndihmë juridike të ndërsjellë.
- CEG ka propozuar hartimin e protokolleve shtesë me qëllim që të adresohen disa nga sfidat ekzistuese, respektivisht lehtësimi i regjimit të qasjes në të dhëna për abonuesit dhe për të mundësuar kërkesat e drejtpërdrejta te ISP-të në kushte të caktuara.

2.4.1 Juridiksioni

Shpesh nuk është e qartë për një autoritet të drejtësisë penale se në cilin juridiksion ruhen të dhënat e kërkuara dhe/ose cili regjim ligjor vlen për ato të dhëna³⁸. Një provajder i

³⁷ T-CY (2016)5, Qasja e drejtësisë penale në prova elektronike në internet (cloud): Rekomandime për t'u marrë në konsideratë nga T-CY, Raporti Përfundimtar, 16 shtator 2016. Gjendet në: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>

³⁸ Dokument për diskutime i përgatitur nga T-CY Cloud Evidence Group, Qasja e drejtësisë penale në të dhënat në internet: sfidat, maj 2015. Gjendet në:

shërbimit mund ta ketë selinë në një juridiksion dhe ta zbatojë regjimin ligjor të një juridiksioni tjetër ndërsa të dhënat të jenë të ruajtur në një juridiksion të tretë. Lokacioni i të dhënave përcakton edhe juridiksionin, po ashtu është e mundshme që provajderi i shërbimit nuk mund ta dijë lehtë lokacionin e të dhënave. Madje edhe nëse dihet lokacioni i të dhënave, nuk është e sigurt se cilat rregulla vlejnë për qasje të ligjshme nga autoritetet e drejtësisë penale. Mund të ketë mospajtime nëse lokacioni i selisë së provajderit të shërbimit, ose degës së tyre, ose lokacioni i të dhënave ose ligji i shtetit ku i dyshimti ka abonuar shërbimin, ose lokacioni ose shtetësia e të dyshimit, mund të përcaktojnë edhe juridiksionin.³⁹

2.4.2 Qëndrimi i përgjithshëm

Në të gjitha rastet (me përjashtim të kërkesave emergjente, të diskutuara më poshtë), procesi i Ndihmës së Ndërsjellë Juridike duhet të respektohet me qëllim që të sigurohet qasja në të dhënat për përmbajtjen.

Përkitazi me të dhënat për abonuesit, ISP-të shumëkombëshe kryesisht ndahen në dy kategori; ato të cilat përgjigjen në kërkesat ligjore nga juridiksionet jashtë Shteteve të Bashkuara dhe ato të cilat kërkojnë një kërkesë për ta nënshkruar një traktat për Ndihmë të Ndërsjellë Juridike që duhet t'u dorëzohet atyre nga një gjykatë në Shtete të Bashkuara.

2.4.3 Kërkesat për ruajtje

Disa provajderë të shërbimeve pranojnë kërkesat për ruajtje dhe në bazë të tyre do të ruajnë të dhënat për një periudhë kohore (zakonisht për një periudhë prej 90 ditësh) në pritje të dokumentacionit ligjor zyrtar. Nëse kërkohet ruajtja për më shumë se 90 ditë, duhet t'i dërgohet një letër për vazhdim provajderit të shërbimit para përfundimit të periudhës prej 90 ditësh.

2.4.4 Kërkesat emergjente

Në rastet të cilat përmbajnë rrezik të menjëhershëm për dëme, vdekje ose lëndime të rënda fizike, shumica e provajderëve të shërbimeve shumëkombëshe bashkëpunojnë me kërkesat për informata nga organet e rendit në rastet kur mund të dëshmohet se provajderi i shërbimit ka informata të cilat mund të jenë të nevojshme për ta parandaluar dëmin, vdekjen ose lëndimin e rëndë fizik. Një sfidë praktike në këtë drejtim, e cila theksohet në vende të tjera të këtij kursi⁴⁰, është se shumë shtete nuk kanë legjislacion të miratuar që lejon zbulimin e të dhënave për autoritetet vendore të drejtësisë penale në raste emergjente. Veçanërisht, SHBA-të e kanë një dispozitë të atillë që ua lejon provajderëve të shërbimeve shumëkombëshe me seli në SHBA për t'u përgjigjur në kërkesa emergjente, por në rastet kur provajderi i shërbimit nuk e ka selinë në SHBA, ose një numër i vogël i shteteve të tjera, baza ligjore për zbulim mund të paraqesë një sfidë tjetër praktike.

2.4.5 Shtrirja e kërkesës

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

³⁹ T-CY (2016)5, Qasja e drejtësisë penale në prova elektronike në internet (cloud): Rekomandime për t'u marrë në konsideratë nga T-CY, Raporti Përfundimtar, 16 shtator 2016. Gjetet në:

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

⁴⁰ Shih Kapitullin 4.2.2.2.2

Shumica e provajderëve të shërbimeve shumëkombëshe do t'i refuzojnë kërkesat për informata të cilat janë shumë të gjera në shtrirjen e tyre. Një përkufizim i fushëveprimit të pranueshëm zakonisht nuk jepet, me përjashtim të deklaramit se "kërkesat shumë të gjera ose të paqarta nuk do të përpunohen". Andaj, për t'i siguruar gjasat më të mira për një përgjigje të suksesshme, kërkesat duhet të formulohen me një shtrirje sa më të ngushtë dhe t'u referohen, kurdo që është e mundshme, llogarive të personave me çfarëdo identifikuesi unik që është përdorur në platformën specifike në fjalë.

Mund të mos jetë përherë e qartë se çfarë identifikuesi unik është në përdorim në një platformë të caktuar. Në shumicën e rasteve, por jo gjithmonë, mjaftojnë emri i përdoruesit dhe/ose adresa e emailit që kanë të bëjnë menjë llogari të caktuar.

2.4.6 Njoftimi i subjektit të kërkesës

Në shumë raste, kur pranohet një kërkesë nga një organ i rendit në lidhje me një përdorues të një provajderi të shërbimeve shumëkombëshe, është politikë e provajderit të shërbimit që ta informojë subjektin e kërkesës rreth ekzistencës së kërkesës. Kjo do të bëhet përveç rasteve kur njoftimi parandalohet me ligj ose me urdhër të gjykatës.

Andaj, nëse njoftimi i subjektit mund ta komprometojë hetimin, urdhri që përbën bazën për kërkesë të informatës nga provajderi i shërbimit duhet ta përfshijë edhe ndalimin e informimit të subjektit të kërkesës.

Veç kësaj, disa provajderë të shërbimeve tregojnë se nëse një kërkesë nga një organ i zbatimit të ligjit ua tërheqë vëmendjen për një shkelje të kushteve të tyre të shërbimit, mund të merren masa për ta parandaluar keqpërdorimin e mëtejshëm, përfshirë veprime të cilat mund ta njoftojnë përdoruesin se provajderi i shërbimit është në dijeni për këtë sjellje.

PYETJE PËR VETËREFLEKTIM

- 1. Pse është e rëndësishme që të urdhërohet ndaras një provajder i shërbimit për t'i ruajtur të dhënat që kërkohen në një procedurë penale, në pritje të pranimit të dokumenteve zyrtare për zbulim të provave?**
- 2. Cilat kushte duhet të plotësohen para se një urdhër për një provajder të një shërbimi që e detyron zbulimin e informatave rreth një përdoruesi të atij provajderi të shërbimit të përfshijë një dispozitë për t'ia parandaluar provajderit të shërbimit që ta njoftojë (në mënyrë të drejtpërdrejtë ose të tërthortë) subjektin e kërkesës?**
- 3. Çfarë opsionesh ka në dispozicion në një skenar ku një llogari e një provajderi të një shërbimi shumëkombësh është e njohur se ka lidhje me aktivitete penale në juridiksionin tuaj, por nuk është e mundshme të dihet, pa siguruar informata nga provajderi i shërbimit, nëse mbajtësi i asaj llogarie është ose nuk është i pranishëm në juridiksionin tuaj?**
- 4. Duke marrë parasysh vonesat që shoqërojnë procesin e Ndihmës së Ndërsjellë Juridike, çfarë opsionesh (nëse ka) ekzistojnë për ta përsheptuar qasjen në të dhëna për përmbajtjen që mbahen nga një provajder i shërbimeve shumëkombëshe?**

3 Hetimet financiare

3.1 Hyrje

Koncepti i shënjestrimit të të ardhurave nga krimet kibernetike bashkon qasjet e hetimeve të krimit kibernetik, hetimeve financiare dhe hetimet e pastrimit të parave me qëllim që të rritet efikasiteti dhe suksesi i hetimeve penale dhe i procedurave penale si nga këndvështrimi i ndjekjes së kriminelëve dhe ashtu edhe i luftimit dhe konfiskimit të të ardhurave nga krimi.

Doracaku i kursit bazik përmban shpjegime elementare dhe të hollësishme të hetimeve financiare, përfshirë përkufizimin e fushëveprimit dhe elementeve të tyre. Përkufizimi i hetimeve financiare dhe i elementeve të tyre dhe disa specifikave që lidhen me krimet kibernetike, përfshirë hetimin e krimeve kibernetike do të adresohen shkurtimisht dhe do të jepen disa hollësi më shumë rreth zhvillimeve të fundit rreth konceptit të hetimeve financiare në BE.

3.2 Hetimet financiare dhe të ardhurat nga krimi kibernetik

Hetimet financiare mund të kenë disa kuptime, që sillen nga hetimi i krimeve financiare deri te, për shembull, hetimi për qëllime tatimore. Instrumentet ligjore ndërkombëtare nuk ofrojnë një përkufizim të hetimit financiar, por brenda kornizës së ngrirjes dhe konfiskimit të të ardhurave nga krimi, mund të shfrytëzohet si shembull përkufizimi përshkruar nga Taskforca për Veprim Financiar (FATF).

Po ashtu duhet të theksohet se termi hetim financiar mund të përfshijë si hetimin e ndjekjes së të ardhurave nga krimi brenda kornizës së procedurës penale, ashtu edhe në procedurën (e veçuar) civile (in rem). Duhet të theksohet se hetimi financiar, mundet por jo doemos, të përkojë me hetimin e pastrimit të parave.

Hetimi financiar është një metodë hetuese dhe duhet të kryhet në mënyrë paralele me hetimin penal të një krimi profitabil madje edhe gjatë fazës gjyqësore me qëllimin kryesor (por jë të vetëm) të gjurmimit dhe ngrirjes së të ardhurave nga krimi me qëllim të konfiskimit të tyre përfundimtar.

FATF e ka kufizuar hetimin financiar⁴¹ si hetim të çështjeve financiare që ndërlidhen me një aktivitet kriminal, me qëllim që:

- Identifikimit të shkallës së rrjeteve kriminale ose përmasave të kriminalitetit
- Identifikimit dhe gjurmimit të të ardhurave nga krimi, fondeve terroriste ose çfarëdo pasurie tjetër që është, ose mund të jetë, subjekt i konfiskimit
- dhe të grumbullojë prova të cilat mund të shfrytëzohen në procedurën penale.

Pasi që përfitimet nga krimi kanë tendencë që së paku të legalizohen pjesërisht dhe të ripërdoren në ekonominë e ligjshme, hetimi financiar mund të ndërlidhet me një hetim të pastrimit të parave ose ta udhëheqë atë. Hetimi financiar mund të shpie te dyshimi për veprën penale të pastrimit të parave ose anasjelltas, kur një njësi e inteligjencës financiare (NJIF) analizon transaksionet e dyshimta ose heton veprën penale të pastrimit të parave,

⁴¹ FATF (2012), Shënim sqarues i Rekomandimit 30, paragrafi i 2-të.

Shih edhe: Raporti i FATF për çështje operative. Udhëzues për hetime financiare, 2012.

të ardhurat nga një krim i presupozuar mund të jenë subjekt i konfiskimit (si objekt nga vepra penale e pastrimit të parave).

3.2.1 Elementet e hetimeve financiare

Hetimi financiar mund të përkufizohet më së miri përmes përkufizimit të elementeve të tij ⁴² dhe përmes identifikimit të dispozitave relevante ligjore ndërkombëtare dhe kombëtare të cilat zbatohen në praktikë.

Siç përshkruhet në kursin bazik, elementet e hetimit financiar janë:

1. Zbulimi i veprës penale dhe i keqbërësve (krahas hetimit penal)
2. Caktimi i (vlerës së) të ardhurave nga krimi
3. Përcaktimi i pasurisë që mund të konfiskohet
4. Urdhri për ngrirje - masat e përkohshme për sigurim të konfiskimit.

Rezultat i hetimit financiar e mundësisht edhe i një urdhri për ngrirje do të ishte konfiskimi përfundimtar i të ardhurave nga krimi.

3.2.2 Aspekte të hetimeve financiare të krimeve kibernetike

Siç është paraqitur më në hollësi në kursin bazik, katër elementet e hetimeve financiare mund të aplikohen edhe në hetimet e krimeve kibernetike dhe/ose hetimin e krimeve elektronike, përfshirë të ardhurat nga krimi nga interneti.

Ekzistojnë disa specifika që lidhen me hetimin e krimit elektronik të cilat duhet të merren në konsideratë:

- Ku është keqbërësi dhe ku janë provat e krimit?
 - Kjo pyetje lidhet me çështjen e identifikimit të të dyshimit që e përdor një adresë të IP-së, qasjen në të dhënat për abonuesin, të dhëna për komunikime elektronike ose në rrjete sociale, e mundësisht edhe të dhënat për trafikun dhe përmbajtjen; bashkëpunimi me ISP-të, si kombëtare edhe ndërkombëtare; krijimi i kërkesave për ruajtje të të dhënave dhe urdhrat e gjykatës për të sekuestruar dhe siguruar prova elektronike.
- Çka janë të ardhurat nga krimi?
 - Kjo pyetje ndërlidhet me asetet dhe sistemet e pagesave siç janë paratë elektronike (e-money), valutat virtuale (p.sh. bitcoin) dhe pagesat bankare përmes internetit; llogaritë bankare jashtë shtetit, transaksionet e shumëfishta të llojeve të ndryshme, që ka mundësi të jenë strukturuar për t'i fshehur burimet e fondeve, tipologjitë e pastrimit të parave.
- Çka mund të konfiskohet/pasuria e të dyshimit?
 - Kur të merret në konsideratë rrjedha e parave në internet, ekziston edhe çështja e juridiksionit. Viktimat dhe keqbërësit shpesh nuk janë në të njëjtin vend. Duhet të shqyrtohet edhe konfiskimi i të ardhurave nga krimi kibernetik përmes hetimit financiar ose qasjes së pastrimit të parave. Përqendrimi dhe caku të paktën duhet të jenë në të ardhurat e drejtpërdrejta nga krimi (pagesa e zhvatjes ose transaksionet mashtruese) dhe ngrirja e vlerës në llogaritë e identifikuar bankare të përdorura për veprën penale (zhvatjen elektronike, mashtrimin kompjuterik).

⁴²Për më shumë hollësi shih Doracakun e Kursit Bazik (1.1.3).

- Rëndësia e kryerjes së një hetimi financiar paralel në hetimet e krimeve kibernetike për t'i zbuluar të ardhurat (llogaritë bankare dhe rrjedha e parave, transferet e valutave virtuale) dhe pasuria aktuale e keqbërësit.
- Urdhri për ngrirje
 - Veprimi i shpejtë është kyç në rastet e e-banking dhe internetit në përgjithësi. Kërkimi i veprës penale të pastrimit të parave dhe shfrytëzimi i pushtetit dhe lidhjeve ndërkombëtare të Njesisë së Inteligjencës Financiare mund të jenë një zgjidhje e mundshme. Urdhri nga gjykata dhe ndihma e ndërsjellë juridike duhet të pasojnë shpejt. Duhet të shqyrtohen edhe kanali i INTERPOL-it për ndihmë të ndërsjellë juridike, Konventa e Varshavës dhe mundësitë shtesë të Konventës së Budapestit, marrëveshjet e ndërsjella dhe qasja reciproke.
- Konfiskimi
 - Disa çështje shfaqen në rastet ndërkombëtare të ndihmës së ndërsjellë juridike përkitazi me regjimet e ndryshme të konfiskimit dhe ndarjes së aseteve.

3.2.3 Hetimet financiare në Bashkimin Evropian

Presidenca holandeze e BE-së në vitin 2016 ka identifikuar çështjen e luftimit të të ardhurave nga krimi dhe hetimet financiare si një nga prioritetet e saj. Është prezantuar një vlerësim i nevojave për instrumentet dhe metodat e hetimit financiar në Bashkimin Evropian si dhe 'gjashtë gjërat që duhet ditur për hetimet financiare'⁴³.

Vlerësimi i nevojave⁴⁴ ka vënë në pah se:

- **Hetimet financiare mund të aplikohen për të gjitha të hyrat e gjeneruara nga krimi:** ato nuk kufizohen vetëm brenda luftimit të krimeve financiare/ekonomike, përfshirë pastrimin e parave ose mbledhjen e provave kryesisht për rikthim të pasurisë.
- **Hetimet financiare mund të kryhen në të gjitha fazat e hetimeve penale dhe procedurave gjyqësore:** nga identifikimi i kriminalitetit, angazhimi i inteligjencës, mbledhja e provave (ndërtimi i rastit), përmes ndjekjes penale, paraburgimit dhe konfiskimit të pasurisë.

'Gjashtë gjërat që duhet ditur për hetimet financiare' po ashtu theksuan se profiti financiar është shpesh movitimi kryesor për kryerjen e krimeve, të ardhurat shpenzohen në mallra dhe pastrohen në ekonomi shpesh duke përdorur kompani dhe lehtësues legjitimë. Hetimet financiare janë një instrument shtesë hetues në pakon e mjeteve të zbatimit të ligjit të cilat mund të përdoren për t'i vënë personat që janë në krye të një organizate penale pas grilave dhe për t'ua marrë paratë dhe pasurinë. Privimi i njerëzve udhëheqës nga financat e tyre e bën shumë të vështirë për ata që t'i vazhdojnë aktivitetet penale. Kjo e bën hetimin financiar si instrument shumë efektiv në përçarjen e krimit të organizuar dhe terrorizmit.

⁴³Broshura: 6 gjërat që duhet ditur për Hetimet financiare, shkurt 2016. Gjetet në: <https://english.eu2016.nl/documents/publications/2016/02/10/brochure-the-6-need-to-knows-about-financial-investigation>

⁴⁴Vlerësimi i nevojave për instrumentet dhe metodat e hetimit financiar në Bashkimin Evropian, ECORYS, dhjetor 2015. Gjetet në: https://www.wodc.nl/binaries/2612-summary_tcm28-74130.pdf

'Ato që duhet ditur' po ashtu theksojnë:

- **Hetimet financiare mund të aplikohen për çdo lloj krimi:** Hetimet financiare mund dhe duhet të aplikohen në të gjitha llojet e krimeve të rënda dhe të organizuara siç janë trafikimi -dhe kontrabandimi me njerëz, mashtrimi, trafikimi i drogës dhe armëve dhe terrorizmi. Ekziston një keqkuptim i përgjithshëm se hetimet financiare janë të kufizuara vetëm brenda luftimit të krimeve ekonomike siç janë mashtrimet, veprat penale tatimore, korrupsioni dhe pastrimi i parave.
- **Hetimet financiare gjatë gjithë procedurës penale:** Në rastin ideal, hetimet financiare aplikohen në të gjitha fazat e hetimeve penale dhe procedurës gjyqësore. Që nga identifikimi proaktiv i krimit ose rrjetit kriminal te hetimet e rastit dhe mbledhja e provave deri te ndjekja penale dhe burgosja e keqbërësve dhe konfiskimi i pasurisë. Megjithatë, në shumë raste, hetuesit financiarë përfshihen në hetime penale në fazën përfundimtare, me qëllim që të gjurmojnë, identifikojnë dhe konfiskojnë të hyrat nga krimi. Kjo është një mundësi e humbur. Hetimet financiare duhet të fillojnë sa më parë që të jetë e mundshme.
- **Vetëdijesimi për fushëveprimin e gjerë financiar është kyç** Vetëdijesimi financiar është i nevojshëm në të gjitha nivelet e sistemit të zbatimit të ligjit - nga vetëdijesimi financiar bazik në nivel të politikave të komunitetit deri te ekspertiza shumë e specializuar e llogaridhënies forenzike që është e nevojshme për ta hequr atë 'vellon e korporatës' që fshihet pas strukturave komplekse ndërkufitare të pastrimit të parave. Është e rëndësishme që hetuesit penalë të jenë të vetëdijshëm për nevojën për të mbledhur prova financiare në një vend të krimit dhe për ta ftuar ekspertizën e specializuar financiare kur të ketë nevojë. Për më tepër, ekspertiza financiare mes prokurorëve dhe gjyqtarëve është kyçe për t'i kuptuar dhe vlerësuar dosjet e përgatitura nga hetuesit financiarë.
- **Bashkëpunimi ndërkufitar është kyç për suksesin e hetimeve financiare:** Hetuesit duhet të jenë në dijeni si për mundësitë e këmbimit joformal të informatave (CARIN, Europol, INTERPOL) për t'i vazhduar hetimet ashtu edhe për ato zyrtare, p.sh. Kërkesat për Ndihmë të Ndërsjellë Juridike.
- **Rëndësia e bashkëpunimit shumëdisiplinor:** Kur autoritetet publike që janë të angazhuara në hetimet financiare, siç janë organet e rendit, prokurorët publikë, Njësitë e Inteligjencës Financiare (NJIF) dhe autoritetet tatimore i kombinojnë ekspertizat e tyre, punojnë së bashku dhe i këmbejnë informatat, arrihen rezultatet më të mira. Për më tepër, ekziston një vetëdijesim dhe dëshirë në rritje që palët private si bankat, agjencitë e patundshmërisë dhe provajderët e shërbimeve të tjera profesionale do të mundnin dhe do të duhej të jepnin kontribut të çmuar në hetimet financiare.

PYETJE PËR VETËREFLEKTIM

1. Çfarë pengesash praktike ose ligjore, nëse ka, mund të parashihni të cilat mund ta pamundësojnë që një hetim financiar të kryhet paralelisht me një hetim të krimeve kibernetike?
2. Çfarë pengesash praktike ose ligjore, nëse ka, mund të parashihni të cilat mund ta parandalojnë identifikimin e të ardhurave kriminale që mbahen në forma elektronike ose virtuale?
3. Në çfarë momenti në procedurën penale (të hetimeve, gjyqësore, etj.)

mund të niset një hetim financiar?

- 4. Cilat kushte duhet të përmbushen para se të miratohet një urdhër për ngrirje të pasurisë?**

4 Bashkëpunimi ndërkufitar

4.1 Përmbledhje

Interneti, përveç aspekteve pozitive që ka, krijon edhe mundësi për keqpërdorime nga kriminelët të cilët mund të veprojnë në mënyra pothuajse të pavërejtshme, të shpejta dhe anonime, duke fshehur identitetin e tyre, provat dhe gjurmët e përfitimeve kriminele. Kjo karakteristikë përfaqëson një sfidë për agjencitë e zbatimit të ligjit.

Është e rëndësishme të pranohen përfitimet nga mundësitë e ndryshme për bashkëpunim ndërkombëtar duke kombinuar tri aspekte të hetimit të të ardhurave nga krimi elektronik: hetimi i krimit kibernetik, hetimi financiar paralel dhe hetimi i pastrimit të parave⁴⁵. Konventa e Varshavës dhe Konventa e Budapestit e Këshillit të Evropës janë instrumente të rëndësishme për t'i adresuar këto aspekte.

Kursi Bazik përmban prezantimin e aspekteve kryesore të bashkëpunimit ndërkombëtar, siç është përparësia e kombinimit të mënyrave të bashkëpunimit ndërkombëtar në fushën e krimeve kibernetike dhe provave elektronike si dhe të hetimeve financiare dhe të parandalimit dhe hetimit të pastrimit të parave, duke bërë dallimin mes bashkëpunimit ndërkombëtar për këmbim të informatave (operacionale) dhe ndihmës së ndërsjellë juridike për qëllime të provave, të rrjeteve dhe organizatave relevante ndërkombëtare për këmbim të informatave, dispozitave të rëndësishme të konventave të Budapestit dhe Varshavës, etj.

Në të njëjtën kohë, ekzistojnë një varg sfidash që kanë të bëjnë me bashkëpunimin ndërkombëtar e sidomos me ndihmën e ndërsjellë juridike e cila duhet të merret në konsideratë.

Konventat e Budapestit dhe Varshavës paraqesin mënyrat për bashkëpunim ndërkombëtar të cilat aplikohen kur të kombinohet hetimi paralel i krimit (kibernetik) dhe hetimi financiar. Megjithatë, bashkëpunimi ndërkombëtar përballet me sfida specifike ligjore dhe praktike, që kanë të bëjnë me secilin nga traktatet, si rezultat i rrethanave praktike, siç është natyra e provave elektronike, teknologjia e ruajtjes së të dhënave në internet (cloud), por edhe identifikimi i të ardhurave nga krimi, sekuestrimi dhe konfiskimi i pasurisë jashtë vendit, marrja në konsideratë e regjimeve të ndryshme për konfiskim dhe dallimeve ligjore mes palëve. Këto sfida janë identifikuar dhe adresuar nga organet relevante të Këshillit të Evropës, siç është Komiteti i Ekspertëve për Funkcionimin e Konventave Evropiane për Bashkëpunim në Çështje Penale (PC-OC) dhe Komiteti i Konventës kundër Krimeve kibernetike (T-CZ).

Kur të kombinohen aspektet e hetimit kibernetik, hetimit financiar me parandalimin dhe hetimin e pastrimit të parave, ia vlen të jeni të vetëdijshëm për të gjitha këto aspekte të ndryshme, përfitime dhe sfida ekzistuese të mënyrave për bashkëpunim të ofruara nga konventat e Budapestit dhe Varshavës.

Ndonëse ndihma e ndërsjellë ligjore ende konsiderohet si mjeti kryesor për t'i zbatuar urdhrat e gjykatës dhe për të mbledhur prova jashtë vendit, kohëzgjatja e procedurës paraqet një pengesë të rëndësishme. Megjithatë, shfrytëzimi i hetimeve të përbashkëta

⁴⁵Megjithatë duhet të vihet në pah se me gjithë instrumentet e mundshme efikase për ta parandaluar dhe luftuar pastrimin e parave në shumë vende, ndjekja penale e pastrimit të parave ende mbetet sfidë.

dhe i ekipeve të përbashkëta hetuese mund t'i adresojë disa sfida të efikasitetit. Bashkëpunimi mes organeve të zbatimit të ligjit (policisë dhe prokurorisë) dhe këmbimi i informacioneve janë të domosdoshme në rastet ndërkufitare. Rrjetet dhe organizatat relevante ndërkombëtare luajnë rol të rëndësishëm në këtë drejtim dhe po ashtu ndihmojnë edhe në ndërtimin e besimit. Kanalet dhe instrumentet për bashkëpunim të ofruara prej tyre janë thelbësore për këmbim të informatave dhe provave në hetimet penale.

4.1.1 Rrjetet dhe organizatat relevante për këmbim të informatave dhe ndihma e ndërsjellë juridike

Bashkëpunimi ndërkombëtar - këmbimi i informatave (operacionale) Policia me polici, prokurorët me prokurorë	
Rrjeti 24/7	Rrjeti (pikat kontaktuese të policisë dhe/ose prokurorisë) Neni 35 i Konventës së Budapestit
Grupi EGMONT	Rrjeti i NJIF-ëve - parandalimi i pastrimit të parave, shtyrja e transaksioneve të dyshimta. Neni 46 i Konventës së Varshavës
Rrjeti CARIN	Rrjeti Camden i agjencive për rikthim të pasurisë Rrjeti i ekspertëve për konfiskim të të ardhurave nga krimi
INTERPOL	Kanali për këmbim të informatave dhe për dërgim të kërkesave për NNJ
Europol (EC3)	Marrëveshjet relevante të BE-së me vendet joanëtare të BE-së
Eurojust	Rrjeti gjyqësor evropian kundër krimeve kibernetike (2016) Marrëveshjet relevante të BE-së me vendet joanëtare të BE-së
Bashkëpunimi ndërkombëtar - Ndihma e Ndërsjellë Juridike (NNJ) Bashkëpunimi zyrtar - provat	
NNJ: Bashkëpunimi zyrtar, rezultati i një kërkesë për NNJ mund të përdoret si provë në gjykatë. Kanalet e zakonshme të komunikimit bëhen përmes autoriteteve të përcaktuara qendrore, shpesh ministritë e drejtësisë ose ministritë e punëve të jashtme.	
Bashkëpunimi i drejtpërdrejtë: gjyqtarët me gjyqtarë, prokurorët me prokurorë (marrëveshjet dypalëshe të BE-së) Konventat e Varshavës (Neni 34) dhe Budapestit (Neni 27/9) po ashtu parashohin bashkëpunimin e drejtpërdrejtë mes autoriteteve përgjegjëse gjyqësore dhe të prokurorisë në raste urgjente, krahas dërgimit të kërkesave zyrtare përmes autoriteteve qendrore.	
Opsionet e tjera	Ekipet e përbashkëta hetuese (JITs) Hetimet paralele Transferimi i procedurës.

Kriminelët fshihen (ose mbajnë) pasurinë e tyre jashtë shtetit. Në hetimin e krimeve elektronike të kryera nga grupet kriminale ndërkombëtare është e nevojshme të verifikohet nëse kriminelët kanë ndonjë pasuri jashtë shtetit. Në rastet e tilla **bashkëpunimi mes policisë dhe prokurorisë** është shumë i rëndësishëm. Një person kontaktues i policisë së një vendi të huaj mund të këshillojë se çfarë të dhënash mund të

sigurohen nga burimet publike, përmes bashkëpunimit policor apo përmes kërkesave për ndihmë juridike. Informatat e tilla mund ta bëjnë sigurimin e të dhënave shumë më të lehtë dhe më të shpejtë. Bashkëpunimi i tillë është operacional dhe këtu përjashtohen urdhrat e gjykatës.

Kontaktet operationale dhe bashkëpunimi mund të shpijnë te krijimi i ekipeve të përbashkëta hetuese, të cilat në parim mund ta lehtësojnë një qasje më efikase të ndihmës së ndërsjellë juridike. Kjo po ashtu mund të shpie te aranzhimi i hetimeve paralele në raste ndërkufitare të cilat përfshijnë më shumë keqbërës dhe viktime.

Ndihma e ndërsjellë juridike është bashkëpunim zyrtar dhe rezultati i kërkesës mund të përdoret si provë në gjykatë. Kanalet e zakonshme të komunikimit bëhen përmes autoriteteve të përcaktuara qendrore, shpesh ministrive të drejtësisë. Kanalet e mundshme po ashtu mund të jenë Ministria e Punëve të Jashtme ose në rastet urgjente INTERPOL, Europol ose Eurojust.

Brenda BE-së, ndihma e ndërsjellë juridike kryhet drejtpërsëdrejti mes autoriteteve përgjegjëse (prokurorisë/gjykatave). Konventat e Varshavës (Neni 34) dhe Budapestit (Neni 27/9) po ashtu parashohin qasje të tilla në raste urgjente, krahas dërgimit të kërkesave zyrtare përmes autoriteteve qendrore.

4.1.2 Mjetet Ligjore Ndërkombëtare

Krimet kibernetike	Hetimet financiare
Këshilli i Evropës	
Konventa e Budapestit kundër Krimit Kibernetik dhe Protokoli kundër Ksenofobisë dhe Racizmit ⁴⁶	Konventa e Varshavës kundër Pastrimit, Kërkimit, Sekuestrimit dhe Konfiskimit të të Ardhurave nga Krimi dhe kundër Financimit të Terrorizmit ⁴⁸
Shënime udhëzuese T-CY ⁴⁷	Konventa e Strasburgut e vitit 1990 kundër pastrimit, kontrollit, sekuestrimit dhe konfiskimit të të ardhurave nga krimi ⁴⁹
BE	
Direktiva 2013/40/EU e Parlamentit Evropian dhe e Këshillit e datës 12 gusht 2013 mbi sulmet kundër sistemeve informative që e zëvendëson Vendimin Kornizë të Këshillit 2005/222/JHA ⁵⁰	Direktiva 2014/42/EU për ngrirjen dhe konfiskimin e përfitimeve të krimit në Bashkimin Evropian ⁵¹

⁴⁶Konventa kundër Krimit Kibernetik (ETS 185, 21,11) dhe Protokoli shtesë i Konventës kundër krimit kibernetik, lidhur me penalizimin e akteve të natyrës raciste dhe ksenofobe të kryera përmes sistemeve kompjuterike ETS 189, 28.01.2003.

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

⁴⁸Konventa mbi Pastrimin, Kërkimin, Sekuestrimin dhe Konfiskimin e të Ardhurave nga Krimi dhe mbi Financimin e Terrorizmit, CETS 198, 16.05.2005.

⁴⁹Konventa mbi Pastrimin, Kërkimin, Sekuestrimin dhe Konfiskimin e të Ardhurave nga Krimi, Strasburg ETS 141, 08.11.1990.

⁵⁰ Direktiva prezanton rregulla të reja që harmonizojnë veprën penale me ndëshkimin për një varg veprash penale që kanë si cak sistemet informative. Ajo po ashtu u bën thirrje vendeve të BE-së t'i shfrytëzojnë pikat e njëjta kontaktuese që i shfrytëzon edhe Këshilli i Evropës

Direktiva 2016/1148 e Parlamentit Evropian dhe e Këshillit të korrikut 2016 që ka të bëjë me masat për një nivel të lartësisë së rëndomtë të sigurisë së rrjeteve dhe sistemeve informative (Direktiva NIS) ⁵²	Veprimi i përbashkët 98/699/JHA mbi pastrimin e parave, identifikimin, gjurmimin, ngrirjen, sekuestrimin, konfiskimin e dobive dhe të ardhurave nga krimi ⁵³
Të gjeturat e Këshillit të Bashkimit Evropian për përmirësimin e drejtësisë penale në raste të krimeve kibernetike dhe të gjeturat e Rrjetit të Gjyqësorit Evropian kundër krimeve kibernetike ⁵⁴ , qershor 2016.	Vendimi Kornizë 2001/500/JHA mbi pastrimin e parave, identifikimin, gjurmimin, ngrirjen, sekuestrimin, konfiskimin e dobive dhe të ardhurave nga krimi ⁵⁵
	Direktiva që ndryshon Direktivën (EU) 2015/849 për parandalimin e përdorimit të sistemit financiar për qëllime të pastrimit të parave ose financimit të terrorizmit dhe ndryshimi i Direktivës 2009/101/EC ⁵⁶
	Vendimi Kornizë 2005/212/JHA për konfiskimin e të ardhurave, dobive dhe pasurive që lidhen me krimin ⁵⁷
	Vendimi kornizë 2003/577/JHA për ekzekutimin e urdhrave për ngrirjen e pasurisë ose provave në Bashkimin Evropian ⁵⁸

dhe G8 për të reaguar shpejt ndaj kërcënimeve që kanë të bëjnë me teknologjinë e avancuar. Gjendet në: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040>

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

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

⁵³ Në përpjekje për ta përmirësuar bashkëpunimin mes shteteve anëtare të Bashkimit Evropian (BE-së), ky veprim i përbashkët siguron përgatitje, brenda fushëveprimit të operacioneve të Rrjetit Evropian për Gjyqësi, të udhëzimeve që përdoren lehtë për identifikimin, gjurmimin, ngrirjen, sekuestrimin dhe konfiskimin e dobive dhe të ardhurave nga krimi. Gjendet në: <http://eur-lex.europa.eu/legal-content/NLN/TXT/?uri=uriserv%3A32013L0040>

⁵⁴ Të gjeturat përqendrohen në: bashkëpunimin me provajderët e shërbimit që lejojnë zbulim të shpejtë të të dhënave; procese më pak rigoroze ligjore mund të parashihen për të siguruar kategori specifike të të dhënave, sidomos të dhënat për abonuesit. Procedurat për Ndhimë të Ndërsjellë Juridike (NNJ) që kanë të bëjnë me të dhënat elektronike duhet të përshpejtohen dhe harmonizohen; volumi i kërkesave për NNJ mes autoriteteve kompetente duhet të reduktohet me rritjen e bashkëpunimit me provajderët e shërbimeve. Procedurat për njohje të ndërsjellë duhet të shfrytëzohen në mënyrë efikase për të siguruar dhe ruajtur provat elektronike. Përcaktimi i faktorëve ndërlidhës për zbatimin e juridiksionit në krimet kibernetike, përfshirë rastet kur lokacioni i të dhënave nuk dihet (ende) ose kur është i paqëndrueshëm. Gjendet në: <http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace/>.

⁵⁵ Vendimi Kornizë i Këshillit 2001/500/JHA i datës 26 qershor 2001 mbi pastrimin e parave, identifikimin, gjurmimin, ngrirjen, sekuestrimin, konfiskimin e dobive dhe të ardhurave nga krimi (OJ L 182, 5.7.2001, p.1). Gjendet në: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A2001F0500>

⁵⁶ Ajo po ashtu synon të rregullojë valutat virtuale duke obliguar provajderët e shërbimeve të këmbimit dhe provajderët e custodial wallet (kuletës kujdestare) që mes tjerash të bashkëpunojnë edhe me Njësitë e tyre të Inteligjencës Financiare (NJIF). Gjendet në: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:0450:FIN%20>

⁵⁷ Vendimi Kornizë i Këshillit 2005/212/JHA i datës 24 shkurt 2005 për për konfiskimin e të ardhurave, dobive dhe pasurive që lidhen me krimin (OJ L 68, 15.3.2005, p.49). Gjendet në: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:068:0049:0051:en:PDF>

⁵⁸ Vendimi Kornizë i Këshillit 2003/755/JHA i datës 22 shkurt 2003 për ekzekutimin e urdhrave për ngrirjen e pasurisë ose provave në Bashkimin Evropian (OJ L 196, 2.8.2003, f.45). Gjendet në: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003F0577>

	Vendimi Kornizë 2006/783/JHA për zbatimin e parimit të pranimet reciprok të urdhrave për konfiskim ⁵⁹
	Vendimi i Këshillit 2007/845/JHA që ka të bëjë me bashkëpunimin mes Zyrave për Rikthim të Pronës së Shteteve Anëtare në fushën e gjurmimit dhe identifikimit të të hyrave nga krimi, ose pronave të tjera që lidhen me krimin – (ka përcaktuar obligimin për të themeluar Zyra(t) për Rikthim të Pronës (AROs)) ⁶⁰
	Direktiva 2014/41/EU për Urdhrin Evropian për Hetime të gështjeve penale ⁶¹
KB	
Rezolutat për luftimin e keqpërdorimit kriminal të teknologjive informative (Rezolutat 55/63 dhe 56/121) ⁶²	Konventa e KB 1988 kundër trafikut të paligjshëm me droga narkotike dhe substanca psikotropike ⁶³
Rezoluta e Asamblesë së Përgjithshme të KB 64/211 (mars 2010) për krijimin e një kulture globale të sigurisë kibernetike ⁶⁴	Konventa e KB 2000 kundër krimit të organizuar transnacional ⁶⁵
	Konventa e KB 2003 kundër korrupsionit ⁶⁶
Të tjera (traktatet rajonale)	
Konventa e Unionit Afrikan për siguri kibernetike dhe mbrojtje të të dhënave personale ⁶⁷	
Konventa arabe për luftimin e veprave penale të teknologjisë informative ⁶⁸	
Marrëveshja e Federatës së Shteteve të Pavarura për bashkëpunim në luftimin e	

⁵⁹ Vendimi Kornizë i Këshillit 2006/783/JHA i datës 6 tetor 2006 për ekzekutimin e urdhrave për zbatimin e parimit të pranimet reciprok të urdhrave për konfiskim (OJ L 328, 24.11.2006, f.59).

Gjendet në: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32006F0783>

⁶⁰ Vendimi përcakton kriteret për themelimin e Zyrave kombëtare për Rikthim të Pronës (AROs) në vendet e BE-së. Gjendet në: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007D0845>

⁶¹ Direktiva për Urdhrin Evropian për Hetime (EIO) përcakton një sistem të ri gjithëpërfshirës që u mundëson shteteve të BE-së të sigurojnë prova në vendet e tjera të BE-së, për rastet penale që mbulojnë më shumë se një shtet. Gjendet në: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041>

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

⁶³ Konventa e Kombeve të Bashkuara kundër trafikut të paligjshëm me droga narkotike dhe substanca psikotropike, Vjenë, 19.12.1988 (Neni 5).

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

⁶⁵ Konventa e Kombeve të Bashkuara kundër krimit të organizuar transnacional, Nju Jork, 15.11.2000 (Nenet 12-14).

⁶⁶ Konventa e Kombeve të Bashkuara kundër korrupsionit, Nju Jork, 31.10.2003 (Nenet 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

veprave që lidhen me informata kompjuterike ⁶⁹	
Marrëveshja e Organizatës për Bashkëpunim Shanghai në fushën e sigurisë ndërkombëtare të informatës ⁷⁰	

Brenda BE-së, parimi i pranimit të ndërsjellë, në vend të ndihmës së ndërsjellë, është futur në përdorim që nga viti 2003 për ekzekutimin e urdhrave për ngrirje dhe në vitin 2006 edhe për urdhra për konfiskim. Edhe hapësira e refuzimit të ekzekutimit të urdhrave ishte kufizuar me zbehjen e parimit të kriminalitetit të dyfishtë dhe ngrirjes së dyfishtë. BE-ja ka bërë edhe hapa të tjerë për ta lehtësuar bashkëpunimin duke prezantuar Urdhrin Evropian për Hetime

4.1.3 Dispozitat e Bashkëpunimit Ndërkombëtar

Instrumentet ligjore ndërkombëtare trajtojnë aspekte të kriminalizimit të sjelljes, bashkëpunimin procedural (instrumentet hetuese) dhe ndërkombëtar, përfshirë bazën ligjore për ndihmë të ndërsjellë juridike (NNJ). Konventat e Varshavës dhe Budapestit mundësojnë mënyra të cilat mund të përdoren dhe të kombinohen me qëllim që të arrihen rezultatet më të mëdha gjatë kryerjes së hetimeve paralele financiare dhe të krimeve (kibernetike). Bashkëpunimi u nënshtrohet dispozitave shtetërore me mbrojtje për shtyrje ose refuzim të kërkesave (Konventa e Varshavës, Kapitulli 5, Neni 27 dhe Konventa e Budapestit, Neni 25/4 dhe 27/4 dhe 5). Fushat kryesore të bashkëpunimit janë theksuar si më poshtë:

Dispozitat e Bashkëpunimit Ndërkombëtar	
Konventa e Budapestit	Konventa e Varshavës
Parimet elementare	
<p>(Nenet 23-25)</p> <p>Palët duhet të jenë në gjendje të ofrojnë ndihmë të ndërsjellë për qëllime të hetimit ose procedurës në lidhje me:</p> <ul style="list-style-type: none"> - krimet kibernetike (Nenet 2-10) - ose për mbledhjen e provave në formë elektronike të një veprë penale. 	<p>(Neni 15)</p> <p>Palët duhet të bashkëpunojnë në mënyrë të ndërsjellë për qëllime të hetimit dhe procedurës me qëllim të konfiskimit të dobive dhe të ardhurave.</p> <p>Kërkesa për:</p> <ul style="list-style-type: none"> - konfiskim të artikujve të caktuar - ose të paguajë një shumë parash që korrespondon me vlerën e të ardhurave - dhe për ndihmë për hetime dhe masa të përkohshme me qëllim të konfiskimit.
Informimi spontan	
(Neni 26)	(Neni 20)

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>

<p>Një palë, mundet brenda kufijve të ligjit vendor dhe pa ndonjë kërkesë paraprake, t'i përcjellë një pale tjetër informata të siguruar brenda kornizës së hetimeve të veta kur merr në konsideratë se zbulimi i këtyre informatave mund ta ndihmojë palën pranuese për të nisur dhe kryer hetime ose procedura në lidhje me veprat penale të përkufizuara në përputhje me këtë konventë ose mund të shpie te një kërkesë për bashkëpunim nga ajo palë në këtë kaptinë.</p>	<p>Dispozita të ngjashme</p>
<p>Masat e përkohshme</p>	
<p>(Nenet 29-30)</p> <p>Ruajtja e përshpejtuar e të dhënave të mbajtura në kompjuter. Zbulimi i përshpejtuar i të dhënave të ruajtura për trafikun.</p>	<p>(Nenet 21-22)</p> <p>Ngjirja ose sekuestrimi, për ta parandaluar çdo trajtim, transfer ose heqje qafe të pronës dhe për t'i siguruar në mënyrë spontane të gjitha informatat relevante për masa të përkohshme.</p>
<p>Ndihma për hetime</p>	
<p>(Nenet 31-34)</p> <p>Ndihma e ndërsjellë në lidhje me kompetencat hetuese:</p> <ul style="list-style-type: none"> - Qasja në të dhëna të ruajtura në kompjuter; - Qasja ndërkufitare në të dhënat e ruajtura në kompjuter me pëlqim ose në rastet kur janë në dispozicion publik; - Mbledhja në kohë reale e të dhënave për trafikun; dhe - Përgjimi i të dhëna për përmbajtjen. 	<p>(Nenet 16-19)</p> <p>Palët ndihmojnë në identifikimin dhe gjurmimin e dobive dhe të ardhurave, që përfshijnë sigurimin e provave rreth ekzistencës, lokacionit ose lëvizjes, natyrës, statusit ligjor ose vlerës së pronës së lartpërmendur. Ndihma e tillë përfshin edhe kërkesat për:</p> <ul style="list-style-type: none"> - informata për llogaritë bankare; - për transaksione bankare; dhe - monitorimi i transaksioneve bankare.
	<p>Konfiskimi</p>
	<p>(Nenet 23-25)</p> <ul style="list-style-type: none"> - Zbatimi i urdhrit për konfiskim; ose - dorëzimi i kërkesës në autoritetet e saj kompetente për qëllim të sigurimit të një urdhri për konfiskim dhe për ta zbatuar atë përfshirë kërkesën për të paguar një shumë parash që përkon me vlerën e të ardhurave, ose për konfiskim të një artikulli ose aseti të caktuar.
	<p>(Neni 23/5)</p>

	<p>Masat ekuivalente me konfiskimin:</p> <ul style="list-style-type: none"> - sanksionet jopenale (konfiskimi që nuk bazohet në paraburgim); - rregullat për këmbim të aseteve (kompensim ndaj viktimave, pronarëve legjitimë).
Rrjetet për bashkëpunim	
<p>Rrjeti 24/7 (Neni 35)</p> <p>Secila palë cakton një pikë kontaktuese në dispozicion 24/7 me qëllim që të sigurohet ofrimi i ndihmës së menjëhershme për qëllime të</p> <ul style="list-style-type: none"> - hetime ose procedura në lidhje me veprat penale që kanë të bëjnë me sistemet dhe të dhënat kompjuterike, - ose për mbledhjen e provave në formë elektronike të një vepre penale. <p>Një ndihmë e tillë përfshin lehtësimin, ose, nëse lejohet me ligjin dhe praktikën vendore, kryerjen e drejtpërdrejtë të masave të mëposhtme:</p> <ul style="list-style-type: none"> - ofrimin e këshillave teknike; - ruajtjen e të dhënave (Nenet 29 dhe 30); - mbledhja e provave, - ofrimi i informatave ligjore, - dhe lokalizimi i të dyshimëve. 	<p>Bashkëpunimi mes NJIF-ve (Nenet 46-47)</p> <p>NJIF këmbëjnë, në mënyrë spontane ose me kërkesë, të çfarëdo informate të qasshme që mund të jetë e rëndësishme</p> <ul style="list-style-type: none"> - për përpunim ose analizë të informatës, ose - për hetime nga NJIF në lidhje të transaksioneve financiare që kanë të bëjnë me pastrim të parave dhe me personat e përfshirë fizikë ose juridikë. <p>Kompetencat e NJIF për t'i shtyrë transaksionet e dyshimta</p>

PYETJE PËR VETËREFLEKTIM

1. Cilat kushte duhet të plotësohen para se të këmbëhen informatat në mënyrë spontane me një juridiksion tjetër?
2. Çfarë bazash ekzistojnë në legjislacionin tuaj për ta refuzuar bashkëpunimin me një kërkesë ndërkombëtare për ndihmë?
3. Çfarë kushtesh duhet të plotësohen për ta përsheptuar zbulimin e të dhënave të ruajtura për trafikun?
4. Çfarë masash praktike janë të miratuara për ta mundur menaxhimin, hedhjen ose këmbimin e pasurisë së konfiskuar me një juridiksion tjetër? A duhet të bëhen këto aranzhime në bazë të rasteve të caktuara?

4.2 Vlerësimi i zbatimit të dispozitave për bashkëpunim ndërkombëtar

Është e rëndësishme të shënohen dhe të kuptohen mundësitë dhe pengesat për bashkëpunim ndërkombëtar në fushën e hetimeve të krimeve financiare dhe kibernetike dhe provave elektronike siç janë identifikuar nga organizatat ndërkombëtare.

4.2.1 Vlerësimet përkitazi me targetimin e të ardhurave nga krimi

4.2.1.1 GENVAL

Në BE⁷¹, në kontekst të rrethit të pestë të vlerësimeve të ndërsjella të "krimeve financiare dhe hetimeve financiare", Grupi Punues për Çështje të Përgjithshme përfshirë vlerësimet (GENVAL) në raportin e tij përfundimtar 2012⁷² vuri në pah sfidat kryesore që prekin këtë fushë, respektivisht:

1. Menaxhimi i rasteve (përfshirë menaxhimin e kohës dhe burimeve) dhe bashkëpunimi mes autoriteteve kompetente në nivel kombëtar dhe ndërkombëtar,
2. Rregullat ligjore shpesh të komplikuar dhe të ndryshme dhe traditat, brenda shtetit dhe në nivel të BE-së, të shoqëruara nganjëherë me zbatim të dobët,
3. Provat dhe çështja e të dhënave elektronike, dhe
4. Koha. Hetimet financiare shpesh marrin kohë të gjatë dhe mund të marrin shumë burime, në aspekt të kohës, angazhimit të njerëzve dhe mjeteve financiare.

Raporti po ashtu përmban një varg rekomandimesh për Shtetet Anëtare dhe BE-në të cilat mund të jenë të rëndësishme për çdo juridiksion:

- Hetimet financiare duhet të kryhen në të gjitha rastet e krimeve të rënda dhe të krimit të organizuar (përfshirë terrorizmin) përveç veprave penale ekonomike dhe financiare. Andaj duhet të hartohet një politikë gjithëpërfshirëse rreth krimeve financiare dhe hetimeve financiare, që mbulon të gjitha autoritetet relevante, përfshirë ndjekjen penale, e cila ka për qëllim përshpejtimin e hetimeve komplekse dhe të gjata në fushën e krimit financiar. Ajo duhet të pasqyrojë prioritetet relevante për të cilat është arritur pajtueshmëria në nivel të BE-së dhe të caktojë bazën për hetime proaktive. Vëmendje më e lartë duhet t'u kushtohet përfitimeve nga bashkëpunim ndërkombëtar, e sidomos në nivel të BE-së.
- Politika kundër krimeve financiare dhe hetimet financiare duhet të pasqyrohen në strategjinë afatgjatë kombëtare. Kurdo që është e mundshme, një koncept i politikave të udhëhequra nga inteligjenca financiare duhet të përfshihet në strategji, për të mundësuar masa proaktive të zbatimit në bazë të rezultateve të analizave. Strategjia duhet të kombinohet me rishikime të rregullta dhe një metodologji të vlerësimit si dhe me një mekanizëm të njëmendtë raportues për entitetet e përfshira. Në përcaktimin e një strategjie të tillë duhet të merren në konsideratë disa kritere, rregulla dhe udhëzime elementare për ta qartësuar ndarjen e detyrave mes autoriteteve të ndryshme me kompetenca të përzgjedhura, si dhe përfshirjen e prioritetëve kyçe, përfshirë rastet e krimeve të rënda ndërkombëtare. Strategjia po ashtu duhet të mbështetet nga një menaxhim i plotë brenda policisë, me qëllim që të promovohet një qasje proaktive e udhëhequr nga inteligjenca.

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

⁷² EU GENVAL 2012 Raporti përfundimtar për rrethin e pestë të vlerësimit të ndërsjellë – "Krimet financiare dhe hetimet financiare". Gjetet në: <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012657%202012%20REV%202>

- Shtetet Anëtare duhet ta zbatojnë legjislacionin e BE-së në lidhje me njohjen e ndërsjellë dhe bashkëpunimin gjyqësor në çështje penale. Veç kësaj, duhet të bëhet një rishikim i zbatimit të vendimeve relevante kornizë dhe zbatimit të mekanizmave për ndihmë të ndërsjellë juridike nga Shtetet Anëtare dhe agjencitë relevante të BE-së. Përmes kësaj, Shtetet Anëtare duhet të identifikojnë dhe trajtojnë pengesat për këmbim efikas të të dhënave proaktive me autoritetet ndërkombëtare të zbatimit të ligjit, agjencitë e BE-së dhe palët e tjera relevante. Këmbimi spontan i informatave në përputhje me Vendimin e Këshillit 2007/845/JHA të datës 6 dhjetor 2007 për bashkëpunim mes zyra për rikthim të pasurisë së Shteteve Anëtare në fushën e gjurmimit dhe identifikimit të të ardhurave, ose pasurive të tjera, të ndërlidhura me krimin, duhet të rritet edhe më tej dhe përdorimi i Vendimit Kornizë të Këshillit 2006/960/JHA i datës 18 dhjetor 2006 për thjeshtëzimin e këmbimit të informatave dhe inteligjencës mes autoriteteve të zbatimit të ligjit dhe Shteteve Anëtare të BE-së duhet të promovohet.

4.2.1.2 Pyetësi PC-OC

Komiteti i Ekspertëve i Këshillit të Evropës për funksionimin e konventave evropiane për bashkëpunim në çështje penale (PC-OC) përqendroi vëmendjen në fushën e luftimit të të ardhurave nga krimi në vitin 2014. Përgjigjet në pyetësin e PC-OC⁷³ treguan, mes tjerash, se ekzistojnë dallime mes palëve kur është fjala te zbatimi i dispozitave të konventave të Strasburgut dhe Varshavës, që janë të rëndësishme për bashkëpunim ndërkombëtar.

Disa nga aspektet e adresuara në pyetësor ishin:

- Shtetet nuk janë gjithmonë në gjendje ta sigurojnë zbatimin e një kërkesë që mbështetet në një sistem të konfiskimit të ashtuquajtur të bazuar në vlera. Sistemi përshkruhet në të dy konventat si sistem me të cilin është e mundur të bashkëpunohet përveç të ashtuquajturit sistem i konfiskimit i bazuar në objekt. Në të dy sistemet është i nevojshëm dënimi penal. Në sistemin e konfiskimit të bazuar në vlera, përfitimet nga krimi llogariten. Në fund, në bazë të këtyre kalkulimeve, gjyqtari shqipton një obligim për ta paguar një shumë të parave që është ekuivalente me profitin e siguruar kriminal. Urdhri për konfiskim pastaj mund të ekzekutohet ndaj të gjitha aseteve që i përkasin personit të dënuar. Në këtë drejtim, nuk është kriter që të dëshmohet se këto asete janë siguruar drejtpërsëdrejti nga vepra penale.
- Disa shtete e pranojnë mundësinë e sekuestrimit dhe konfiskimit të aseteve të cilat de fakto i përkasin personit të akuzuar/dënuar por të cilat konsiderohen nga aspekti ligjor t'i përkasin një personi të tretë, kryesisht persona që përdoren si mbulesë.
- Vetëm disa shtete janë në gjendje të ofrojnë ndihmë të ndërsjellë juridike për qëllime, ose që kanë të bëjnë, me, konfiskimet pa dënim dhe masat e tjera (për shembull konfiskimet civile). Kjo e përfshin edhe fazën e mbledhjes së informatave, gjatë së cilës informatat inkriminuese shpesh kërkohen brenda një procedure pa dënim (NCB), kontrolli, sekuestrimi dhe konfiskimi të të ardhurave nga krimi.

⁷³ Pyetësi për përdorimin dhe efikasitetin e instrumenteve të Këshillit të Evropës në lidhje me bashkëpunimin ndërkombëtar në fushën e sekuestrimit dhe konfiskimit të të ardhurave nga krimi, përfshirë menaxhimin e mallrave dhe ndarjen e aseteve, PC-OC Mod (2015) 06Rev4, 19.5.2016. Gjetet në: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680666607>

- Disa shtete janë në gjendje të ofrojnë ndihmë në procedura administrative penale, civile dhe administrative që kanë të bëjnë me detyrimet e entiteteve ligjore për qëllime të sekuestrimit dhe konfiskimit të të ardhurave nga krimi.
- Vetëm disa shtete janë në gjendje të ofrojnë ndihmë në procedurat që kanë të bëjnë me valutat virtuale siç janë bitkoinët, sidomos në lidhje me sekuestrimin dhe konfiskimin.

4.2.1.3 MONEYVAL

Komiteti i ekspertëve për vlerësimin e masave kundër pastrimit të parave dhe financimit të terrorizmit - MONEYVAL⁷⁴ është një organ permanent monitorues i Këshillit të Evropës të cilit i është besuar detyra e vlerësimit të përputhshmërisë standardet kryesore ndërkombëtare të luftimit të pastrimit të parave dhe financimit të terrorizmit dhe efikasitetit të zbatimit të tyre, si dhe detyra e nxjerrjes së rekomandimeve për autoritetet e shteteve në lidhje me përmirësimet e nevojshme të sistemeve të tyre.

Përmes një procesi dinamik të vlerësimeve të ndërsjella, rishikimeve kolegjiale dhe përditësimit të rregullt të raporteve të tyre, MONEYVAL synon të përmirësojë kapacitetet e autoriteteve shtetërore për ta luftuar pastrimin e parave dhe financimin e terrorizmit me efikasitet më të lartë.

Raportet vlerësuese janë të publikuara në mënyrë elektronike.⁷⁵

4.2.2 Vlerësimet që lidhen me krime kibernetike

4.2.2.1 GENVAL

Rrethi i shtatë i vlerësimeve të ndërsjella të BE-së i kushtohet zbatimit praktik dhe funksionimit të politikave evropiane për parandalimin dhe luftimin e krimeve kibernetike. Raportet përfundimtare të vlerësimit janë bërë publike dhe mund t'u shërbejnë vendeve të tjera për t'i rishikuar legjislacionin dhe strategjitë e tyre për krimet kibernetike.⁷⁶

Të njëjtën kohë, projektraporti përfundimtar vë në pah disa aspekte problematike që kanë të bëjnë me bashkëpunim ndërkombëtar, respektivisht se korniza e kohës mesatare për t'u përgjigjur në një kërkesë për NNJ shkon deri në disa muaj dhe ndryshon nëse NNJ është ofruar në bazë të një marrëveshjeje ndërkombëtare ose reciprocitetit. Në rastet e fundit, koha e përgjigjes është edhe më e gjatë. Megjithatë, për shkak të veçantisë së krimeve kibernetike, "procedurat e tejzgjatura të NNJ i bëjnë kanalet e NNJ mjaft joefikase, me pasoja negative për kryerjen dhe suksesin e hetimeve, pasi që provat digjitale janë të paqëndrueshme dhe duhet të trajtohen shpejt dhe me efikasitet, pasi që vonesat mund të rezultojnë me humbje të të dhënave. Si rrjedhojë ekziston një nevojë e përgjithshme për ta përshpejtuar trajtimin e kërkesave për NNJ në hetimin e krimeve kibernetike". Projektraporti po ashtu thekson se duhet të gjenden zgjidhje ndërkombëtare për t'i përmirësuar procedurat e NNJ me shtetet e treta, për shembull duke përdorimi i një formulari të kërkesave për sigurim të shpejtë të urdhrit në marrëveshje me autoritetet ekzekutuese të shtetit në fjalë, është përmendur si praktika më e mirë e identifikuar në një Shtet Anëtar. Në frymën e njëjtë, krijimi i kontakteve jozyrtare dhe personale me autoritetet kompetente të Shteteve të treta para dërgimit të një kërkesë për NNJ është

⁷⁴Komisioni i Ekspertëve për Vlerësimin e Masave kundër Pastrimit të Parave dhe Financimit të Terrorizmit (MONEYVAL):

http://www.coe.int/t/dghl/monitoring/moneyval/default_en.asp?expandable=0

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

⁷⁶Raportet e miratuara mund të gjenden në: <http://www.coe.int/da/web/octopus/blog/-/blogs/genval-evaluation-reports-on-cybercrime>

theksuar si praktikë e dobishme që mund të shpie te një bashkëpunim më i mirë dhe më i shpejtë për ekzekutimin e kërkesave të tilla zyrtare.⁷⁷

Rekomandimet në vazhdim u janë përcjellë Shteteve Anëtare:

- Shtetet Anëtare duhet ta përmirësojnë cilësinë e kërkesave të NNJ që i dërgojnë te vendet e tjera, sidomos për t'u siguruar se janë të plotësuar mjaftueshëm dhe për t'i shqyrtuar metodat e përsheptimit dhe rritjes së cilësisë së përgjigjeve në kërkesat për NNJ.
- Shteteve Anëtare u rekomandohet të forcojnë efikasitetin e procesit të komunikimit me Shtetet e tjera Anëtare dhe vendet e treta duke krijuar një sistem të regjistrimit dhe menaxhimit të të NNJ që e bën të mundshme përcjelljen e një rasti nga regjistrimi deri te dërgimi i përgjigjes te vendi kërkuar.
- Shtetet anëtare inkurajohen të përdorin më shpesh instrumentet e Eurojust, EJNI dhe Europol dhe të krijojnë kontakte joformale me autoritetet e huaja kompetente me qëllim që të sigurojnë përgjigje më të shpejta në kërkesat e tyre për NNJ nga vendet e treta.
- BE duhet të marrë në konsideratë përpjekjet për bashkërendim për ta krijuar një mënyrë efektive të komunikimit dhe ekzekutimit të kërkesave për NNJ nga Shtetet Anëtare të saj me shtetet joanëtare, ose për ta përcaktuar një kornizë për bashkëpunim të drejtpërdrejtë me ISP-të relevante që nuk janë anëtare të BE-së.
- BE duhet të punojë në gjetjen e zgjidhjeve për të përmirësuar dhe shpejtuar procesin e komunikimit mes Shteteve Anëtare dhe vendeve të treta, e sidomos Shteteve të Bashkuara, veçanërisht në lidhje me këmbimin e informatave operacionale dhe kërkesat për NNJ dhe ekzekutimin e tyre.

4.2.2.2 T-CY

Komiteti i Konventës së Këshillit të Evropës kundër krimeve kibernetike (T-CY) monitoron dhe zbaton Konventën e Budapestit kundër krimeve kibernetike dhe zhvillon standarde të mëtejme dhe shënime udhëzuese me qëllim të lehtësimit të shfrytëzimit efikas dhe zbatimit të Konventës së Budapestit edhe në frymën e zhvillimeve ligjore, teknologjike dhe të politikave.

4.2.2.2.1 Ndhma e ndërsjellë juridike

Ndhma e ndërsjellë juridike mbetet mjeti kryesor për të siguruar prova elektronike nga juridiksionet e huaja për shfrytëzim në procedurat penale vendore. Në dhjetor të vitit 2014, T-CZ kreu një vlerësim të funksionimit të dispozitave për ndihmë të ndërsjellë juridike të Konventës së Budapestit.⁷⁸ Ai erdhi në përfundim, mes tjerash, se procesi i ndihmës së ndërsjellë juridike (NNJ) në përgjithësi konsiderohet joefikas, e sidomos në lidhje me sigurimin e provave elektronike. Koha për përgjigje në kërkesa prej gjashtë në 24 muaj duket të jetë bërë normë. Kështu që hiqet dorë nga shumë kërkesa dhe hetime. Kjo ndikon negativisht në obligimin pozitiv të qeverive për të mbrojtur shoqëritë dhe individët kundër krimeve kibernetike dhe krimeve të tjera që përfshijnë prova elektronike.

⁷⁷Projektraporti përfundimtar i rrethit të shtatë të vlerësimeve të ndërsjella të "zbatimit dhe funksionimit praktik të politikave evropiane për parandalimin dhe luftimin e krimeve kibernetike", qershor 2017. Shih fq. 82-88. Gjendet në:

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

⁷⁸ T-CY(2013)17rev, 3 dhjetor 2014, raporti vlerësues T-CY: Dispozitat e Konventës së Budapestit për ndihmë të ndërsjellë juridike në rastet e krimeve kibernetike. Gjendet në:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>

Raporti i vlerësimit kishte nxjerrë edhe një përfundim se jo të gjitha llojet e të dhënave kërkohen me urgjencë të njëjtë: përkitazi me llojin e të dhënave që kërkohen, informatat për abonuesin janë veçuar si informatat që kërkohen më së shpeshti. Numri i madh i kërkesave për informata të tilla bëhet barrë e rëndë për autoritetet përgjegjëse për procesimin dhe ekzekutimin e kërkesave për NNJ dhe ngadalëson - e shpesh edhe e parandalon - ndjekjen penale. Kjo sugjeron se zgjidhja e sfidës rreth informatave për abonuesin do ta bënte NNJ më efikase.

Raporti T-CY ka identifikuar problemet e hasura si më poshtë:

- Koha, ngarkesa dhe kompleksiteti i procedurave të nevojshme për ta përgatitur ose ekzekutuar një kërkesë për NNJ
- Vonesat (6 - 24 muaj) në përgjigjet ndaj kërkesave në përgjithësi ose në lidhje me vende të caktuara
- Vonesat në sigurimin e të dhënave për abonuesit
- Refuzimi për të bashkëpunuar në vepra "të vogla" nga disa vende
- Refuzimi për të bashkëpunuar ose mospërgjigja nga disa vende
- Problemi i bashkëpunimit me pikat kontaktuese 24/7
- Mungesa e fletëpranimit se kërkesa për NNJ është pranuar ose se të dhënat janë ruajtur
- Kriteret e paqarta për kërkesat "urgjente"
- Problemi i gjuhës, cilësisë së përkthimit, terminologjisë së përdorur
- Kërkesat e pranura janë shumë të gjera për një numër të madh të dhënash
- Mospërputhjet mes sistemeve ligjore, siç janë kompetencat hetuese
- Kufizimet ligjore (mbrojtja e të dhënave)
- Refuzimi për bashkëpunim nga shteti i huaj pa kërkesë për NNJ. Megjithatë, kërkesa për NNJ kërkon informata dhe prova të mjaftueshme të cilat nuk mund të sigurohen pa bashkëpunimin e shtetit të huaj (rreth vicioz)
- Kërkesa mund të mos e përmbushë prapun ligjor ose kriteret formale të shtetit kërkues ose kërkesa nuk është e plotë ose pragu/standardi i kërkuar shumë i lartë
- Pamjaftueshmëria e ligjeve
- Mospërmbushja e kriterëve për kriminalitet të dyfishtë
- Nuk është dërguar kërkesa paraprake për ruajtje të të dhënave para dërgimit të kërkesës për NNJ për t'u siguruar se të dhënat janë ende në dispozicion
- Të dhënat nuk janë ruajtur edhe pse është dërguar kërkesa për ruajtje në shtetin e huaj
- Të dhënat nuk janë më në dispozicion në shtetin e huaj ose shtetin e vet
- Politikat e ndryshme nga provajderët për t'i vënë të dhënat në dispozicion
- Personi kontaktues për raste emergjente ose autoriteti kompetent në shtetin e huaj nuk dihet duke sfiduar identifikimin e shqetësimeve të autoritetit, p.sh. provajderi i uebhostingut.
- Mbingarkesa me kërkesa të tepërta
- Shkathtësi dhe njohuri të kufizuara teknike në lidhje me provat elektronike në Shtetin kërkues.
- Pushteti i kufizuar i policisë gjyqësore
- Pragu i "shkakut të mundshëm".

T-CY ka miratuar një pako rekomandimesh për ta bërë procesin e NNJ në lidhje me krimet kibernetike dhe provat elektronike më efikas përmes shfrytëzimit efektiv të dispozitave ekzistuese të Konventës së Budapestit kundër Krimeve kibernetike dhe të marrëveshjeve të tjera por edhe përmes propozimit të zgjidhjeve shtesë⁷⁹, siç janë:

⁷⁹ Shih fq. 125-127 të raportit vlerësues të T-CY: Dispozitat e Konventës së Budapestit për ndihmë të ndërsjellë juridike në rastet e krimeve kibernetike.

- Palët duhet t'i zbatojnë plotësisht kompetencat e Konventës së Budapestit (Rec 1) për ruajtje, ta monitorojnë efikasitetin e procesit për NNJ (Rec 2), të caktojnë më shumë staf dhe staf më të trajnuar dhe më shumë burime për NNJ (Rec 3 dhe 4), të forcojnë rolin dhe kapacitetet e pikave kontaktuese 24/7 (Rec 5), të përcaktojnë procedurat për raste emergjente (Rec 8), e kështu me radhë.
- Palët duhet të marrin në konsideratë - mundësisht përmes një Protokolli të Konventës së Budapestit - që të lejojnë zbulimin e përsheptuar të informatave për abonuesin (Rec 19), mundësinë e sigurimit të urdhrave ndërkombëtarë (Rec 20), bashkëpunimin e drejtpërdrejtë mes autoriteteve gjyqësore (Rec 21), adresimi i praktikave të sigurimit të drejtpërdrejtë të informatës nga provajderët e huaj të shërbimeve (Rec 22), hetimet e përbashkëta dhe/ose hetimet e përbashkëta dhe/ose ekipet e përbashkëta hetuese mes Palëve (Rec 23), që mundësojnë dërgimin e kërkesave në gjuhën angleze (Rec 24).

4.2.2.2.2 Sfida të tjera praktike

Disa sfida dhe aspekte të tjera që kanë të bëjnë me bashkëpunimin ndërkombëtar do të shtjellohen më në hollësi:

Kushtet për qasje të drejtpërdrejtë në të dhënat për përmbajtjen në kompjuterin e të dyshimit, madje edhe nëse të dhënat janë të ruajtura jashtë vendit dhe çështja e ndërlidhur e pëlqimit dhe juridiksionit

Në raportin përfundimtar të T-CY Cloud Evidence Group (CEG) qasja e drejtësisë penale në të dhënat në internet: Rekomandime për t'u marrë në konsideratë nga T-CY⁸⁰ është theksuar si rregull se kompetencat për zbatim të ligjit zakonisht përcaktohen nga parimi i territorialitetit. Sipas këtij parimi, asnjë shtet nuk mund të zbatojë juridiksionin e saj në territorin e një shteti tjetër sovran. Qasja e drejtësisë penale në të dhënat nëpër serverë ose sisteme kompjuterike që në përgjithësi ndodhen në juridiksione të tjera pa përfshirjen e autoriteteve të atyre juridiksioneve ngrit shqetësime.

Megjithatë, në rastet kur një kompjuter në një vend të ngjarjes ose i një personi që është nën hetim është "live" (është në punë dhe aktiv), autoritetet e drejtësisë penale teknikisht do të mund t'u qaseshin të dhënave (përfshirë ato që ruhen në serverë cloud) pa dijeninë e juridiksionit ku ndodhet serveri apo ku janë të ruajtura të dhënat. Neni 32b i Konventës së Budapestit ofron zgjidhje vetëm për disa situata shumë të kufizuara siç përshkruhen në Shënimin Udhëzues në miratuar nga T-CY në dhjetor 2014.⁸¹

Për shkak të kufizimeve të Nenit 32b të Konventës së Budapestit (pajtimi vullnetar i të dyshimit për qasje në llogarinë e emailit gjatë hetimit "live") disa shtete ndjekin zgjidhje të njëanshme në praktikë. Duket si praktikë e shprehur gjithandej se organet e rendit në një hetim të caktuar penal u qasen të dhënave jo vetëm në pajisjen e të dyshimit por edhe në pajisjet e tjera të kyçura siç janë emaili ose llogaritë e tjera të shërbimeve cloud nëse pajisja është e hapur ose kredencialet për qasje janë siguruar në mënyrë të ligjshme, madje edhe nëse e dinë se janë duke u lidhur me një vend tjetër, por të ditur.

⁸⁰ T-CY (2016)5, 16 shtator 2016, Qasja e drejtësisë penale në prova elektronike në internet (cloud): Rekomandime për t'u marrë në konsideratë nga T-CY. Gjendet në:

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

⁸¹ T-CY Shënim udhëzues #3 për qasje ndërkufitare (Neni 32), 3 dhjetor 2014, Gjendet në: <https://rm.coe.int/16802e726a>

CEG ka shqyrtuar doktrinën e kamotshme të ligjit të BE-së për konkurrencën (anti-trust) (Rastet *ICI* 48/69; *Woodpulp* 89/85) dhe ka vënë në pah se Komisioni Evropian rekomandon që autoritetet konkurruese brenda Bashkimit Evropian duhet të sigurojnë qasje në serverë kudo në botë për të mbledhur prova në procedurën konkurruese. Që të sigurohen kompetencat e vërteta për të mbledhur prova elektronike është e rëndësishme që autoritetet të jenë në gjendje t'i ushtrojnë kompetencat e tyre inspektuese për të mbledhur informata digjitale në të cilat ka qasje ndërmarrja apo personi, objektet e të cilëve janë duke u inspektuar, pavarësisht se ku ruhen ato, përfshirë softuerë ose mjete të tjera të ruajtjes së informatës jashtë territorit të autoritetit të caktuar konkurrues nacional ose jashtë Bashkimit Evropian. Kushtet dhe mbrojtjet për këtë qasje në të dhëna duhet të përkufizohen në një protokoll.

CEG ka nxjerrë përfundimin se një kornizë për qasje ndërkufitare duhet t'i përkufizojë kushtet dhe mbrojtjet për qasje të tillë në të dhëna me qëllim që të mbrohen të drejtat e individëve dhe të parandalohet paragjyrimi i kompetencave ose të drejtave të qeverive të tjera ose subjekteve të tyre.

Qasja në të dhënat për abonuesit

Të dhënat për abonusit janë më pak të ndjeshme për privatësinë dhe kërkojnë më së shpeshti. Urdhri i lëshuar nga policia ose prokuroria mjafton në shumë shtete, megjithatë disa kërkojnë edhe urdhër të gjykatës në raste të ndonjë IP dinamike, pasi që ajo përfshin disa të dhëna për trafikun.

Raporti përfundimtar i CEG për qasje të drejtësisë penale në prova elektronike në cloud ka rekomanduar:

- Pasi që informata për abonuesin është më pak e ndjeshme për privatësinë se të dhënat për trafikun dhe të dhëna për përmbajtjen, kushtet për sigurim të urdhrit për informata për abonuesin duhet t'i nënshtrohen një mbrojtje më të pakët sesa për llojet e tjera të të dhënave ose për llojet e tjera të kompetencave ndërhyrëse.
- Një regjim më i lehtë për sigurimin e informatave për abonuesin do t'i lehtësonte hetimet vendore dhe bashkëpunimin ndërkombëtar në kontekst të një cloud-i.

Janë shqyrtuar kushtet për ta përdorur një urdhër vendor (Neni 18 i Konventës së Budapestit) për të dhëna për abonuesin në raste të provajderëve të shërbimeve shumëkombëshe, që ofrojnë shërbime në territorin e një shteti, pavarësisht nga përfaqësia e tyre jashtë vendit dhe lokacionit të të dhënave.

Një autoritet i drejtësisë penale mund ose të hartojë legjislacion për ta zbatuar duke u përqendruar në lokacionin e sistemit kompjuterik ose të pajisjes së ruajtjes (kjo mbulohet nga dispozitat për kontroll dhe sekuestrim të Nenit 19 të Konventës së Budapestit) ose personit fizik apo juridik (përfshirë provajderët e shërbimeve) që kanë në posedim ose kontroll të dhënat e kërkuara.⁸² Kjo e fundit mbulohet nga Neni 18 për sigurim të urdhrit.

Ndihma e ndërsjellë juridike presupozon se lokacioni i të dhënave të kërkuara është i ditur dhe se është e realizueshme dhe e ditur se në cilin shtet dhe cilin autoritet kompetent të adresohet kërkesa për NNJ. Megjithatë, shpesh nuk është e qartë për një autoritet të drejtësisë penale se në cilin juridiksion ruhen të dhënat e kërkuara dhe/ose cili regjim

⁸² Shih për shembull, Direktivën e Bashkimit Evropian 2016/1148 për sigurinë e rrjeteve dhe sistemeve informative ("NIS Directive") të datës 6 korrik 2016, Neni 18 Juridiksioni dhe territorialiteti.

ligjor vlen për ato të dhëna. Një provajder i shërbimit mund ta ketë selinë në një juridiksion dhe ta zbatojë regjimin ligjor të një juridiksioni tjetër ndërsa të dhënat të jenë të ruajtur në një juridiksion të tretë. Të dhënat mund të pasqyrohen në disa juridiksione dhe të kalojnë nga një juridiksion në tjetrin. Nëse lokacioni i të dhënave përcakton juridiksionin, është e kuptueshme që një provajder i një shërbimi cloud t'i largojë të dhënat në mënyrë sistematike për ta parandaluar qasjen e drejtësisë penale.

Pasi që interneti nuk ka kufij, informatat për abonuesin që janë të nevojshme për një hetim mund të mbahen nga një provajder i një shërbimi "që i ofron shërbimet e tij brenda një territori" të një Pale ndonëse provajderi mund ta ketë selinë dhe informatat e kërkuara mund të jenë të ruajtura në juridiksione të tjera.

CEG mendon se interpretimi logjik i Nenit 18.1.b të Konventës së Budapestit ofron një zgjidhje. Autoritetet kompetente të një Pale duhet të jenë në gjendje të kërkojnë informata për abonuesin nga një provajder i shërbimit që ofron një shërbim në territorin e tyre pavarësisht se ku ruhen të dhënat dhe ku ndodhet provajderi. Shënimi udhëzues # 10 për sigurimin e urdhrit për informata për abonuesin⁸³ që është miratuar nga T-CY promovon një interpretim të tillë dhe zbatimin e Nenit 18 të Konventës së Budapestit. Një zbatim i tillë në mënyrë efektive u shmanget kërkesave për NNJ.

Shënimi udhëzues thekson se urdhri sipas Nenit 18.1.b mund të aplikohet në raste të caktuara në lidhje me abonues të caktuar, nëse provajderi i shërbimit është ka në posedim ose kontroll informatat për abonuesin dhe nëse provajderi i shërbimit "ofron shërbimin në territorin e Palës", në rastet kur:

- Provajderi i shërbimit ua mundëson personave në territorin e Palës që të abonohen në shërbimet e tij (dhe nuk e bllokun, për shembull, qasjen në ato shërbime); dhe
- i orienton aktivitetet e veta drejt këtyre abonuesve (për shembull, duke bërë reklama lokale ose duke reklamuar në gjuhën e territorit të Palës), ose i shfrytëzon informatat për abonuesin (ose të dhënat e ndërlidhura me trafikun) gjatë aktiviteteve të tij, ose bashkëvepron me abonuesit në atë Palë dhe
- dhe se informatat që duhet të sigurohen lidhen me shërbimet e një provajderi të ofruara në territorin e Palës.

Edhe akvendimi i Gjykatës Supreme të Belgjikës ka konfirmuar një interpretim të tillë duke vendosur që provajderi i shërbimit që funksionon në territorin e një shteti i nënshtrohet dhe duhet ta respektojë legjislacionin në fuqi në atë shtet. Gjykata Supreme e Belgjikës në rastin e Yahoo!⁸⁴ vendosi se një urdhër për urdhër për sigurim të informatave për abonuesin që i dorëzohet një provajderi që i ofron këto shërbime dhe që është i "pranishëm" në territorin e një Pale konsiderohet urdhër vendor (si në Nenin 18.1.b) e jo çështje e bashkëpunimit ndërkombëtar ose e ushtrimit të juridiksionit jashtë shtetit (ekstra territorial). Yahoo! Inc. ishte ankuar kundër një vendimi të mëhershëm të Gjykatës së Apelit në Antwerp më 20 nëntor 2013, mes arsyeve të tjera se sipas të drejtës

⁸³ Shënimi udhëzues #10: Sigurimi i urdhrave për informata për abonuesin (Neni 18 i Konventës së Budapestit), i miratuar sipas procedurës me shkrim nga T-CZ më 28 shkurt 2017. Gjendet në: <https://rm.coe.int/doc/09000016806f943e>

⁸⁴ Aktvendimi i Gjykatës Supreme të Belgjikës në rastin e Yahoo! Më 1 dhjetor 2015, Gjykata Supreme e Belgjikës ka nxjerrë një aktvendim përfundimtar rreth Yahoo! Inc. e regjistruar në Kaliforni, SHBA, është e obliguar t'i ofrojë informatat për abonuesin dhe u nënshtrohet rregullave detyruese të Nenit 46bis të Rregullave të Procedurës Penale të Belgjikës. Gjendet në gjuhën holandeze: http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1

ndërkombëtare zakonore një shtet nuk ka kompetenca të cilat mund t'i ushtrojë jashtë shtetit të vet.

Gjykata Supreme Belge vendosi që:

- Në përgjithësi, një shtet mund t'i zbatojë masat detyruese vetëm në territorin e vet, përndryshe do ta shkelte sovranitetin e një shteti tjetër.
- "Një shtet imponon një masë detyruese në territorin e vet për atë që ekziston një lidhje e mjaftueshme territoriale mes asaj mase dhe atij territori."
- Neni 46bis §2 i Rregullave Belge të Procedurës Penale "vetëm synojnë të zbatojnë mbi operatorët dhe furnizuesit që janë aktivë në Belgjikë një masë me qëllim të sigurimit vetëm të të dhënave identifikuese në raste në ndonjë krimi ose shkeljeje, hetimi i të cilave bie brenda kompetencave të autoriteteve të prokurorisë belge. Kjo masë nuk e paraqet si kriter praninë jashtë shtetit të policisë ose gjyqtarëve belgë, e as agjentëve që veprojnë në emër të tyre. Kjo masë po ashtu nuk kërkon ndonjë veprim ose akt të rëndësishëm jashtë vendit. Andaj kjo masë mbulon një fushëveprim dhe aspekt të kufizuar, ekzekutimi i së cilës nuk parasheh ndonjë intervenim jashtë territorit të Belgjikës".
- Yahoo! Inc., "si ofrues i shërbimit pa pagesë të uebmailit është e pranishme në territorin e Belgjikës dhe në mënyrë vullnetare i nënshtrohet ligjit të Belgjikës pasi që në mënyrë aktive merr pjesë në jetën ekonomike belge, në mënyrë specifike duke përdorur emrin e domenit 'www.yahoo.be', përdorë gjuhën lokale, bën reklama në lokacionet e përdoruesve të shërbimeve të saj dhe për shkak të mbulueshmërisë së këtyre përdoruesve në Belgjikë duke instaluar një kuti ankesash dhe një tryezë për pyetjet më të shpeshta (FAQ)."
- "Prokurori publik kërkon asgjë në Shtetet e Bashkuara nga një entitetet amerikan, por kërkon diçka në Belgjikë nga një entitet amerikan që ofron shërbime në territorin e Belgjikës".
- Andaj nuk ka ushtrim të juridiksionit ekstraterritorial.

Bashkëpunimi i drejtpërdrejtë me provajderët e shërbimeve shumëkombëshe

Bashkëpunimi me SHBA-të është i rëndësishëm parësor pasi që shumë provajderë të shërbimeve shumëkombëshe e kanë selinë atje dhe se numri i kërkesave për NNJ është në rritje. Raporti përfundimtar i CEG për qasje të drejtësisë penale në prova elektronike të ruajtura në cloud tregon se provajderët e shërbimeve në SHBA mund të zbulojnë informata për abonuesin dhe të dhëna për trafikun për autoritetet e huaja në bazë të kërkesës ligjore dhe se kjo është në përputhje me qëllimin e Nenit 18.1.b të Konventës së Budapestit. Megjithatë, ai vuri në pah se paqëndrueshmëria e politikave të provajderëve⁸⁵ dhe paparashikueshmëria e zbulimit shpie te mungesa e parashikimeve nga organet e rendit dhe nga klientët dhe paraqet probleme që lidhen me sundimin e ligjit.

Në rastin e provajderëve evropianë, një bashkëpunim i tillë nuk është i mundshëm për shkak të rregullave për mbrojtje të të dhënave, andaj duhet të bëhet kërkesa për NNJ.

Provajderët e shërbimeve në SHBA pranojnë kërkesat për ruajtje të çfarëdo të dhëne që pranohet drejtpërsëdrejti nga autoritetet e huaja në pritje se kjo do të pasohet nga një kërkesë për zbulim të tyre përmes NNJ. Provajderët evropianë nuk i pranojnë kërkesat për

⁸⁵Për një vështrim të përgjithshëm të politikave të provajderëve të ndryshëm shih qasjen e Drejtësisë penale në të dhënat në cloud: bashkëpunimi me provajderët e huaj të shërbimeve, T-CY Cloud Evidence Group, maj 2016. Gjetet në: <https://rm.coe.int/168064b77d>

ruajtje të pranuar drejtpërsëdrejti nga autoritetet e zbatimit të ligjit në juridiksione të tjera.

Procedurat emergjente

Rekomandimi 8 i Raportit të Vlerësimit të T-CY për ndihmë të ndërsjellë juridike deklaroi se Palët inkurajohen të krijojnë procedura emergjente për kërkesat që lidhen me rrezikun për jetën dhe rrethana të tjera urgjente. Një studim i kryer nga CEG⁸⁶ në vitin 2016, në të cilin morën pjesë 33 shtete, tregon se:

- Shumica e palëve nuk kanë legjislacion të miratuar që lejon zbulimin e të dhënave të autoritetet vendore të drejtësisë penale në raste emergjente;
- më pak se 20% kanë procedura të miratuara që ua lejojnë autoriteteve kompetente vendore të zbulojnë të dhëna për autoritetet e huaja në mënyrë të përsheptuar;
- vetëm dy palë ua kanë lejuar provajderëve të shërbimeve në territorin e tyre t'i zbulojnë të dhënat për autoritetet e huaja kompetente në raste emergjente.

CEG ka propozuar që të Rekomandimi 8 të adresohet edhe përmes një Protokollit të Konventës së Budapestit.

Protokollet shtesë të Konventës së Budapestit

CEG ka rekomanduar që të fillohen negociatat për një Protokoll shtesë të Konventës së Budapestit kundër krimeve kibernetike me qëllim që të mundësohet ndihmë e ndërsjellë juridike më efikase, të lehtësohet bashkëpunimi i drejtpërdrejtë me provajderët e shërbimeve në juridiksionet e tjera kur të jetë e nevojshme, në përputhje me kriteret dhe mbrojtjet, për t'i strukturuar dhe përcaktuar kushtet dhe mbrojtjet rreth praktikave ekzistuese të qasjes ndërkufitare në të dhëna dhe për t'i përcaktuar kriteret e mbrojtjes së të dhënave.

Një Protokoll shtesë i Konventës së Budapestit do të mund:

- Të qartësonte procedurat dhe kushtet për bashkëpunim të drejtpërdrejtë me provajderët e shërbimeve në juridiksione të tjera, si dhe pranueshmërinë e provave të pranuar në procedurë penale;
- Të krijonte bazën ligjore për kërkesa të drejtpërdrejta për ruajtje të provajderët e huaj të shërbimeve. Kjo veçse është bërë praktikë e pranuar nga provajderët e shërbimeve në SHBA;
- Të siguronte procedurat emergjente që lejojnë bashkëpunim të drejtpërdrejtë me provajderët e shërbimeve në juridiksionet e huaja në raste të caktuara emergjente.

Elementet e mundshme të një Protokollit:

- Dispozita për ndihmë të ndërsjellë juridike më efikase:

⁸⁶ Kërkesat emergjente për zbulim të menjëhershëm të të dhënave të ruajtura në një juridiksion tjetër përmes kanaleve të ndihmës së ndërsjellë juridike ose përmes kërkesave të drejtpërdrejta të provajderit të shërbimit, T-CY Cloud Evidence Group, maj 2016
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651a6f>

- një regjim i thjeshtësuar për kërkesa për ndihmë të ndërsjellë juridike për informata për abonuesin;
 - Sigurimi i urdhrave ndërkombëtar;
 - bashkëpunimi i drejtpërdrejtë mes autoriteteve gjyqësore në kërkesat për ndihmë të ndërsjellë juridike;
 - Hetime të përbashkëta dhe ekupe të përbashkëta hetuese;
 - Kërkesa në gjuhën angleze;
 - Dëgjim me audio/video të dëshmitarëve, viktimave dhe ekspertëve;
 - Procedura emergjente për NNJ.
- Dispozita që mundësojnë bashkëpunim të drejtpërdrejtë me provajderët e shërbimeve në juridiksionet e tjera në lidhje me kërkesat për informata për abonuesin, kërkesa për ruajtje dhe kërkesa emergjente.
 - Kornizë më të qartë dhe mbrojtje më të mira për praktikën ekzistuese të qasjes ndërkufitare në të dhëna.
 - Mbrojtje, përfshirë kriteret për mbrojtje të të dhënave.

Termat e referencës për përgatitjen e një drafti të dytë të Protokollit Shtesë të Konventës së Budapestit kundër krimeve kibernetike u miratuan në takimin e 17-të plenar të T-CY në qershor 2017.⁸⁷

4.3 Përdorimi i shabllonëve dhe formularëve për Ndhimë të ndërsjellë juridike

Kërkesat për NNJ ndryshojnë, madje edhe nëse ato bazohen në instrumente të së drejtës ndërkombëtare, pasi që ato varen nga legjislacioni shtetëror i vendit që i dërgon, si dhe nga legjislacioni dhe pritjet praktike të shtetit që i pranon ato. Formularët e kërkesave për NNJ mund t'u ndihmojnë shteteve deri në njëfarë mase andaj edhe janë bërë përpjekje për t'i krijuar disa modele të shablloneve.

Komiteti i Këshillit të Evropës PC-OC ka krijuar në vitin 2016 një Model të formularit të kërkesës për ndihmë të ndërsjellë juridike në çështje penale⁸⁸.

T-CY në Raportin e Vlerësimit të vitit 2014 të dispozitave të ndihmës së ndërsjellë juridike të Konventës së Budapestit kundër krimeve kibernetike në Rekomandimin 17 deklaroi se Këshilli i Evropës duhet - përmes projekteve për ngritje të kapaciteteve - t'i krijojë ose të lidhet me shabllonët në shumë gjuhë për kërkesat që bëhen në përputhje me Nenin 31⁸⁹.

Përfundimet e Këshillit të BE në lidhje me përmirësimin e drejtësisë penale në hapësirën kibernetike (qershor 2016), mes tjerash, i bëjnë thirrje Komisionit, që në bashkëpunim me

⁸⁷ T-CY(2017)3 Termat e referencës për përgatitjen e draftit të dytë të Protokollit Shtesë të Konventës së Budapestit kundër krimeve kibernetike, qershor 2017. Gjetet në: <https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-protocol/168072362b>

⁸⁸ Shih dokumentet nga takimi i 69-të (maj 2016): Një draft i kërkesës model për NNJ dhe udhëzime praktike për profesionistët: <http://www.coe.int/en/web/transnational-criminal-justice-pcoc/pc-oc-69th-meeting>
<http://www.coe.int/en/web/transnational-criminal-justice-pcoc/model-request-form-for-mutual-assistance-in-criminal-matters>

⁸⁹ Dispozitat e Konventës së Budapestit për ndihmë të ndërsjellë juridike në rastet e krimeve kibernetike, 3.12.2014 (T-CY(2013)17rev).
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>

shtetet anëtare, Eurojust dhe vendet e treta të marrin në konsideratë dhe të bëjnë rekomandime se si të përshtaten, aty ku shihet e udhës, formularët dhe procedurat e standardizuara për të kërkuar ruajtjen dhe sigurimin e provave elektronike.

Një shembull i një formulari të një urdhri për konfiskim mund të gjendet në vendimin Kornizë të Këshillit 2006/783/JHA të datës 6 tetor 2006 për zbatimin e parimit të njohjes së ndërsjellë të urdhrave për konfiskim⁹⁰.

Shembull tjetër është Direktiva 2014/41/EU e Parlamentit Evropian dhe e Këshillit e datës 3 prill 2014 në lidhje me Urdhrin Evropian për Hetime në çështje penale⁹¹.

Në fund, UNODC ka zhvilluar një instrument për hartimin e kërkesave për Ndihmë të Ndërsjellë Juridike⁹².

Është evidente se qasjet tradicionale të NNJ nuk janë më adekuate në një botë globale të krimit kibernetik. Vetëdijesimi rreth mundësive dhe sfidave që dalin nga të dy instrumentet e Këshillit të Evropës: Konventës së Budapestit (p.sh. qasja në të dhëna në cloud) dhe Konventën e Varshavës (ekzekutimi i urdhrave për ngrirje dhe konfiskim) do t'i kontribuojë rezultateve më të mira gjatë kombinimit të hetimit të krimeve kibernetike dhe hetimit paralel financiar.

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 Valutat virtuale

Kriptovalutat, e në veçanti Bitcoin, mbesin valutat e preferuara për shumë krime kibernetike, qoftë kur ato përdoren për pagesë të shërbimeve kriminale ose për të pranuar pagesa nga viktimat e zhvatura. Madje edhe anëtarë kyç të komunitetit të Bitcoin, siç janë këmbyesit, po e gjejnë veten përherë e më shumë si viktimat të kriminelëve kibernetikë⁹³. Pas prezantimit të valutave virtuale në kursin bazik, kursi i avancuar ofron informata më të hollësishme rreth funksionimit të valutave virtuale (e sidomos të Bitcoin) dhe një diskutim të rreziqeve që shoqërojnë përdorimin e këtyre valutave virtuale. Ky kapitull paraqet disa konstatime rreth sfidave hetuese dhe të ngrirjes/sekuestrimit të cilat janë përjetuar me valutat virtuale.

5.1 Përmbledhje e kursit bazik

Në bazë të përkufizimeve FATF⁹⁴, kursi bazik ka përkufizuar termet dhe kategoritë në vazhdim që kanë të bëjnë me valutat virtuale:

- Valutat virtuale
- Paratë elektronike/e-money
- Valutat digjitale
- Valutat virtuale të konvertueshme në raport me valutat e pakonvertueshme
- Valutat virtuale të centralizuara në raport me ato të decentralizuara

Këto terme janë të përmbledhura në tabelën e mëposhtme.

Valutat virtuale	“Valuta virtuale është një përfaqësim digjital i vlerës që mund të tregtohet në internet dhe që mund të funksionojë si (1) mjet këmbimi; dhe/ose (2) një njësi llogaritëse; dhe/ose (3) një rezervë me vlerë, por që nuk e ka statusin e monedhës ligjore në asnjë juridiksion”
Paratë elektronike/e-money	“Valutat virtuale ndryshojnë nga paratë elektronike (e-money), të cilat janë një përfaqësim digjital i valutës së shtypur që përdoret për ta bartur në mënyrë elektronike vlerën që
Valutat digjitale	“Valuta digjitale mund të nënkuptojë një përfaqësim digjital ose të valutës virtuale (që nuk është e shtypur) ose të parave elektronike (të shtypura) dhe kjo shpesh përdoret në vend të termit valutë virtuale.”
Valutat virtuale të konvertueshme në raport me valutat e pakonvertueshme	Valutat e konvertueshme virtuale (të hapura) kanë një vlerë ekuivalente në valutat reale dhe mund të këmbehen në të dy drejtimet me valutat reale. Valutat e pakonvertueshme virtuale (të mbyllura) synohen të jenë specifike për një domen ose botë të caktuar virtuale dhe sipas rregullave që drejtojnë përdorimin e tyre, nuk mund të këmbehen me valutën e shtypur.
Valutat virtuale të centralizuara në raport me ato të decentralizuara	Valutat virtuale të centralizuara kanë një autoritet të vetëm administrues (administratorin) - do të thotë një palë të tretë që e kontrollon sistemin. Administratori e lëshon në qarkullim një

⁹³ Vlerësimi i Kërcënimit nga Krimi i Organizuar në Internet (IOCTA), Europol, 2016 Gjendet në: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016>

⁹⁴ Raporti FATF, Përkufizimet Kryesore për Valutat virtuale rreziqet e mundshme për LPP/LFT, qershor 2014. Gjendet në: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

decentralizuara	valutë, i përcakton rregullat për përdorimin e saj, e mirëmban një libër qendror të llogaritjes së pagesave dhe e ka autoritetin ta tërheqë nga tregu valutën (ta tërheqë nga qarkullimi). Valutat virtuale të decentralizuara janë valuta virtuale të shpërndara, me burime të hapura, të bazuara në llogaritje matematikore, nga personi në person, të cilat nuk e kanë një autoritet qendror administrues dhe nuk kanë monitorim ose mbikëqyrje qendrore.
------------------------	--

5.2 Hyrje në valutat virtuale

5.2.1 Terminologji më e zgjeruar e valutave virtuale⁹⁵

Kriptovalutat	U referohen valutave të decentralizuara të mbështetura në llogaritje matematikore të cilat mbrohen nga kriptografia - do të thotë, që përfshijnë parimet e kriptografisë për ta zbatuar një ekonomi informative të klasifikuar, të decentralizuar dhe të sigurt. Kriptovalutat mbështeten në çelësa publikë dhe privatë për ta transferuar vlerën nga një person në një tjetër (qoftë person apo entitet) dhe duhet të nënshkruhet në mënyrë kriptografike sa herë që bëhet transferi. Siguria, integriteti dhe baraspesha e librave të llogarive të kriptovalutave sigurohen përmes një rrjeti të palëve të cilat nuk i besojnë njëra tjetrës (në Bitcoin njihen si minatorë) të cilët e mbrojnë rrjetin në këmbim të mundësisë për të siguruar një tarifë të shpërndarë pa ndonjë rregull të caktuar (në Bitcoin, një numër të vogël të bitcoin-ëve të sapokrijuar, të quajtur "shpërblimi në bllok" dhe në disa raste edhe tarifën për transaksione të paguara nga përdoruesit si një nxitje për minatorët (miners) për t'i përfshirë transaksionet e tyre në bllokun e radhës). Janë përkufizuar me qindra specifikacione të kriptovalutave, kryesisht që rrjedhin nga Bitcoin, i cili përdor një sistem të verifikimit të punës (proof of work) për të vlerësuar transaksionet dhe për ta ruajtur zinxhirin e bllokut. Ndonëse Bitcoin ka siguruar protokollin e parë të zbatuar plotësisht të kriptovalutës, ekziston një interesim në rritje për të zhvilluar metoda alternative, mundësisht më efikase e të sigurta, siç janë sistemet e bazuara në verifikimin e gatishmërisë për të rrezikuar (proof of stake).
Bitcoin	I lansuar në vitin 2009, ishte valuta e parë virtuale e konvertueshme e decentralizuar dhe kriptovaluta e parë. Bitcoins janë njësi të llogarive të bëra nga vargje unike të numrave dhe shkronjave që përbëjnë njësi të valutës dhe të cilët kanë vlerë vetëm pse përdoruesit janë të gatshëm të paguajnë për to. Bitcoin-ët tregtohen në mënyrë digjitale mes përdoruesve me shkallë të lartë të fshehtësisë dhe mund të këmbehen (blihen ose të shiten) me dollarë amerikanë, euro ose valuta të tjera të shtypura ose virtuale.
Etherumi	Kriptovaluta e vetme (me përjashtim të degëzimit të saj Ethereum Classic) që ngërthen në vete një gjuhë të plotë programuese. Kjo mund të përdoret për të lidhur kontrata të mençura - skripta

⁹⁵ Raporti FATF, Përkufizimet Kryesore për Valutat virtuale rreziqet e mundshme për LPP/LFT, qershor 2014. Gjetet në: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

		vetëekzekutuese, kur një pagesë dërgohet pasi të plotësohen kushtet e paracaktuara.
Altcoin		I referohet valutës së konvertueshme të decentralizuar të bazuar në llogaritje matematikore, valutën e tillë origjinale. Shembujt përfshijnë Ripple, PeerCoin, Lite-Coin, zerocoin, anoncoin dhe dogecoin.
Monero		E krijuar në prill të vitit 2014, ajo është një kriptovalutë me burim të hapur që mbase ofron shkallën më të lartë të privatësisë duke përdorur disa teknologji të cilat e bëjnë gjurmimin tradicional joefikas, pasi që si adresa dërguese ashtu edhe ajo pranuese janë të paqarta. Edhe shuma e transaksionit është e fshehur. Andaj kështu sigurohen karakteristikat e privatësisë së transaksioneve.
Nyjet		Një klient i cili përhap transaksionet nga rrjeti i bitcoin te nyjet e tjera.
Çelësi privat		Çelësi sekret mundëson kryerjen e një transaksioni me bitcoin dhe përdoret për ta krijuar një nënshkrim për një transaksion që nuk mund të falsifikohet. Pronari i çelësit privat i kontrollon bitcoin-ët.
Çelësi publik		Një çelës i njohur publik që buron nga një çelës privat.
Transaksioni me bitcoin		Bitcoin-ët kalojnë nga një adresë në tjetrën. Kur të kryhet një transaksion përdoruesi e shfrytëzon një kuletë Bitcoin të instaluar në kompjuterin e tij ose një shërbim elektronik që ofron funksionalitetet relevante. Transaksioni me bitcoin është transaksion që kryhet një herë dhe nuk mund të kthehet prapa. Transaksionet me bitcoin janë transparente dhe mund të shihen në internet në shumë mënyra. Të dhënat mund të shikohen, siç janë adresa e dërguesit të Bitcoin, adresa e pranuesit të Bitcoin dhe shumë e bitcoin-ëve të përfshirë në transaksion.
Sekuestrimi		Kalimi i bitcoin-ëve nga një adresë e të dyshimit në një adresë të kontrolluar nga organet e rendit.
Anonimuset (instrumenti i anonimitetit)	i	U referohet instrumenteve dhe shërbimeve të dizajnuara për ta turbulluar burimin e transaksionit me bitcoin dhe për ta lehtësuar anonimitetin.
Mikseri (shërbimi i pastrimit, tumbler)	i	Është emri që i është dhënë një lloji të anonimitetit që e turbullon zinxhirin e transaksioneve në blockchain duke i lidhur të gjitha transaksionet në një adresë të vetme të bitcoin dhe duke i dërguar ato bashkë në një mënyrë që i bën të duken sikur janë dërguar nga një adresë tjetër. Një mikser ose tumbler i dërgon transaksionet përmes një vargu kompleks, gjysmë të rastësishëm të transaksioneve që e bën jashtëzakonisht të vështirë lidhjen me monedhat e caktuara virtuale (adresat) me një transaksion të caktuar. Shërbimet e mikserit veprojnë duke pranuar udhëzime nga një dërgues për t'i dërguar fonde në një adresë të caktuar të bitcoin-it. Shërbimi i miksimit pastaj i "përzien" këtë transaksion me transaksionet e tjera të përdoruesit, në mënyrë që e bën të paqartë te kush e ka menduar dërguesi t'i orientojë fondet.
Tor (Ruteri qepë)		Quhet një rrjet nëntokësor i kompjuterëve të shpërndarë në internet që i fsheh adresat e vërteta të IP-së, si rrjedhojë edhe identitetet e përdoruesve të rrjetit duke e përçuar komunikimin nëpër kompjuterë të shumëfishtë nëpër botë dhe duke e mbështjellë atë me nivele të shumta të enkriptimit.
Kuleta e zezë		Quhet një kuletë e zgjeruar e mbështetur në brauzer që kërkon të sigurojë fshehtësinë e transaksioneve me bitcoin duke inkorporuar karakteristikat në vazhdim: auto-anonimuesin (mikserin), tregtinë

	e decentralizuar, platforma të pacensuruara të financimit të turmave, platformat e stoqeve dhe tregjet e zeza të informatave dhe vendet e tregjeve të decentralizuara siç është Silk Road.
Ruajtja e ftohtë	I referohet një kulete offline të bitcoin-ëve - do të thotë një kulete që nuk është e lidhur në internet. Ruajtja e ftohtë mendohet të ndihmojë mbrojtjen e valutave të ruajtura virtuale kundër piraterisë informative (hakimit) dhe vjedhjes.
Ruajtja e nxehtë	I referohet një kulete elektronike (online) të bitconi-ëve - e kundërta e Ruajtjes së ftohtë.
Sistemi lokal i tregtisë këmbyses (LETS)	Është një organizatë ekonomike që funksionon në brenda një lokacioni që u mundëson anëtarëve të këmbjnë mallra dhe shërbime me të tjerët brenda grupit. LETS përdor një valutë të krijuar lokale për t'i emërtuar njësitë e vlerës të cilat mund të tregtohen ose këmben me mallra ose shërbime. Në teori, bitcoin-ët do të mund të miratoheshin si valuta lokale e përdorur me LETS

5.2.2 Pjesëmarrësit në valuta virtuale

Këmbyesi (njihet edhe si këmbyes i valutave virtuale)	Është një person ose entitet i angazhuar si biznes për këmbimin e valutave virtuale me valuta reale, fonde, ose forma të tjera të valutave virtuale dhe metaleve të çmuara dhe anasjelltas për një pagesë (përqindje). Këmbyesit në përgjithësi pranojnë një varg të gjerë të pagesave përfshirë para të thata, transfere elektronike, kartela kreditore, ose valuta të tjera virtuale dhe mund të jetë ose mos jetë i ndërlidhur me administratorin, ose të jetë një provajder i palëve të treta. Këmbyesit mund të shërbejnë si bursë ose si një zyre këmbimore. Personat në mënyrë tipike i shfrytëzojnë këmbyesit për të depozituar ose tërhequr para nga llogaritë e valutave virtuale.
Administratori	Është një person ose entitet i angazhuar në biznesin e lëshimit në qarkullim të një valute virtuale të centralizuar, caktimit të rregullave për përdorimin e saj, mirëmbajtjen e një libri qendror të pagesave dhe ta caktojë se kush e ka autoritetin ta tërheqë (nga qarkullimi) valutën virtuale.
Përdoruesi	Personi ose entiteti që e siguron valutën virtuale dhe e përdorë atë për të blerë të mira virtuale ose reale ose shërbime ose që dërgon transfere në cilësinë personale të një person (për përdorim personal), ose i cili i mban valutat virtuale si investim (personal).
Minatori	Është një person ose entitet i cili merr pjesë në një rrjet të decentralizuar të valutave virtuale duke udhëhequr një softuer të veçantë të algoritmave komplekse në një sistem të shpërndarë të verifikimit të punës (proof-of-work) ose ndonjë sistem tjetër të verifikimit të transaksioneve në sistemin e valutave virtuale. Minatorët mund të jenë përdorues nëse ata gjenerojnë vetë valuta të konvertueshme virtuale për qëllime të veta. Minatorët po ashtu mund të marrin pjesë në një sistem të valutave virtuale si këmbyes, duke krijuar valutën virtuale si biznes, me qëllim që ta shesin atë për valuta reale ose për valuta të tjera virtuale.
Kuleta e valutave virtuale (klienti)	Është një mjet (aplikacion softuerik ose tjetër) për mbajtje, ruajtje dhe transferim të bitkoinëve ose të valutave të tjera virtuale.

Provajderi i kuletës Është një entitet që e siguron kuletën e valutës virtuale për mbajtje, ruajtje dhe transferim të bitcoinëve ose të valutave të tjera virtuale. Kuleta përmban çelësin privat të përdoruesit që i lejon përdoruesit t'i shpenzojë valutat virtuale të cilat janë shpërndarë në adresën e valutës virtuale në atë zinxhir blloku (blockchain). Ofruesi i një kulete lehtëson pjesëmarrjen në sistemin e valutave virtuale duke u mundësuar përdoruesve, këmbyesve dhe tregtarëve që të kryejnë më lehtë transaksionet e valutave virtuale. Ofruesi i kuletës e ruan baraspeshën e valutës virtuale të klientit dhe në përgjithësi ofron edhe ruajtje dhe siguri të transaksioneve.

Edhe entitete të tjera të ndryshme mund të marrin pjesë në sistemin e valutave virtuale dhe mund të jenë të ndërlidhura me këmbyes dhe/ose administratorë ose mund të jenë të pavarura. Këto përfshijnë, mes tjerash, provajderë të shërbimit për administrim të rrjetit (do të thotë administratorët e rrjetit), procesorë të pagesave të palëve të treta (që lehtësojnë pranimin e një tregtari), krijues të softuerëve dhe ofrues të aplikacioneve.

5.2.3 Bitcoin

Bitcoin është një rrjet pagese i decentralizuar nga një person te tjetri i cili fuqizohet nga përdoruesit pa ndonjë autoritet qendror ose pa ndërmjetësues. Satoshi Nakamoto publikoi specifikat e para të Bitcoin dhe prova të konceptit në një listë adresash të kriptografisë në vitin 2009⁹⁶. Në thelb, qëllimi i operimit të rrjetit Bitcoin ka të bëjë me menaxhimin dhe ndarjen e një libri publik të llogarive, të njohur si "blockchain". Ky libër llogarish përmban çdo transaksion që është kryer ndonjëherë dhe përdoret për ta verifikuar vlefshmërinë e çdo transaksioni⁹⁷. Integriteti dhe rendi kronologjik i transaksioneve në librin e llogarive zbatohen përmes kriptografisë. Bitcoinët janë një valutë virtuale e konvertueshme dhe e decentralizuar, zakonisht e njohur si kripto valutë.

Kjo pjesë ofron një përshkrim se si funksionon valuta virtuale Bitcoin.

5.2.3.1 Transferimi i vlerës

Pyetja më e evidente rreth një valute virtuale është si e bartin përdoruesit vlerën e valutës te njëri tjetri. Në rastin e Bitcoin, çdo përdorues ka një ose më shumë adresa të Bitcoin. Një përdorues mund të krijojë sa të dëshirojë adresa të Bitcoin, madje edhe adresa të veçanta për secilin transaksion nëse dëshirojnë. Në praktikë, softueri i Bitcoin dhe shërbimet përfaqësojnë bitcoinët e një përdoruesi të cilat ruhen në një "kuletë". Një kuletë mund ta përfaqësojë një adresë të vetme të bitcoin ose adresa të shumëfishta, varësisht nga karakteristikat specifike të atij softueri ose shërbimi. Adresa shërben si një vlerë unike identifikuese e cila përdoret për ta përfaqësuar pronësinë e një bitcoin të veçantë⁹⁸. Që Personi A të dërgojë para te Personi B, ata i dërgojnë një porosi rrjetit të Bitcoin që përmban ID-në e adresës së dërguesit, ID-në e adresës së pranuesit ("adresën e pranuesit") dhe shumën e transferit të shprehur në bitcoin. Çdo njeje në rrjetin Bitcoin që e pranon këtë porosi do ta përditësojë kopjen e tyre të librit të llogarive dhe pastaj do ta përcjellin mesazhin e transaksionit te nyjet e tjera.

⁹⁶ <https://bitcoin.org/en/faq>

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

⁹⁸ Më saktësisht, çdo adresë është një çift i çelësit privat/publik. Çelësi publik është "adresa". Çelësi privat mbahet sekret dhe përdoret për të nënshkruar transaksionet në mënyrë digjitale përfshirë edhe adresën, me qëllim që të verifikohet autenticiteti i transaksionit.

Për ta parandaluar një sulmues, Personin C, që ai të dërgojë një porosi duke u përpjekur të transferojë bitcoinët nga kuleta e Personit A te kuleta e Personit C, autenticiteti i transaksioneve sigurohet përmes pranisë së nënshkrimit digjital nga Personi A. Për t'u kryer një mesazh për një transaksion të vlefshëm të bitcoinëve nga kuleta e Personit A, personi që e bën mesazhin duhet ta ketë fjalëkalimin që lidhet me çelësin privat të kuletës.

5.2.3.2 Vërtetimi i pronësisë

Si mundet pranuesi, Personi B, në shembullin e mësipërm, ta dijë se bitcoinët që po pranohen në të vërtetë i përkasin Personit A? Me qëllim që ta krijojë një mesazh të vlefshëm për transferim të bitcoinëve, dërguesi i bitcoinëve duhet ta dëshmojë se ata janë pronarë aktualë të atyre bitcoinëve.

Ta zëmë se Personi A po i dërgon pesë bitcoin Personit B. Personi A duhet të përfshijë në transaksion, referencat e transaksioneve të mëhershme ku pranuesi i transaksionit ka qenë Personi A dhe se vlera e përgjithshme të transaksioneve të mëhershme ka qenë më e madhe se pesë bitcoin. Këto njihen si "inputet" (hyrjet) e transaksionit.

Të gjithë përdoruesit e rrjetit bitcoin mbajnë një kopje të librit të llogarive ("block chain") që përmban historikun e të gjitha transaksioneve të mëhershme. Kështu Personi B mund të verifikojë se bitcoinët e përmendur në të dhënat e transaksionit të Personit A i takojnë me të vërtetë Personit A. Për ta thjeshtësuar procesin, ekziston një rregull se transaksionet duhet të jenë në baraspeshë. Me fjalë të tjera, numri i bitcoinëve në "inputet" e transaksionit duhet të jetë i barabartë me numrin e bitcoinëve në "outputet" (daljet) e transaksionit. Nëse ekziston mungesë ekuilibri, atëherë Personi A mund t'ia transferojë vetes pjesën e mbetur të hyrjeve.

5.2.3.3 Shpenzimi i dyfishtë

Në një rrjet nga personi në person siç është rrjeti Bitcoin, nuk ka garanci se rendi i transaksioneve të pranuar nga një nyjë e caktuar në rrjet përfaqëson rendin e njëjtë me të cilin janë krijuar. Në praktikë, kjo paraqet mundësinë që Personi A të krijojë një mesazh për transaksion për t'ia dërguar bitcoinët Personit B dhe në të njëjtën kohë ta krijojë mesazh për një transaksion të dytë për t'ia dërguar bitcoinët dikujt tjetër. Kjo njihet si shpenzim i dyfishtë. Është krejtësisht e mundshme që disa nyje në rrjetin Bitcoin ta pranojnë transaksionin e dytë së pari. Kur të arrijë transaksioni i parë te këto nyje, dikur më vonë, ai konsiderohet i pavlefshëm pasi që ai i ripërdor inputet të cilat veçse janë përdorë, nga këndvështrimi i tyre, në një transaksion tjetër. Përparësia kyçe teknologjike e protokollit të bitcoinëve është mekanizmi përmes të cilit zgjidhet kjo çështje.

Transaksionet mblidhen në grupe, të njohur si blloqe, dhe blloqet lidhen mes veti për ta krijuar së bashku një zinxhir blloku (block chain). Transaksionet brenda një blloku konsiderohet se ndodhin në të njëjtën kohë. Blloqet janë të renditura sipas faktit se secili bllok i referohet bllokut paraprak në zinxhir. Transaksionet të cilat ende nuk janë në bllok quhen "të pakonfirmuara". Secila nyje në rrjet mund të mbledhë një varg të transaksioneve të pakonfirmuara, t'i grumbullojë ato në një bllok dhe t'i propozojë si bllokun e radhës në zinxhir. Blloku i propozuar duhet ta përmbajë zgjidhjen e një problemi të ndërlikuar matematikor i cili është vështirë të llogaritet me kompjuter⁹⁹. Rrjeti bitcoin

⁹⁹Nyja që e krijon bllokun duhet të gjejë një vlerë numerike, e cila kur të kombinohet me të dhënat e tjera në bllok, u jep të dhënave të kombinuara që përfitohen një përzierje kriptografike me një vlerë nën një prag të caktuar.

në mënyrë dinamike e përshtat vështirësinë e problemit matematikor, kështu që një bllok i ri i shtohet zinxhirit mesatarisht çdo dhjetë minuta¹⁰⁰.

Ndonëse ka pak të ngjarë, mund të ndodhë që nyje të shumta në rrjetin Bitcoin mund të propozojnë blloqe thuajse në të njëjtën kohë. Në këtë rast zinxhiri i blloqeve degëzohet përkohësisht pasi që nyje të ndryshme në rrjet shtojnë blloqe të ndryshme në zinxhirin e blloqeve. Situata zgjidhet kur shtohet blloku i radhës në zinxhir. Siç është përmendur tashmë, blloku i ri përmban një referencë të bllokut paraparak në zinxhir. Andaj ai do t'i shtohet njëres nga degët e mundshme në zinxhir, duke e bërë njëren degë më të gjatë se tjetrën. Rregulli i rrjetit Bitcoin është se nyjet duhet të kalojnë te dega më e gjatë në dispozicion dhe si rezultat zinxhiri i bllokut stabilizohet shumë shpejt. Për më tepër, të gjitha nyjet do të pajtohen për të gjitha blloqet të cilat kanë mbetur mbrapa nga fundi i zinxhirit. Andaj konsiderohet më e sigurt të pritët pak kohë para se të transferohen mallrat në bazë të një transferi me bitcoin. Pasi që çdo bllok i duhen mesatarisht rreth dhjetë minuta të shtohet në zinxhir, pritja për gjashtë blloqe nënkupton një pritje prej një ore.

5.2.3.4 Minimi

Procesi i përshkruar më lart i ndërtimit të blloqeve dhe i shtimit të tyre në zinxhirin e blloqeve njihet si minim. Kushdo që e zgjidh bllokun dhe e shton në zinxhir të bllokut pranon një shpërblim prej 25 bitcoinësh. Shpërblimi për krijim të blloqeve përgjysmohet çdo katër vjet deri kur një ditë nuk do të lëshohen më bitcoin në qarkullim. Do të krijohet një total prej 21 milionë bitcoin.

Përveç shpërblimit për bitcoin, minatorët po ashtu do të pranojnë një tarifë për transaksionin e cila ka mundësi të përfshihet me transaksione. Aktualisht shpërblimi kryesor për minim është shpërblimi i krijimit të bllokut por me kohë edhe tarifat për transaksione mund të bëhen joshje për minim.

Pjesa më e madhe e minimeve nuk kryhet nga individët, por më shumë nga grupe të minatorëve, të njohur si ekipe minatorësh. Shpërblimi për blloqet e llogaritura ndahet mes anëtarëve të ekipit në raport me përpjekjet llogaritare që çdo anëtar i ka siguruar në ekip.

5.3 Rreziqet e valutave virtuale

Valutat virtuale e konvertueshme të cilat mund të këmbehen me para të vërteta ose me valuta të tjera virtuale kanë mundësi të keqpërdoren për pastrim të parave dhe për financim të terrorizmit për shumë arsye. Ky kapitull do t'i përshkruajë rreziqet të cilat janë numëruar në lidhje me këto dy kërcënime ndaj integritetit financiar¹⁰¹.

Së pari, ato mund të mundësojnë anonimitet më të madh se metodat e tjera të pagesës tradicionale pa para të thata. Sistemet e valutave virtuale mund të tregtohen në internet dhe në përgjithësi karakterizohen me raporte të cilat nuk i vënë klientët ballë për ballë dhe mund të lejojnë financime anonime (financime me para të thata ose financime të palëve të treta përmes këmbyesve anonimë të cilët nuk i identifikojnë në mënyrën e duhur burimet

¹⁰⁰Kjo arrihet duke reduktuar vlerën e pragut në kalkulimin e përzierjes, do të thotë se ekziston një numër më i vogël i përgjigjeve të pranuar, gjë që e bën identifikimin e një vlerë të vërtetë më të vështirë.

¹⁰¹Një dokument i shkëlqyeshëm është përgatitur nga Autoriteti Evropian për Shërbime Bankare (EBA) rendit rreziqet që paraqesin valutat virtuale për sistemin financiar. Gjetet në: <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>

financiare). Ato po ashtu mund të lejojnë transfere anonime, nëse dërguesi dhe pranuesi nuk identifikohen në mënyrën e duhur. Sistemet e decentralizuara janë veçanërisht të ndjeshme ndaj rreziqeve të anonimitetit. Për shembull, për nga modeli, adresat e Bitcoin, të cilat funksionojnë si llogari, nuk kanë emra ose identifikime të tjera të klientëve dhe sistemi nuk ka server qendror apo provajder të shërbimit. Protokollin e Bitcoin nuk kërkon ose nuk ofron identifikim dhe verifikim të pjesëmarrësve ose nuk gjeneron të dhëna për historikun e transaksioneve të cilat doemos ndërlidhen me identitetin e botës reale.

Nuk ka ndonjë organ qendror të mbikëqyrjes dhe nuk ka softuer kundër pastrimit të parave që është në dispozicion aktual për të monitoruar dhe për të identifikuar mostrat e dyshimta të transaksioneve. Organet e rendit nuk mund të përqendrohen në një lokacion qendror ose një entitet (administrator) për qëllime hetimore ose të sekuestrimit të pasurisë (ndonëse autoritetet mund të përqendrohen në këmbyesit individualë për informata për klientët të cilat këmbyesit mund t'i mbledhin). Kështu kjo ofron një nivel të anonimitetit të mundshëm që ka qenë i pamundur me sistemet tradicionale të kartelave kreditore ose debitore ose sistemet më të zhvilluara të pagesave elektronike, siç është PayPal. Andaj shtrirja globale e valutave virtuale e rrit mundësinë e rreziqeve për pastrim të parave/financim të terrorizmit.

Sistemet e valutave virtuale mund të qasen përmes internetit (përfshirë telefonat mobile) dhe mund të shfrytëzohen për pagesa ndërkufitare dhe transfere të fondeve. Veç kësaj, valutat virtuale zakonisht mbështeten edhe në infrastrukturë komplekse që përfshin disa entitete, të cilat shpesh janë të shpërndara në disa shtete, për të transferuar fonde dhe për të kryer pagesa. Kjo shpërndarje e shërbimeve nënkupton se përgjegjësia për përputhshmëri me kriteret për luftim dhe mbikëqyrje të pastrimit të parave/financimit të terrorizmit mund të mos jetë e qartë. Për më tepër, të dhënat për klientët dhe transaksionet mund të mbahen nga entitete të ndryshme, shpesh në juridiksione të ndryshme, duke e bërë edhe më të vështirë për organet e rendit dhe rregullatorët për t'iu qasur atyre. Ky problem keqësohet edhe më shumë nga natyra që evoluon shumë shpejt e teknologjisë së decentralizuar të valutave virtuale dhe modeleve të bizneseve, përfshirë ndryshimin e numrit dhe llojeve/roleve të pjesëmarrësve që ofrojnë shërbime në sistemet e pagesave të valutave virtuale. Është e rëndësishme të dihet se një sistem i valutave virtuale mund të vendoset në juridiksione të cilat nuk kanë kontrolle adekuate të pastrimit të parave/financimit të terrorizmit. Sistemet e centralizuara të valutave virtuale mund të jenë bashkëfajtorë në rastet e pastrimit të parave, pasi që mund t'i kërkojnë me qëllim juridiksionet të cilat kanë regjime më të dobëta kundër pastrimit të parave/financimit të terrorizmit. Valutat e konvertueshme virtuale e të decentralizuara që lejojnë transaksione nga personi në person mund të duken të ekzistojnë në një univers digjital që është krejtësisht i paarritshëm për cilindo shtet.

Vlerësimi i rrezikut FATF i valutave virtuale¹⁰² tregon se, të paktën në afat të shkurtër kohor, vetëm valutat e konvertueshme virtuale, të cilat mund të përdoren për ta kaluar vlerën brenda dhe jashtë valutave reale dhe sistemi i rregulluar financiar kanë të ngjarë të paraqesin rreziqe për pastrim të parave/financim të terrorizmit. Kështu që, sipas qasjes së mbështetur në rreziq që është përshkruar në raportin e përmendur, shtetet duhet të përqendrojnë përpjekjet e tyre kundër pastrimit të parave/financimit të terrorizmit në valutave virtuale të konvertueshme të rrezikshmërisë më të lartë.

Vlerësimi i rrezikut po ashtu sugjeron se kontrollet e pastrimit të parave/financimit të terrorizmit duhet të përqendrohet në nyjet e valutave virtuale të konvertueshme - do të

¹⁰²Valutat virtuale - Udhëzim për një qasje të bazuar në rreziq, Taskforca e veprimit financiar, qershor 2015. Gjetet në: <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>

thotë, pikat e ndërprerjes të cilat ofrojnë porta për kalim në sisteme të rregulluara financiare - e të mos kërkojnë të rregullojnë përdoruesit të cilët sigurojnë valuta virtuale për të blerë mallra dhe shërbime. Këto nje përfshijnë, mes tjerash, këmbyesit e valutave të konvertueshme virtuale nga palët e treta. Në këto raste, ato duhet të rregullohen sipas Rekomandimeve nga FATF¹⁰³. Kështu, vendet të marrin në konsideratë zbatimin e kriterëve relevante kundër pastrimit të parave/financimit të terrorizmit të përcaktuara nga standardet ndërkombëtare për këmbyesit e valutave të konvertueshme virtuale dhe çfarëdo lloji të institucioneve të tjera të cilat shërbejnë si nje ku aktivitetet e valutave të konvertueshme virtuale kryqëzohen me sistemin e rregulluar financiar të valutave reale.

Sipas qasjes së FATF të bazuar në rrezik, vendet po ashtu mund të marrin në konsideratë institucionet e rregullimeve financiare ose të entiteteve të tjera të cilat dërgojnë, pranojnë ose ruajnë valuta virtuale, por të cilat nuk ofrojnë këmbime ose shërbime për pranim ose dërgim të parave të thata (cash-in/cash-out) mes valutave virtuale dhe atyre reale.

Direktiva e 5-të e ndryshuar kundër pastrimit të parave¹⁰⁴ ofron platforma të këmbimit të valutave virtuale dhe provajderë të kuletës brenda kufijve të rregulloreve kundër pastrimit të parave të cilat imponohen nga Direktiva e cila i përkufizon 'entitetet e obliguara'.

PYETJE PËR VETËREFLEKTIM

1. Ku ndodhë këmbimi nga valuta virtuale në valutë reale?
2. Si identifikohen palët në një transaksion në sistemin e valutave virtuale Bitcoin?
3. Cila është karakteristika themelore e valutave virtuale të decentralizuara që i bën ato të vështira për t'i rregulluar?
4. Si quhet libri i llogarive publike i transaksioneve me bitcoin?

5.4 Sfidat hetimore¹⁰⁵

5.4.1 Si të dihet se janë përdorur valutat virtuale

Sfida e parë që paraqesin hetimet ku përfshihen valutat virtuale është të identifikohet përdorimi i valutave virtuale dhe/ose nëse asetet kriminale mbahen në formë të valutës virtuale. Te valutat virtuale, përfaqësimi i vlerës është thujse gjithmonë i ruajtur në një formë krejtësisht elektronike¹⁰⁶.

¹⁰³ Për të hequr dyshimet, Rekomandimet - Standardet ndërkombëtare për luftimin e pastrimit të parave dhe financimin e terrorizmit dhe përhapjes së armëve, Task Forca e Veprimet Financiar (FATF) Rekomandime, 2012. Gjendet në: <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&DOS_INTERINST=&DOC_SUBJECT=&DOC_SUBTYPE=&DOC_DATE=&document_date_from_date=&document_date_to_date=&document_date_submit=&document_date_to_date_submit=&MEET_DATE=&meeting_date_from_date=&meeting_date_to_date_submit=&meeting_date_to_date_submit=&DOC_LANCD=EN&ROW_SPP=25&NRROWS=500&ORDERBY=DOC_DATE+DESC

¹⁰⁵ Keni parasysh se diskutimet në vazhdim u referohen kohë pas kohe bitcoinëve si shembull i valutës së decentralizuar virtuale. Sfidat e përshkruara këtu vlejnë për shumicën e valutave virtuale, sidomos të valutave virtuale të decentralizuara.

¹⁰⁶ Ekzistojnë disa organizata të cilat rresin përfaqësimin fizik të vlerës së valutave virtuale, por këto janë raste shumë të rralla dhe nuk përdoren shumë. Shih për shembull <http://www.coindesk.com/10-physical-bitcoins-good-bad-ugly/>

Andaj, hetuesit duhet të jenë të vetëdijshëm për mundësinë që fondet kriminale mund të jenë të konvertuara në valutë virtuale. Analistët e forenzikës digjitale duhet t'i zotërojnë shkathtësitë dhe aftësitë teknike për ta kuptuar ku dhe si të kërkojnë përdorimin e valutave virtuale në mjetet e konfiskuara për ruajtje të të dhënave elektronike.

5.4.2 Anonimiteti i transaksionit

Që nga zanafilla e shpërndarjes së valutave virtuale një nga karakteristikat e përmendura shpesh rreth funksionimit të tyre ka qenë anonimiteti i synuar i transaksioneve. Andaj, mbase sfida më e madhe gjatë hetimeve që përfshijnë bitcoinë ka të bëjë me aktivitetet e një kulete të caktuar të bitcoinëve me një individ të botës reale.

Me gjithë faktin se të gjitha transaksionet me bitcoin dhe përmbajtja e kuletës janë të dukshme dhe çdokush mund t'i shohë në zinxhir të blloqeve, nëse nuk e keni çelësin privat nuk mund të transferoni bitcoinët te një mbajtës tjetër i llogarisë¹⁰⁷. Megjithatë, personi nga bota reale i cili e posedon një çelës të caktuar privat nuk tregohet gjatë kryerjes së një transaksioni me bitcoin.

Janë identifikuar teknika të cilat lejojnë, në rrethana të caktuara, adresat e IP-së, të cilat ndërlidhen me një transaksion të caktuar¹⁰⁸. Një nga teknikat e para të identifikimit është përshkruar në një punim akademik të publikuar nga Philip dhe Diana Koshy në vitin 2014¹⁰⁹. Ata ndërtojnë versionin e tyre të softuerit të bitcoin që shkarkon një kopje të secilës pako të bartjes së të dhënave nga çdo kompjuter në rrjetin e bitcoin. Përmes analizës së këtyre të dhënave Koshyt ishin në gjendje të identifikojnë disa mostra të caktuara të të dhënave që mundësonin identifikimin e adresave të IP-së pas transaksioneve të caktuara me bitcoin. Megjithatë, aktualisht, këto teknike mbase nuk janë në dispozicion për shumicën e hetimeve penale për shkak të sfidave llogaritare që ato paraqesin.

5.4.3 Identifikimi i burimit të fondeve

Në hetimet ku vërtetohet se janë përdorur valutat virtuale, në disa raste mund të jetë e nevojshme të vërtetohet nëse fondet janë siguruar në mënyrë të paligjshme. I dyshimti mund të merret në pyetje në këtë pikë por në rastet kur i dyshimti nuk është bashkëpunues dhe/ose i dyshimti nuk është ende në dijeni se është nën hetime, mund të jetë e vështirë të vërtetohet se si janë blerë valutat virtuale.

Në këtë sektor, mbështetja e sektorit privat është kyçe. Këmbyesit e valutave virtuale si cilat janë entitete bashkëpunuese¹¹⁰ do të jenë në gjendje të ofrojnë informata për klientët individualë, emrat tipikë të ruajtur, detajet e verifikuara të kontakteve, kyçjet në IP, regjistrat e aktiviteteve, të gjitha adresat e valutave virtuale të shfrytëzuara nga përdoruesi për këmbim, mesazhe personale, informata për pagesë, një vërtetim të letërnjoftimit (ID) dhe dëshmi për adresën e shtëpisë.

¹⁰⁷ Shih studimin e mësipërm të rastit me bitcoin për një përshkrim se si funksionon bitcoin.

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

¹⁰⁹ Një analizë e anonimitetit në përdorimin bitcoin që përdor trafikun e rrjetit P2P, Koshy et al http://fc14.ifca.ai/papers/fc14_submission_71.pdf

¹¹⁰ Entitetet bashkëpunuese sipas legjislacionit kundër pastrimit të parave/financimit të terrorizmit nuk janë të kufizuara vetëm brenda këmbyesve të valutave virtuale, agjentëve që procesojnë pagesat, kuletave elektronike, vendeve të lojërave dhe shërbimeve të tjera elektronike të cilat po ashtu mund të ndihmojnë hetuesit.

Shfrytëzimi i kompetencave procedurale që parashihen nga Konventa e Budapestit kundër krimeve kibernetike po ashtu lejon qasje në të dhënat që mbahen nga këmbyesit dhe pjesëmarrësit e tjerë në ekosistemin e valutave virtuale (do të thotë përmes urdhrave për ruajtje, mbledhjes në kohë reale të të dhënave për trafikun, etj.)

Sfida e identifikimit të burimit të fondeve në një transaksioni me bitcoin po ashtu bëhet edhe më e vështirë përmes përdorimit të një shërbimi të përzier. Këto shërbime punojnë duke pranuar transaksione nga njerëz të shumtë, duke i ndarë fondet e transferuara në shuma të vogla dhe duke i përzier fondet bashkë me fondet e transferuara nga përdorues të tjerë të shërbimit. Kjo nënkupton, nga këndvështrimi i pranuesit të fondeve, se burimi origjinal i fondeve është shumë i paqartë nëse jo krejtësisht anonim¹¹¹.

5.4.4 Kthimi në para/realizimi dhe konvertimi i të ardhurave

Momenti kur vlera e valutave virtuale konvertohet në vlerë të valutave të letrës (reale) paraqet një mundësi për organet e rendit. Ky konvertim kryesisht ndodh gjatë këmbimit të valutave virtuale, andaj rekomandimet nga FATF në lidhje me valutat virtuale, që janë diskutuar shkurtimisht në Kapitullin 5.3, përqendrohen në rregullimin e nyjeve të valutave virtuale. "Nyjet" në këtë kontekst u referohen pikave ku bota e valutave virtuale takohet me botën financiare tradicionale, që mes tjerash, përfshin edhe këmbimin e valutave virtuale.

Në rastet kur këmbimet e valutave virtuale janë të rregulluara ata duhet të tregojnë kujdes të duhur gjatë identifikimit të klientëve. Në rastin specifik të bitcoin, të gjitha transaksionet vihen në dispozicion publik në zinxhirin e blloqeve. Kjo do të thotë se në rastet kur agjencitë e zbatimit të ligjit bien në dijeni për një adresë të caktuar të valutave virtuale e cila kontrollohet nga një i dyshimtë, është e mundshme duke analizuar transaksionet e kryera nga i dyshimti, që të identifikohet përdorimi i këmbimit të caktuar të valutës virtuale. Në këto raste, autoritetet e rendit mund ta paraqesin një urdhër gjykatë për ndonjë këmbim relevant të valutave virtuale për të zbuluar detaje për klientin, siç janë ID, adresa e shtëpisë, adresat e IP-së, adresat e emailit, numri i telefonit, historiku i transaksionit, adresat e depozitimit dhe tërheqjes, emri i bankës, numri i llogarisë së bankës dhe informata rreth transaksionit.

Në janar të vitit 2016, për shembull, janë arrestuar dhjetë meshkuj në Holandë si pjesë e një bastisjeje ndërkombëtare për tregjet e paligjshme elektronike të drogës. Këta burra janë kapur duke konvertuar bitcoinët në euro në llogari bankare duke përdorur shërbimet komerciale të bitcoin dhe pastaj kanë tërhequr me miliona para të thata nga automatët (ATM). Supozohet se ishin gjurmët e adresave të bitcoinëve që lidhën paratë me shitjen e paligjshme elektronike të drogës që është ndjekur nga FBI dhe Interpol. FATF, në raportin e tyre për valutat virtuale të vitit 2014 ("Valutat virtuale: Përkufizimet kyçe dhe rreziqet e mundshme për LPP/LFT"), ofron shembuj të disa veprimeve mjaft të publikuara të organeve të rendit që përfshijnë valutat virtuale.¹¹² Lexuesi i interesuar inkurajohet t'i shqyrtojë këto raste studimore për t'i kuptuar më mirë dimensionin dhe kompleksitetin e hetimeve të mëhershme që përfshijnë valutat virtuale.

Megjithatë, siç është diskutuar në pjesë të tjera të këtij doracaku, vazhdon të ketë sfida për shkak të natyrës së valutave virtuale të përhapura në gjithë botën. Këto sfida sillen

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

¹¹² Raporti FATF, Përkufizimet Kryesore për Valutat virtuale rreziqet e mundshme për LPP/LFT, qershor 2014. Gjetet në: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

nga fakti se këmbimet e valutave virtuale nuk janë të rregulluara njësoj nëpër botë deri te vështirësitë praktike që ndërlidhen me hetimet ndërkombëtare.

5.5 Sfidat e ngrirjes/sekuestrimit

5.5.1 Valutat virtuale si të ardhura nga krimi

Shumë shtete nuk kanë nevojë të specifikojnë natyrën e të ardhurave nga krimi. Në këto raste, një vlerë e ruajtur, siç është bitcoin, duhet të konsiderohet si e ardhur nga krimi nëse të ardhurat kanë buruar nga aktiviteti kriminal. Megjithatë, kjo duhet të vendoset brenda juridiksionit tuaj të caktuar.

5.5.2 Identifikimi i ekzistencës së valutave virtuale

Sfida e parë është të identifikohet ekzistenca e valutës virtuale dhe të vërtetohet se ajo është nën kontrollin e të dyshimitit. Disa nga çështjet që shfaqen këtu veçse janë diskutuar në Kapitullin 5.4. Ekzistenca dhe kontrolli i valutës virtuale mundet për shembull të shihen nga vëzhgimi, teknikat speciale të hetimeve, ose edhe nga mundësitë e hyrjeve.

5.5.3 Ngrirja/Marrja e kontrollit të valutave virtuale

Pas identifikimit se të ardhurat nga krimi mbahen në formë të valutave virtuale, pyetja e radhës është si të imobilizohen valutat virtuale dhe si të parandalohet shpërndarja e tyre. Pjesë e sfidës me ngrirjen e valutave virtuale është natyra e tyre virtuale, do të thotë se mund të ekzistojnë shumë kopje të kuletës së valutave virtuale. Madje edhe në rastet kur është sekuestruar një kuletë elektronike, ose një kuletë që mbahet në kompjuterin e të dyshimitit, kjo nuk është bazë për të besuar se valuta virtuale është hequr nga kontrolli i të dyshimitit. Ndodh shpesh që një i dyshimtë të ketë çelësa rezervë/kuletë që ruhet diku tjetër në cloud (hapësirën e ruajtjes në internet). Andaj, përpjekjet për të marrë kontrollin mbi kuletën e valutave virtuale të një të dyshimti nuk mund të ofrojnë siguri se asetet janë hequr nga kontrolli i të dyshimitit.

Duhet të theksohet se valutat virtuale nuk ruhen në pajisje si të tilla. Në rastin e bitcoin, është çelësi privat që i mundëson dikujt t'i shpenzojë ato. Ekzistojnë dy mënyra për t'i kapur bitcoinët, respektivisht duke siguruar qasje në çelësin privat të të dyshimitit ose përmes bashkëpunimit me sektorin privat (do të thotë, këmbyesit) të cilët kontrollojnë çelësin privat të të dyshimitit. Sapo që hetuesit të kenë në posedim çelësin privat të të dyshimitit, për ta kompletuar sekuestrimin, kërkohet që fondet të transferohen, pasi që i dyshimti ose ndonjë person tjetër që e kontrollon çelësin privat mund t'i bartë fondet në ndonjë adresë tjetër. Këto duhet të transferohen në një adresë të bitcoin të kontrolluar nga autoritetet e rendit (hetuesit ose prokuroria publike). Keni parasysh se kjo varet nga legjislacioni vendor në fuqi.

Prokurori mund ta sigurojë një urdhër gjykatë ose një urdhër të veçantë për ngrirje që ia pamundëson të dyshimitit ose agjentëve të tij t'i shpërndajnë valutat virtuale. Kjo nuk do t'i parandalojë agjentët që ndodhen në shtete të jashtme, aty ku urdhri mund të mos ketë efekt, që ata të veprojnë dhe t'i kalojnë ose t'i shpërndajnë valutat virtuale.

Nëse është e mundshme prokuroria duhet të kërkojë të likuidohet bilanci i valutës virtuale sa më parë (shih Kapitullin 5.5.4). Kjo kërkon ekzekutimin me kohë të një procesi për marrje të kontrollit të aseteve, në rast se një i dyshimtë ka qasje në një kopje rezervë të kuletës së synuar të valutës virtuale. Për më tepër, valutat virtuale janë shpesh të brishta për nga vlera dhe kur veproni për t'i likuiduar dhe për ta vënë baraspeshën në një llogari

qeveritare ju duhet të siguroheni ta ruani vlerën e përfaqësuar nga valuta virtuale në kohën e hetimit dhe ta vini atë në dispozicion për konfiskim eventual në rast të dënimit.

5.5.4 Menaxhimi i aseteve

Praktika më e mirë e rekomanduar është të likuidohet vlera e ruajtur e valutës virtuale. Kjo bazohet në nevojën për ta ruajtur vlerën e mallrave të sekuestruara (p.sh., letrave të çmuara të sekuestruara dhe valutat e huaja në para të thata). Kjo ruan vlerën e asetit dhe mbrohet nga paqëndrueshmëria në treg. Kjo po ashtu ofron garanci se valuta virtuale nuk mund të lëvizet, transferohet ose të vihet përtej dorës së gjykatës. Shumica e juridiksioneve kanë dispozita në legjislacionet e tyre për t'i likuiduar asetet për ta ruajtur vlerën për konfiskim eventual por kjo duhet të rregullohet në juridiksionin tuaj.

Direktiva e BE-së për Konfiskim¹¹³ rekomandon hapjen e një zyreje për t'i menaxhuar asetet e sekuestruara dhe të konfiskuara¹¹⁴. Nëse hapet një zyrë e tillë në juridiksionin tuaj, mund t'ia vlejë të familjarizoheni me kapacitetet e kësaj zyreje për ta likuiduar vlerën e ruajtur të valutave virtuale. Në të kundërtën, nëse një zyrë e tillë nuk ekziston, mundësia për ta likuiduar vlerën e valutës virtuale do të varet nga kapacitetet e çfarëdo lloj aranzhimi që bëhet për të menaxhuar asetet para konfiskimit.

PYETJE PËR VETËREFLEKTIM

1. Pse është praktika më e mirë që të likuidohet valuta virtuale sa më parë që të jetë e mundur?
2. A është e nevojshme në juridiksionin tuaj të vërtetohet burimi i paligjshëm i të ardhurave të caktuara nga krimi? Nëse po, si mund të bëhet kjo në rastin e valutave virtuale?
3. Cilat kushte duhet të përmbushen para se të sigurohet një urdhër për sekuestrim të valutave virtuale?
4. Çfarë masash duhet të përdoren për të identifikuar ekzistencën ose shfrytëzimin e valutave virtuale? Çfarë mbrojtjesh ekzistojnë për të mbrojtur interesat e palëve të treta të pafajshme?

¹¹³ Direktiva 2014/42/EU e Parlamentit Evropian dhe e Këshillit e datës 3 prill 2014 për ngrirjen dhe konfiskimin e dobive dhe të hyrave nga krimi në Bashkimin Evropian.

¹¹⁴ *Ibid* Preambula para 32.

6 Punë praktike/raste studimore

6.1 Hulumtim i literaturës

Luteni të përmendni nenet relevante në legjislacionin e juaj vendor dhe jurisprudencën relevante me një përshkrim të shkurtër, lidhur me pikat në vazhdim:

1. Konfiskimin e të ardhurave nga krimi si obligim sipas Kodit Penal dhe Kodit të Procedurës Penale/ligjeve të veçanta.
2. Përkufizimi i hetimit financiar, kur duhet të bëhet një hetim financiar, kush e kryen hetimin financiar?
3. Qasjen në të dhënat bankare dhe monitorimin e një llogarie bankare.
4. Përkufizimin dhe shfrytëzimin e masave të veçanta hetuese.
5. Qasja në të dhënat e tjera të pronësisë (regjistri i tokës, regjistri i veturave, etj.)
6. Urdhri për ngrirje.
7. Vendimi për konfiskim.
8. Regjimi i konfiskimit (procedura penale, konfiskimi në bazë të vlerës, konfiskimi i zgjeruar, supozimi i mungesës së ekuilibrit, konfiskimi që nuk bazohet në dënim (in rem)).
9. Ndihma e ndërsjellë juridike
10. Institucionet e specializuara.
11. Krijimi i një taskforce (prokurori, polici, NJIF, shërbime tatimore, dogana).
12. Qasja në të dhënat për abonuesin (adresa e IP-së, uebfaqet, adresa e emailave).
13. Qasja në të dhënat për abonuesit dhe në të dhënat për përmbajtjen.
14. Kërkesa për ruajtje.
15. Sekuestrimi i provave elektronike.

6.2 Rasti studimor 1: Shqyrtimi i bazës ligjore për veprime

Policia e shtetit tuaj ka nisur një hetim kundër të dyshimtëve A, B dhe C, të cilët janë duke e formuar një grup të organizuar kriminal për të shitur sasi të mëdha të mariuhanës te blerësit, D dhe E.

Përmes përdorimit të masave të fshehta (vëzhgim i fshehtë dhe përgjim i telekomunikimeve) është vërtetuar se më 15 tetor 2016 personi A i ka dorëzuar 1kg mariuhanë personit D, i cili i ka paguar 1,000 euro në para të thata në një valixhe. Është autorizuar shtyrja e sekuestrimit dhe arrestimit. Të njëjtën ditë, personi A ia dorëzon valixhen me para personit B. Është vërtetuar po ashtu se personi A është pajtuar përmes telefonit me personin E për t'ia shitur 2kg mariuhanë, për të cilat do të transferohen 2,000 euro në llogarinë bankare nr. 11.

Ju keni vendosur se keni nevojë t'u qaseni të dhënave të pronarit të llogarisë bankare me nr. 11, përfshirë mbajtësin e llogarisë dhe të dhënat për transaksionet gjatë x muajve të fundit. Po ashtu, ju vendosni se keni nevojë të filloni monitorimin e transaksioneve për llogaritë e personave A, B dhe E.

PYETJE: Përshkruani bazën ligjore në legjislacionin tuaj, duke iu referuar neneve të caktuara dhe kushteve për qasje në të dhëna bankare, të dhëna për transaksione dhe për monitorim të llogarive.

Përmes kësaj mase ju e identifikoni se A, B dhe E që të gjithë kanë llogari bankare në vendin tuaj. Ju po ashtu identifikoni një llogari bankare në emër të personit B në Austri.

Ju vendosni të kërkonti një urdhër gjykatë për të dhënat bankare, të dhënat e transaksioneve dhe për monitorim të llogarisë së personit B në Austri dhe të kërkonti ndihmë të ndërsjellë juridike në këtë çështje.

PYETJE: Tregoni bazën ligjore në legjislacionin tuaj shtetëror që i referohet neneve dhe kushteve të caktuara për ndihmë të ndërsjellë juridike.

Përmes analizës së llogarive bankare A, B dhe E bëhet e qartë se ka transaksione të shpeshta mes A dhe B, transaksione të shpeshta mes E dhe B dhe po ashtu edhe transaksione nga B jashtë vendit (në një vend tjetër në rajon dhe në Luksemburg). Ju i krahasoni dhe i ndërlidhni dinamikën e transaksioneve me të gjeturat gjatë hetimeve penale.

Përgjimet telefonike zbulojnë se B po negocion me C, i cili banon mes vendit tuaj dhe një vendi tjetër në rajon, për furnizimin me një sasi më të madhe të mariuhanës pas një muaji më 15 dhjetor 2016. C kërkon për një pagesë paradhënie, para 1 dhjetorit 2016, të gjysmës së çmimit (100,000 euro) në llogarinë bankare 22 (në emër të personit juridik DOO), ndërsa pjesa e mbetur prej 100,000 eurosh të paguhet në llogarinë bankare 33, në një bankë në Luksemburg.

Ju vendosni të siguroni të dhëna për llogaritë bankare të C në vendin tuaj dhe në vendin tjetër në rajon dhe ta siguroni një urdhër monitorues. Ju po ashtu vendosni të vërtetoni pronësinë e personit juridik DOO dhe llogarive të tij bankare dhe të urdhëroni sigurimin e të dhënave për transaksionet gjatë x muajve të fundit dhe monitorimin e llogarive të DOO.

PYETJE: Tregoni bazën ligjore në legjislacionin tuaj shtetëror, përfshirë referencën e neneve dhe kushteve për qasje në të dhënat e personave juridikë, të dhënat bankare dhe të transaksioneve të personave juridikë dhe të regjistrave tatimore të personave juridikë.

Me ndihmën e administratës tatimore ju vendosni të vërtetoni se si bën biznes DOO dhe kush janë partnerët afaristë. Ju zbuloni se DOO po ashtu tregton me kanabis industrial.

Ju i kërkonti të dhënat bankare nga llogaria 33 në Luksemburg dhe gjeni se ajo i përket një personi juridik në vendin tuaj, në pronësi të C.

PYETJE: A ekziston dyshimi për pastrim parash? Në çfarë momenti lind dyshimi? A duhet ta përfshini NJIF-in në taskforcën hetuese? Me çka mund të ndihmojë NJIF? Cilat tipologji të mundshme të pastrimit të parave shfrytëzohen këtu? Tregoni bazën ligjore, elementet dhe kushtet në legjislacionin tuaj shtetëror për pastrimin e parave. Tregoni bazën ligjore, elementet dhe kushtet në legjislacionin tuaj shtetëror për angazhimin e NJIF-it.

Përgjimi i telefonatave vërteton se personi B i është referuar komunikimit me email me personin A që përmban informata rreth transaksioneve dhe pagesave me bitcoin.

Ju vendosni se keni nevojë të identifikoni adresat e emailit që përdoren nga personi A dhe personi B dhe ta dini përmbajtjen e emailave. Ju vërtetoni se personi A po e përdor një adresë të emailit që ofrohet nga një provajder lokal i shërbimit të internetit.

PYETJE: Tregoni bazën ligjore në legjislacionin tuaj, përfshirë referencën e neneve dhe kushteve për bashkëpunim me ISP-të dhe për qasje në të dhënat e emaileve.

Përmes përmbajtjes së emaileve të A ju identifikoni transaksionet e droges të D dhe E dhe të tjerë dhe transaksione të parave në llogari bankare si dhe transfere të vlerës në bitcoin.

Ju vendosni të angazhoni ndihmën e NJIF-it për të analizuar transaksionet bankare dhe për të kërkuar lidhje dhe të dhëna për mbajtësit e llogarive jashtë vendit (në Austri dhe Luksemburg dhe në vendet e tjera të rajonit tuaj).

PYETJE: Tregoni bazën ligjore në legjislacionin tuaj, përfshirë referencën e neneve dhe kushteve për qasje në të dhëna bankare përmes NJIF dhe përmes bashkëpunimit me NJIF-ët ndërkombëtarë.

Përmes hetimeve ju identifikoni se një pagesë me bitcoin do të bëhet nga personi C te personi B më 15 dhjetor 2016. Ju e identifikoni se kuleta e bitcoin e personit B mbahet nga një këmbim bitcoinësh në Luksemburg.

PYETJE: Tregoni bazën ligjore në legjislacionin tuaj, përfshirë referencën e neneve dhe kushteve për të kërkuar informata për abonuesin nga një këmbimore bitcoinësh. Një këmbimore bitcoinësh në vendin tuaj a është e obliguar t'i mbajë të dhënat dhe të bashkëpunojë?

PYETJE:

- Çfarë masash do të ndërmerren në lidhje me pagesën e planifikuar të bëhet më 1 dhjetor 2016 në llogarinë 22 të personit juridik DOO?
- A do ta urdhëronit ngrirjen e transaksionit paraprakisht? Kur duhet të zbulohet urdhri për ngrirje? A do ta rrezikonte ngrirja e transaksionit në llogarinë DOO kapjen e një sasive të madhe të drogës që pritet të dorëzohet më 15 dhjetor 2016?
- Pasi të jenë arrestuar të dyshimtët, çfarë masash do të merren në lidhje me pagesën me para të thata të datës 15 dhjetor 2016?
- Pasi që grupi A, B dhe C janë marrë me biznes droge për një kohë të gjatë, sa dhe cilat asete mund të konfiskohen? Tregoni bazën në legjislacionin tuaj shtetëror për përgjigjen tuaj.
- A mund të akuzohet personi DOO për trafikim të drogës dhe/ose pastrim të parave? Nëse po, tregoni bazën ligjore në legjislacionin tuaj shtetëror dhe kushtet për dënimin e personit juridik. Tregoni një shembull të një vendimi dhe arsyetimin në lidhje me një konfiskim nga një person juridik.

Përmes analizës së komunikimit me email mes B dhe A ju zbuloni se grupi është duke shitur drogë edhe përmes një uebfaqeje të caktuar në një rrjet të fshehtë të uebfaqeve (darkweb). Kjo konfirmohet nga njëri nga blerësit i cili zbulon gjatë marrjes në pyetje si funksionon porositja dhe dorëzimi i drogës në darkweb dhe se si pagesat kërkohen ose përmes llogarive bankare ose me bitcoin¹¹⁵.

PYETJE: Cilat do të ishin veprimet tuaja rreth provave për aktivitetet e darkueb. A do të mund të angazhoni hetimet e fshehta si blerës dhe të blini drogë, të

¹¹⁵ Shih për shembull: <https://www.bitstamp.net/help/what-is-bitcoin/>

zbuloni llogaritë e rëndësishme bankare dhe kuletat e bitcoin dhe të ngrini paratë dhe pasurinë.

6.3 Rasti studimor 2: Marrja parasysh e bashkëveprimit me NJIF/Organet e rendit

Njësia e Inteligjencës Financiare (NJIF) në shtetin tuaj pranon një raport nga një bankë që tregon se ata dyshojnë për disa transaksione të cilat po bëhen përmes shërbimeve elektronike bankare. Institucioni ka identifikuar se shuma të mëdha parash janë transferuar në disa llogari të klientëve, ku këto shuma të parave nuk do të ishin tipike për klientët në fjalë. Veç kësaj, është theksuar nga institucioni financiar se klientët duket se janë kyçur në llogaritë e tyre bankare elektronike përmes adresave të IP-së në Rumani, një vend ku asnjëri nga këta klientë nuk janë kyçur më herët. Kjo sjellje është vërejtur te gjithsej 20 llogari klientësh dhe vlera totale hyrëse përmes këtyre 20 llogarive kap shifrën prej 750,000 eurosh.

NJIF kryen një analizë dhe identifikon raporte të tjera të transaksioneve të dyshimta (STR) të cilat kalojnë nëpër llogari bankare të klientëve të tjerë. NJIF përgatit një raport dhe e dërgon në polici.

Hulumtimi nga inteligjenca e policisë identifikon se ekziston një hetim policor i subjekteve rumune (në të vërtetë moldave por që banojnë në vendin tuaj) në lidhje me dokumente të falsifikuara të identifikimit.

Policia i arreston subjektet dhe kontrollon objektet e tyre duke sekuestruar disa laptopë. Ekzaminimi forenzik i laptopëve zbulon se ata janë përdorur për të kontrolluar mbi 200 llogari bankare të shfrytëzuara për të pranuar dhe pastruar para që kanë buruar nga llogari bankare të personave kompjuterët e të cilëve janë infektuar me Trojan 'Driedex'¹¹⁶ i cili i ka mbledhur kredencialet e tyre të llogarive elektronike bankare. Shuma e përgjithshme e parave të pastruara përmes këtyre llogarive është mbi 3 milionë euro.

Të dyshimtët ndiqen penalisht dhe dënohen me nga 8 dhe 5 vjet burgim. Nuk janë kthyer kurrfarë të hyrash nga krimi.

PYETJE: Cila është baza ligjore në të cilën NJIF mbështetet për ta raportuar rastin te policia?

Mund të ekzistojë edhe baza legjislative për këtë bashkëveprim, por në shumë raste, policia dhe NJIF (dhe organizatat e tjera siç janë autoritetet tatimore, doganat, etj.) nënshkruajnë një Memorandum të Mirëkuptimit që mundëson këmbimin e informatave. Kjo bazë mund të varet edhe nga natyra e raportit që i dorëzohet policisë. Për shembull, informatat të cilat i përcillen policisë mund të konsiderohen (nga policia) si inteligjencë ose mund të konsiderohen si kallëzim penal.

Ju lusim ta hetoni situatën në vendin tuaj.

PYETJE: Cilat dispozita të kodit tuaj të procedurës penale janë relevante për hetimet policore?

¹¹⁶ Dridex është një trojan shumë agresiv që kryesisht përdoret për të vjedhur kredencialet bankare. Softueri keqbërës konfigurohet për t'i targetuar klientët e afër 300 organizatave të ndryshme në mbi 40 rajone. Dridex përqendrohet me të madhe në klientët e institucioneve financiare në vendet e pasura anglisht folëse, ku shumica e këtyre organizatave të synuara ndodhen. Sulmuesit po ashtu i kanë caktuar si prioritet disa vende evropiane, krahas atyre në rajone të Azisë përgjatë Pacifikut.

Përkitazi me fushën e krimeve kibernetike, hetimeve financiare dhe pastrimit të parave ekzistojnë disa veprime që ndërmerren nga policia në këtë rast ilustrues; bëhet kontrolli i subjekteve dhe objekteve të tyre, laptopët sekuestrohen dhe ekzaminohen në mënyrë forenzike, provat mbledhen nga llogaritë e kompromentuara bankare.

Qëllimi i kësaj pyetjeje është të shqyrtohet baza ligjor e kodin e juaj të procedurës penale për këto veprime.

PYETJE: Cilat dispozita të kodit tuaj penal e kriminalizojnë infektimin e një kompjuteri të një klienti me një virus?

Nëse vendi juaj e ka ratifikuar Konventën e Budapestit, atëherë infektimi i një kompjuteri personal me virus është vepër penale. Cila është dispozita në Kodin tuaj Penal që e transponon nënin relevant nga Konventa e Budapestit?

Nëse vendi juaj nuk e ka ratifikuar Konventën e Budapestit, a keni dispozita ekuivalente? Si kriminalizohen krimet kompjuterike?

PYETJE: Si do ta lidhni aktivitetin e Dridex Trojan me të pandehurit?

Të dyshimtët kanë përdorur një softuer dashakeq për t'i vjedhur kredencialet e shërbimeve elektronike bankare. Sidoqoftë, këto kredenciale janë vjedhur nga kompjuterët personalë të viktimave, e jo nga kompjuterët e të dyshimtëve. Andaj, si e lidhni aktivitetin e Trojan me të dyshimtit? A mund ta krijoni një lidhje kauzale nga posedimi i detajeve të llogarisë së komprometuar bankare (që mund të vërtetohet nga prania e tyre në laptopët e të dyshimtëve) me aktin e komprometimit të këtyre detajeve të llogarive me Trojan? Nëse po, si do t'i qaseshit kësaj? Nëse jo, çfarë implikimesh, nëse ka, ka kjo në akuzat të cilat mund të ngrihen kundër të dyshimtëve?

PYETJE: Si mund t'i vërtetoni lidhjet mes rumunëve/moldavëve dhe kontrolluesit të llogarive bankare ku janë transferuar paratë dhe personit i cili e ka shpërndarë virusin. Si mund ta vërtetoni nëse të dyshimtët kanë pasuri (në vendin tuaj ose jashtë vendit)?

Si vazhdimësi e pyetjes paraprake, prania e detajeve nga llogaria bankare në laptopin e të dyshimtit, mund apo nuk mund të demonstrojë se të dyshimtët kanë pasur nën kontroll llogaritë bankare në kohën kur paratë në fjalë janë transferuar. A duhet të vërtetohet kjo ndaras ose a mund të nxirret si përfundim nga posedimi i llogarive bankare? Nëse jo, çka tjetër duhet të vërtetohet?

PYETJE: A mund ta ndiqni penalisht vjedhjen e ndihmuar me kompjuter?

Kompjuterët janë përdorur në këtë rast si një komponentë themelore e vjedhjes. A ka ndonjë dispozitë në legjislacionin tuaj shtetëror që kriminalizon përdorimin e kompjuterëve si mjet në rastin e vjedhjeve/mashtrimeve?

PYETJE: Cilat dispozita procedurale në legjislacionin tuaj shtetëror e rregullojnë mbledhjen dhe përdorimin e provave elektronike?

Në rastet e tilla, provat nga laptopët e të dyshimtëve mund të jenë kyçe. Andaj, a ka dispozita në legjislacionin tuaj shtetëror që e lejojnë mbledhjen dhe përdorimin e provave elektronike?

PYETJE: A ka vendi juaj kapacitete për forenzikë kompjuterike? Si merreni me kapacitetet e forenzikës kompjuterike?

Në aspektin praktik, mbledhja dhe menaxhimi i provave elektronike kërkon instrumente dhe shkathtësi të specializuara. Si është e rregulluar kjo në vendin tuaj?

PYETJE: A duhet të kryhet një hetim financiar në këto raste? Në çfarë faze duhet të fillohet një hetim financiar?

Siç u përshkrua në këtë skenar, qartazi ekzistojnë implikacione serioze financiare që ndërlidhen me aktivitetin e të dyshimtëve. Në vendin tuaj, a kryhet (a do të duhej të kryhej) një hetim financiar në këtë rast? Nëse po, në çfarë momenti duhet të fillojë hetimi financiar?

PYETJE: Cilat dispozita në legjislacionin tuaj shtetëror e rregullojnë kontrollin, sekuestrimin dhe konfiskimin e aseteve në këtë rast? Si do t'i rikthenit paratë e vjedhura? A mund t'i ngrini ato (nga NJIF ose nga policia/prokurori)?

Skenari tregon se të dyshimtit janë dënuar me burgim. Sipas dispozitave shtetërore, a është e paraparë që komponenta e konfiskimit të aseteve në procedurë të ndodhë pas procedurës penale, apo a ndodhin ato në të njëjtën procedurë?

A kanë viktimat e mashtruara mundësi për t'i rikthyer fondet e vjedhura? A mund t'i kompensoni viktimat nëse ju i ktheni disa/të gjitha paratë? Cilat janë dispozitat në legjislacionin tuaj që e mundësojnë këtë?

PYETJE: Cilat dispozita në legjislacionin tuaj e përshkruajnë veprën penale të pastrimit të parave? A është kryer vepra penale e pastrimit të parave?

Si përkufizohet vepra penale e pastrimit të parave në legjislacionin tuaj? Duke marrë në konsideratë faktet e përshkruara më lart, a është kryer vepra e pastrimit të parave?

PYETJE: A do ta ndiqnit penalisht edhe veprën penale të pastrimit të parave bashkë me vjedhjen/mashtrimin? Pse po/pse jo?

Kur ta shqyrtoni këtë rast, a do ta përfshinit edhe ndjekjen penale të pastrimit të parave krahas vjedhjes/mashtrimit? Nëse po, pse? Nëse jo, pse jo?

PYETJE: Viktimat janë të shpërndara nëpër shumë shtete, si do ta bashkërendonit hetimin me këto shtete?

Për shkak të natyrës pa kufij të internetit, thuajse të gjitha rastet që kanë si komponentë krimin kibernetik kanë edhe një element ndërkombëtar. Në këtë rast, nëse ka viktimë në shumë shtete, a do të koordinoheshit me ato shtete të tjera? Çka nëse, gjatë hetimeve tuaja, identifikoni më shumë viktimë, për të cilat nuk është ditur më herët?

PYETJE: A keni afate kohore për dorëzimin e provave dhe a do t'i tejkalonin kërkesat për NNJ këto afate? Si do t'i reduktonit vonesat kohore lidhur me kërkesat për NNJ?

Nëse një komponentë ndërkombëtare është e përfshirë, mund të ketë nevojë për shfrytëzimin e procesit të ndihmës së ndërsjellë juridike, e cila mund të shkaktojë disa

vonesa të theksuara për hetime. Afatet kohore rreth procesit të ndihmës së ndërsjellë juridike a paraqesin sfida për hetimet në vendin tuaj? Si do të mund të reduktoheshin vonesat kohore? A mund të përdorni ekipe të përbashkëta hetuese, për shembull? A mund t'i përdorni kanalet jozyrtare të komunikimit për t'i lehtësuar pyetjet para ndihmës së ndërsjellë juridike?

6.4 Rasti studimor 3: Shqyrtimi i bashkëveprimit në raste të krimit kibernetik/pastrimit të parave

Disa qytetarë në vendin tuaj raportojnë se u janë infektuar kompjuterët personalë me një softuer dashakeq që i ka enkriptuar të gjitha fotot dhe dokumentet e tyre. Softueri dashakeq pastaj u ka kërkuar një pagesë me bitcoin para dekriptimit të fotove dhe dokumenteve. Në disa raste, qytetarët e kanë paguar haraçin.

Gjatë hetimeve, policia bashkëpunojnë me NJIF për të ndihmuar në gjurmimin e bitcoinëve. NJIF janë në gjendje të gjurmojnë bitcoin deri te këmbimorja ku bitcoinët janë konvertuar në valuta reale. Këmbimorja e bitcoinëve ndodhet në Shtetet e Bashkuara të Amerikës.

Një kërkesë për ndihmë të ndërsjellë juridike (NNJ) dërgohet në Shtetet e Bashkuara të Amerikës që kërkon hollësi rreth llogarive që i kanë kryer transaksionet. Kur të pranohet përgjigja nga Shtetet e Bashkuara kuptohet se vlera e bitcoinëve është transferuar në llogari bankare në shtetin tuaj nga individë të cilët i përdorin adresat e IP-së në shtetin tuaj.

PYETJE: Si do t'i identifikoni të dyshimtët (adresën e IP-së)? Si mund t'i siguronit këto të dhëna - brenda apo jashtë shtetit? Çka nëse adresat e IP-së nuk janë në vendin tuaj?

Lidhja mes adresës së IP-së dhe një personi nga bota reale është një nga aspektet më të rëndësishme të çdo hetimi elektronik. Nëse adresa e IP-së është në vendin tuaj, si u qasen provajderëve kombëtarë të shërbimeve të internetit për të siguruar qasje në ato të dhëna? Cilat dispozita ligjore e mundësojnë këtë qasje? Çfarë obligimesh u ngarkohen provajderëve të shërbimeve të internetit për t'i ruajtur dhe vënë në dispozicion këto të dhëna?

Shqyrtoni situatën kur adresa e IP-së nuk ndodhet në vendin tuaj? Çka dallon në këtë rast? Si do t'i qaseshit situatën në këtë rast?

PYETJE: Si do t'i vërtetoni lidhjet mes mbajtësve të llogarive bankare (paragrafi tre i skenarit) dhe mbajtësve të kuletës së bitcoinëve dhe personave që e kanë përdorur softuerin dashakeq? A duhet të kryhet një hetim financiar në këto raste?

Përgjigja në kërkesën për ndihmë të ndërsjellë juridike tregon adresat e IP-së dhe detajet rreth llogarive bankare të cilat janë përdorur për konvertimin e bitcoinëve në valuta reale. Si (a) e kuptoni se cilat institucione financiare e posedojnë atë llogari, nëse nuk e dini dhe (b) u qasen institucioneve financiare për të siguruar informacione rreth mbajtësit të llogarisë bankare. Cilat dispozita ligjore e mundësojnë këtë qasje? Çfarë obligimesh u ngarkohen institucioneve financiare për t'i ruajtur dhe vënë në dispozicion këto të dhëna?

Shqyrtoni situatën kur llogaritë bankare mbahen në një shtet tjetër. Çka ndryshon dhe si do t'i qaseshit situatës në këtë rast?

PYETJE: A do të duhej të fillohej një hetim financiar dhe nëse po, në cilin moment?

Siç u përshkrua në këtë skenar, qartazi ekzistojnë implikacione serioze financiare që ndërlidhen me aktivitetin e të dyshimtëve. Në vendin tuaj, a kryhet (a do të duhej të kryhej) një hetim financiar në këtë rast? Nëse po, në çfarë momenti duhet të fillojë hetimi financiar?

PYETJE: Cilat dispozita në legjislacionin tuaj e përshkruajnë veprën penale të pastrimit të parave? A është kryer vepra penale e pastrimit të parave?

Si përkufizohet vepra penale e pastrimit të parave në legjislacionin tuaj. Duke marrë në konsideratë faktet e përshkruara më lart, a është kryer vepra e pastrimit të parave?

PYETJE: Skenari përshkruan aktivitetin e përbashkët nga policia dhe NJIF për ta analizuar dhe gjurmuar aktivitetin e bitcoin. Çfarë bazash ligjore ekzistojnë për këtë bashkëpunim?

Mund të ekzistojë edhe baza legjislative për këtë bashkëveprim, por në shumë raste, policia dhe NJIF (dhe organizatat e tjera siç janë autoritetet tatimore, doganat, etj.) nënshkruajnë një Memorandum të Mirëkuptimit që mundëson këmbimin e informatave.

Ju lusim ta hetoni situatën në vendin tuaj.

PYETJE: Si janë të rregulluara valutat virtuale, e në veçanti bitcoin, në vendin tuaj?

Ekzistojnë regjime të ndryshme rregullative nëpër botë lidhur me bitcoin. Cila është situata në vendin tuaj?

PYETJE: A janë valutat virtuale entitete që e kanë obligim të raportojnë transaksionet e dyshimta në vendin tuaj?

Në veçanti, a ekziston ndonjë obligim i entiteteve të valutave virtuale siç janë këmbimoret ose shërbimet e kuletës për t'i raportuar aktivitetet e dyshimta?

7 Shtojca: Lista e materialeve relevante për lexim

7.1 Këshilli i Evropës

- Konventa kundër krimeve kibernetike, ETS 185, 23.11.2001:
<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
- Protokolli shtesë i Konventës kundër krimit kibernetik, lidhur me penalizimin e akteve të natyrës raciste dhe ksenofobe të kryera përmes sistemeve kompjuterike ETS 189, 28.01.2003:
<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189>
- Konventa mbi Pastrimin, Kërkimin, Sekuestrimin dhe Konfiskimin e të Ardhurave nga Krimi dhe mbi Financimin e Terrorizmit, CETS 198, 16.05.2005:
<http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/198>
- Konventa mbi Pastrimin, Kërkimin, Sekuestrimin dhe Konfiskimin e të Ardhurave nga Krimi, Strasburg ETS 141, 08.11.1990:
<https://rm.coe.int/168007bd23>
- MONEYVAL/Projekt global kundër krimeve kibernetike, rrjedhës së parave të krimit në internet - hulumtim i tipologjive, mars 2012:
[http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL\(2013\)6_Reptyp_flows_en.pdf](http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2013)6_Reptyp_flows_en.pdf)
- Studimi i Këshillit të Evropës për filtrimin, bllokimin dhe mbylljen e përmbajtjes së paligjshme në internet, qershor 2016:
<https://www.coe.int/en/web/cybercrime/-/study-on-filtering-blocking-and-take-down-of-illegal-content-on-the-internet>
- Pyetësori për përdorimin dhe efikasitetin e instrumenteve të Këshillit të Evropës në lidhje me bashkëpunimin ndërkombëtar në fushën e sekuestrimit dhe konfiskimit të të ardhurave nga krimi, përfshirë menaxhimin e mallrave dhe ndarjen e aseteve. PC-OC Mod (2015) 06Rev4, 19.05.2016:
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680666607>
- Legjislacioni kundër krimeve kibernetike - profilet e shteteve:
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp
- Funksionimi i pikave të kontaktit që janë në dispozicion 24/7 kundër krimeve kibernetike (punim diskutimi i përgatitur nga Projekti kundër Krimeve kibernetike), prill 2009:
<https://rm.coe.int/16802fa3be>
- Udhërrëfyes mbi provat elektronike - Udhërrëfyes elementar për policë, prokurorë dhe gjyqtarë (mars 2013). Sigurohet me kërkesë në:
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp

- T-CY(2006)04 Forcimi i bashkëpunimit mes organeve të rendit dhe sektorit privat, shembuj si sektori privat ka bllokuar sajte të pornografisë së fëmijëve, shkurt 2006:
- <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e6ed1>
- T-CY(2013)17rev, raporti vlerësues T-CY: Dispozitat e Konventës së Budapestit kundër krimeve kibernetike, 3 dhjetor 2014:
- <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>
- T-CY(2014)17 - Rregullat për sigurimin e raportit për informata për abonuesin, dhjetor 2014:
- <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7ad1>
- T-CY(2015)10 - Qasja e drejtësisë penale në cloud: sfidat, dokument diskutimi i përgatitur nga T-CY Cloud Evidence Group, maj 2015:
- <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59>
- T-CY(2016)13 - Kërkesat emergjente për zbulim të menjëhershëm të të dhënave të ruajtura në një juridiksion tjetër përmes kanaleve të ndihmës së ndërsjellë juridike ose përmes kërkesave të drejtpërdrejta te provajderiët e shërbimit, T-CY Cloud Evidence Group, maj 2016:
- <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651a6f>
- T-CY (2016)2 – Qasja e drejtësisë penale në të dhënat në cloud: bashkëpunimi me provajderët e "huaj" të shërbimeve. Historiku i përgatitur nga T-CY Cloud Evidence Group, maj 2016:
- <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d>
- T-CY (2016)7, Qasja e drejtësisë penale në prova elektronike në internet (cloud): Rekomandime për t'u marrë në konsideratë nga T-CY, Raporti Përfundimtar nga T-CY Cloud Evidence Group, 16 shtator 2016.
- <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>
- T-CY(2015)16 Shënim i miratuar për sigurim të urdhrit (Neni 18) - versioni 1 mars 2017 (miratuar në procedurë me shkrim më 28 shkurt 2017):
- <https://rm.coe.int/16806f943e>

7.2 Bashkimi Evropian

- Direktiva 2014/42/EU e Parlamentit Evropian dhe e Këshillit e datës 3 prill 2014 për ngrirjen dhe konfiskimin e dobive dhe të hyrave nga krimi në Bashkimin Evropian OJ L 127/39, 29.4.2014.
- <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0042>

- Direktiva 2015/849 e Parlamentit Evropian dhe e Këshillit e datës 20 maj 2015 për parandalimin e përdorimit të sistemit financiar për qëllime të pastrimit të parave ose financimit të terrorizmit, që e ndryshon Rregulloren (BE) nr. 648/2012 të Parlamentit Evropian dhe të Këshillit, dhe që e shfuqizon Direktivën 2005/60/EC të Parlamentit Evropian dhe të Këshillit dhe Direktivën e Komisionit 2006/70/EC:
<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849>
- Veprimi i përbashkët 98/699/JHA i datës 3 dhjetor 1998 i miratuar nga Këshilli në bazë të Nenit K.3 të Traktatit të Bashkimit Evropian për pastrimin e parave, identifikimin, gjurmimin, ngrirjen, sekuestrimin dhe konfiskimin e dobive dhe të ardhurave nga krimi (OJ L 333, 9.12.1998, p. 1):
<http://eur-lex.europa.eu/legal-content/NLN/TXT/?uri=celex:31998F0699>
- Vendimi Kornizë i Këshillit 2001/500/JHA i datës 26 qershor 2001 mbi pastrimin e parave, identifikimin, gjurmimin, ngrirjen, sekuestrimin, konfiskimin e dobive dhe të ardhurave nga krimi (OJ L 182, 5.7.2001, p.1):
<http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001F0500>
- Vendimi Kornizë i Këshillit 2005/212/JHA i datës 24 shkurt 2005 për për konfiskimin e të ardhurave, dobive dhe pasurive që lidhen me krimin (OJ L 68, 15.3.2005, p. 49):
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:068:0049:0051:en:PDF>
- Vendimi Kornizë i Këshillit 2003/577/JHA i datës 22 shkurt 2003 për ekzekutimin e urdhrave për ngrirjen e pasurisë ose provave në Bashkimin Evropian (OJ L 196, 2.8.2003):
<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003F0577>
- Vendimi Kornizë i Këshillit 2006/783/JHA i datës 6 tetor 2006 për ekzekutimin e urdhrave për zbatimin e parimit të pranimit reciprok të urdhrave për konfiskim (OJ L 328, 24.11.2006):
<http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32006F0783>
- Vendimi i Këshillit 2007/845/JHA i datës 6 dhjetor 2007 që ka të bëjë me bashkëpunimin mes Zyrave për Rikthim të Pronës së Shteteve Anëtare në fushën e gjurmimit dhe identifikimit të të hyrave nga krimi (L 332/103, 18.12.2007):
<http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007D0845>
- Direktiva 2013/40/EU e Parlamentit Evropian dhe e Këshillit e datës 12 gusht 2013 mbi sulmet kundër sistemeve informative që e zëvendëson Vendimin Kornizë të Këshillit 2005/222/JHA:
<http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040>
- Direktiva e Bashkimit Evropian 2016/1148 për sigurinë e rrjeteve dhe sistemeve informative ("NIS Directive") të datës 6 korrik 2016:
<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L.2016.194.01.0001.01.ENG>

- EU GENVAL 2012 Raporti përfundimtar për rrethin e pestë të vlerësimit të ndërsjellë – “Krimet financiare dhe hetimet financiare”:
<http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012657%202012%20REV%202>
- Projektraporti përfundimtar i rrethit të shtatë të vlerësimeve të ndërsjella të “zbatimit dhe funksionimit praktik të politikave evropiane për parandalimin dhe luftimin e krimeve kibernetike”, qershor 2017:
<http://data.consilium.europa.eu/doc/document/ST-9986-2017-INIT/en/pdf>

7.3 Kombet e Bashkuara

- Konventa e Kombeve të Bashkuara kundër trafikut të paligjshëm me droga narkotike dhe substanca psikotropike, Vjenë, 19.12.1988:
<https://www.unodc.org/unodc/en/treaties/illicit-trafficking.html>
- Konventa e Kombeve të Bashkuara kundër krimit të organizuar transnacional, Nju Jork, 15.11.2000:
<https://www.unodc.org/unodc/en/treaties/CTOC/>
- Konventa e Kombeve të Bashkuara kundër korrupsionit, Nju Jork, 31.10.2003:
<http://legal.un.org/avl/ha/uncc/uncc.html>

7.4 Task Forca për Veprim Financiar

- Standardet ndërkombëtare për luftimin e pastrimit të parave dhe financimin e terrorizmit dhe përhapjes së armëve, Rekomandime (FATF), 2012.
<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>
- Pastrimi i parave duke përdorur metodat e reja të pagesës, tetor 2010:
<http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf>
- Përkufizimet Kryesore për Valutat virtuale rrethet e mundshme për LPP/LFT, qershor 2014:
<http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>
- Valutat virtuale - Udhëzim për një qasje të bazuar në rrezik, Taskforca e veprimit financiar, qershor 2015:
<http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>

7.5 Jurisprudenca

- Aktgjykimi nga Gjykata Evropiane e të Drejtave të Njeriut (ECHR) në rastin K.U. Kundër Finlandës, 2 dhjetor 2008, për obligimin e Qeverive për të mbrojtur qytetarët nga krimi, përfshirë përmes të drejtës penale:

[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]})

- Praktika gjyqësore e ECHR rreth mbrojtjes së të dhënave personale:
http://www.echr.coe.int/Documents/FS_Data_ENG.pdf
- Praktika gjyqësore e ECHR rreth teknologjive të reja:
http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf
- Praktika gjyqësore e ECHR rreth përgjimeve masive:
http://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf
- Aktgjykimi i Gjykatës për Drejtësi të Bashkimit Evropian në rastet e bashkuara C-293/12 dhe C-594/12. Të drejtat digjitale Irlanda dhe Seitlinger dhe të tjerët:
<http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>
- Aktgjykimi i Gjykatës për Drejtësi të Bashkimit Evropian në rastin C-582/14, 19 tetor 2016, adresat dinamike të IP-së mund të kualifikohen si 'të dhëna personale' sipas të drejtës private të BE-së:
<http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1034974>
- Aktgjykimi i Gjykatës për Drejtësi të Bashkimit Evropian në rastin C-264/14, 22 tetor 2015, "valuta virtuale 'bitcoin' nuk ka qëllim tjetër pos të jetë mjet pagese që është i pranueshëm për atë qëllim nga operatorë të caktuar":
<http://curia.europa.eu/juris/document/document.jsf?text=&docid=170305&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=160800>
- Aktvendimi i Gjykatës Supreme të Belgjikës në rastin e Belgjikës kundër Yahoo!: http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1
- Gjykata e Apelit e SHBA-ve në rastin Microsoft kundër Shteteve të Bashkuara:
<http://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412>

7.6 Referenca të tjera

- Ruajtja e të Dhënave pas Aktgjykimit nga Gjykata e Drejtësisë e Bashkimit Evropian, Prof. Dr. Franziska Boehm et al., Munster/Luxembourg, 30 qershor 2014:
http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf
- Enkriptimi çështje e të drejtave të njeriut, Raport nga Amnesty International, mars 2016. Gjendet në:
http://www.amnestyusa.org/sites/default/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf

- "Broshura: 6 gjërat që duhet ditur për Hetimet financiare, shkurt 2016:
- <https://english.eu2016.nl/documents/publications/2016/02/10/brochure-the-6-need-to-knows-about-financial-investigation>
- "Vlerësimi i nevojave për instrumentet dhe metodat e hetimit financiar në Bashkimin Evropian, ECORYS, dhjetor 2015:
https://www.wodc.nl/binaries/2612-summary_tcm28-74130.pdf
- Opinioni i autoritetit evropian për shërbime bankare për 'valutat virtuale', EBA/Op/2014/08, July 2014:
<https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>
- Një analizë e anonimitetit në përdorimin bitcoin që përdor trafikun e rrjetit P2P, Koshy et al, Universiteti Shtetëror Pensilvani:
http://fc14.ifca.ai/papers/fc14_submission_71.pdf
- Vlerësimi i Kërcënimit nga Krimi i Organizuar në Internet (IOCTA), Europol, 2016:
<https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016>
- Vlerësimi i Kërcënimit nga Krimi i Organizuar në Internet (IOCTA), Europol, 2017:
<https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>