

КРИВИЧНОПРАВНА ОДГОВОРНОСТ У ТРГОВИНИ ДИГИТАЛНОМ ИМОВИНОМ НА ТРЖИШТУ КАПИТАЛА

Апстракт: Овај рад се бави анализом кривичноправне одговорности у области трговине дигиталном имовином на тржиштима капитала, фокусирајући се на све чешиће злоупотребе њоме: прања новца, манипулације на тржиштима, финансирања тероризма и инвестиционих превара. Рад указује на недовољну нормативну прилагоденост postojećih кривичноправних и тржишних регулатива, како у Републици Србији, тако и у ширем међународном оквиру. Посебан нагласак стављен је на улогу регулатора и међународних институција, као и на изазове у примени postojećih прописа. Циљ рада је да се кроз системску правну анализу и компаративни приступ истакну кључне тачке у postojećем систему заштите тржишта и санкционисања злоупотреба. Посебна пажња посвећена је улози институција њоме Комисије за хартије од вредности, Народне банке Србије, правосудних органа, као и међународних тела њоме ИНТЕРПОЛ-а и Еуропола. Рад је намењен стручњацима у области кривичној и финансијској права, регулаторима, доносиоцима одлука и академској заједници, са циљем да пружи системски увид и предложне конкретне мере за правовремену и ефикасну реакцију на ризике које са собом носи дигитална имовина.

Кључне речи: дигитална имовина, кривично дело, манипулација на тржишту, регулаторни оквир, прање новца.

1. УВОД

1.1. Значај дигиталне имовине на савременим тржиштима капитала

Дигитална имовина, по свему судећи, требало би да представља нову и растућу класу финансијских инструмената која укључује криптовалуте,

* Мастер правник и директор Сектора за учеснике на тржишту у Комисији за хартије од вредности Републике Србије, uros.popovic@sec.gov.rs.

токенизоване хартије од вредности, стабилне новчиће и дигиталне токене. Њен развој има значајан утицај на трансформацију традиционалних модела пословања и трговања на тржиштима капитала, доносећи нове могућности, али и одређене ризике који захтевају пажњу регулатора и правне струке. Према доступним подацима, глобална тржишна капитализација криптовалута је крајем 2024. године достигла приближно 3,35 билиона долара, што представља значајан раст у односу на претходну годину. Овај раст је праћен повећањем вредности водећих криптовалута попут биткоина, чија је тржишна капитализација достигла 2 билиона долара, уз тржишни удео од 56,8%. Такође, друге криптовалуте попут Dogecoina и XRP-а забележиле су значајан раст током исте године.¹

Данас са сигурношћу можемо рећи да главна предност дигиталне имовине лежи у њеној способности да омогући директну, брзу и јефтинију размену вредности између учесника без традиционалних посредника, као што су организациони делови кредитних институција које пружају инвестиционе услуге и активности или инвестициона друштва. Ова карактеристика резултат је технологије блокчејна, која представља основу функционисања криптовалута као што су Биткоин и Етеријум. Блокчејн обезбеђује децентрализовано, транспарентно и непроменљиво евидентирање трансакција, што повећава поверење међу учесницима на тржишту.²

Међутим, упркос овим значајним предностима, дигитална имовина ствара и бројне регулаторне и правне изазове. Традиционални закони, као што су Закон о тржишту капитала³ и Закон о алтернативним инвестиционим фондовима⁴ у Србији, често нису у потпуности прилагођени специфичностима ове класе имовине. Овај недостатак регулаторне јасноће може довести до правних празнина које компликују контролу и надзор над активностима као што су праће новца, манипулације на тржишту и друге злоупотребе.⁵ На пример, анонимност трансакција на блокчејн мрежама компликује праћење и контролу активности које укључују праће новца или манипулације на тржишту.⁶

Истовремено, интересовање за дигиталну имовину константно расте, не само код појединачних, већ и код институционалних инвеститора као што су хеџ фондови и велике компаније. Институционални учесници препознају

- 1 М. Šmirmaul, „Kriptotržište se hladi – je li sad vrijeme za kupovinu?“, *Bloomberg Adria*, 2025, https://hr.bloombergadria.com/trzista/crypto/72147/kriptotrziste-se-hladi-je-li-sad-vrijeme-za-kupovinu/news?utm_, 10. април 2025.
- 2 Ј. Стојић Дабетић, Р. Мирковић, *Уговарање и уговорно право у digitalnom društvu*, Правни факултет за привреду и правосудје у Новом Саду, Нови Сад, 2022, 63–65.
- 3 *Службени гласник РС*, бр. 129/2021.
- 4 *Службени гласник РС*, бр. 73/2019 и 94/2024.
- 5 М. Lehmann, “Digital Assets in The Conflict of Laws: A Comparative Search for The Ideal Rule”, *Singapore Journal of Legal Studies*, Online Edition, 2024, 24–25.
- 6 М. Стојадиновић, „Koliko su podaci korisnika na Blockchainu zaista privatni?“, *Webmind*, 2023, https://web-mind.rs/blokcejn/koliko-su-podaci-korisnika-na-blockchainu-zaista-privatni/?utm_, 10. април 2025.

потенцијал дигиталне имовине за диверсификацију портфолија и остваривање виших приноса, што додатно наглашава важност и неопходност ефикасне регулативе. С обзиром на глобални значај и брзи развој тржишта дигиталне имовине, овај рад ће анализирати не само економске и технолошке аспекте, већ и правне ризике и изазове које она представља за савремена тржишта капитала у Србији, Европској унији и Северној Америци, како би се идентификовале препоруке за даљи развој националне и међународне регулативе.

1.2. Кратак осврт на раст трговине дигиталном имовином и повезаних злоупотреба

Трговина дигиталном имовином бележи значајан раст последњих година, како на глобалном нивоу, тако и у Србији, где се интересовање за ову област постепено повећава. Према најновијим подацима из 2024. године, глобално тржиште криптовалута достигло је укупну капитализацију од приближно 3,37 билиона америчких долара, а значајан део овог тржишта држе водеће платформе за трговање као што су Binance и Coinbase.⁷ Истовремено, раст тржишта дигиталне имовине праћен је и значајним повећањем различитих злоупотреба. Према извештају компаније Chainalysis из 2025. године, криминалне активности повезане са криптовалутама резултирале су трансакцијама вредним преко 40 милијарди америчких долара.⁸ Посебно су изражени проблеми са прањем новца, финансирањем терористичких активности путем анонимних и децентрализованих платформи, као и манипулацијама на тржишту, попут „pump and dump“ шема, где се вештачки подиже вредност одређених дигиталних средстава ради краткорочне добити на штету осталих инвеститора. Додатно, на тржишту дигиталне имовине учестале су и преваре кроз лажне инвестиционе платформе, као и напади на крипто-берзе који изазивају значајне финансијске губитке и смањују поверење учесника на тржишту.⁹

1.3. Ограниченост кривичноправне одговорности у вези са трговањем дигиталном имовином

Трговина дигиталном имовином је у Србији у порасту, али се истовремено јављају и изазови у вези са кривичноправном одговорношћу. Технолошке

7 Binance News, „Global Cryptocurrency Market Value Surpasses \$3.37 Trillion, Bitcoin Dominates with 56.8% Share“, https://www.binance.com/en/square/post/12-27-2024-global-cryptocurrency-market-value-surpasses-3-37-trillion-bitcoin-dominates-with-56-8-share-18126760852378?utm_, 10. април 2025.

8 Chainalysis, *The 2025 Crypto Crime Report*, 2025, 3.

9 *Ibid.*, 7.

иновације, попут блокчејна, омогућавају децентрализовану размену вредности, али истовремено отварају простор за злоупотребе које нису адекватно регулисане постојећим законима. Један од основних проблема је идентификација кривичних дела повезаних с дигиталном имовином, као што су прање новца, манипулације на тржишту и финансирање тероризма.¹⁰ Кривична одговорност мора бити јасно дефинисана како за физичка лица која користе дигиталну имовину за злоупотребе, тако и за правна лица, укључујући берзе и пружаоце услуга повезаних са дигиталном имовином, који својим деловањем или пропустима могу омогућити овакве активности.

Додатни изазов представља уређење поступака истраге и гоњења. Због анонимности трансакција и децентрализоване природе блокчејн мрежа, прикупљање доказа често захтева специјализоване техничке алате и међународну сарадњу.¹¹ Према Националној процени ризика од прања новца и финансирања тероризма из 2024. године, Србија је препознала потребу за јачањем капацитета у овој области.¹² Транснационални аспект трговине дигиталном имовином додатно компликује спровођење закона. Различити правни системи, недостатак хармонизације регулатива и ограничена сарадња између држава често омогућавају учиниоцима да избегну правну одговорност.¹³ На пример, случајеви хаковања берзи или злоупотреба путем децентрализованих финансијских платформи често укључују више јурисдикција, што отежава екстрадицију и координацију правних поступака.

1.4. Циљеви и истраживачка питања рада

Овај рад има за циљ да идентификује и анализира најзначајније кривичноправне изазове у вези са трговином дигиталном имовином, као и да истражи могућности које регулатива тржишта капитала пружа за спречавање ових злоупотреба. За разлику од општих приказа и теоретских расправа, овај рад ће пружити конкретна решења и практичне препоруке засноване на реалним и актуелним примерима. Који су конкретни кривичноправни изазови у трговини дигиталном имовином, посебно када је реч о питањима као што су анонимност трансакција, регулаторне недоречености и технолошке препреке за ефикасно вођење истрага и поступака? Како прецизно дефинисана и ефикасно примењена регулатива тржишта капитала може

10 *Национална љроцена ризика, Йроцена ризика од љрања новца*, Министарство финансија, Управа за спречавање прања новца, 2024, 60.

11 У. Поповић, „Дисруптивни потенцијал блокчејн технологије за унапређење међународне правне сарадње у кривичним стварима“, *Зборник радова са међународне научне конференције „Однос међународној кривичној и националној кривичној љрава“* (ур. М. Шкулић *et al.*), Том II, Београд, 2024, 297–303.

12 *Национална љроцена ризика, Йроцена ризика од љрања новца*, *op. cit.*, 60.

13 Т. Јованић, „Крипто-имовина као пример утицаја дигитализације на право и праксу регулаторних органа“, *Међународна научна конференција „Право и дигитализација“*, *Зборник радова*, Правни факултет Универзитета у Нишу, Ниш, 2021, 22–26.

значајно утицати на смањење ризика и сузбијање различитих облика злоупотреба, укључујући и прање новца, манипулације на тржишту и финансирање тероризма? Одговори на ова питања омогућиће прецизну идентификацију постојећих слабости у националном и међународном регулаторном окружењу, као и давање конкретних предлога за правну реформу и јачање институционалних капацитета. Крајњи резултат истраживања биће сет препорука који ће допринети већој транспарентности, правној сигурности и стабилности на тржишту дигиталне имовине, како у Србији, тако и шире.

2. ДИГИТАЛНА ИМОВИНА У КОНТЕКСТУ ТРЖИШТА КАПИТАЛА

2.1. Дигитална имовина и тржиште капитала

2.1.1. Појам и врсте дигиталне имовине

Дигитална имовина представља врсту нефизичке имовине која постоји искључиво у дигиталном облику и заснована је на технологији блокчејна.¹⁴ У зависности од својих карактеристика и употребе, дигитална имовина се може категоризовати у неколико основних група:¹⁵

- Криптовалуте (нпр. Bitcoin, Ethereum): Децентрализоване дигиталне валуте које се користе за трансакције и складиштење вредности без посредовања традиционалних финансијских институција.
- Токени: Дигитални записи који могу представљати различите облике вредности и права, као што су учешће у капиталу компаније, приступ услугама или специфичним производима.¹⁶
- Стабилни новчићи (Stablecoins): Посебна врста криптовалута чија је вредност везана за стабилну референтну вредност, најчешће фиат валуте попут америчког долара или евра, са циљем смањења волатилности.¹⁷
- Нефунгибилни токени (NFT): Јединствени дигитални записи који представљају власништво над специфичним предметима, попут

14 Аутор намерно не примењује дефиницију дигиталне имовине како је прописана Законом о дигиталној имовини – ЗДИ, *Службени гласник РС*, бр. 153/2020, имајући у виду да иста, посматрана из нормативно-правног и технолошког угла, не задовољава критеријуме прецизности и функционалне применљивости у стручно-научном контексту.

15 P. Mirković, "Digital assets – a legal approach to the regulation of the new property law institute", *LAW – theory and practice*, 40/2023, 23.

16 A. Grace Garnett, "Digital tokens: 8 types of crypto coins", *Britannica Money*, 2024, <https://www.britannica.com/money/what-are-stablecoins>, 10. април 2025.

17 Investopedia, "Digital Asset: Meaning, Types, and Importance", 2024, <https://www.investopedia.com/terms/d/digital-asset-framework.asp?utm>, 10. април 2025.

уметничких дела, колекционарских предмета или виртуелних средстава у дигиталном простору.

2.1.2. Специфичности дигиталне имовине у односу на традиционалне финансијске инструменте

Дигитална имовина се битно разликује од традиционалних финансијских инструмената у неколико аспеката: За разлику од традиционалних финансијских инструмената који су обично централизовано контролисани од стране институција попут банака или берзи, дигитална имовина функционише на децентрализованим мрежама без централног ауторитета.¹⁸ Блокчејн технологија, која је основа већине дигиталних инструмената, обезбеђује транспарентност трансакција и непроменљивост записа, чиме се смањује могућност манипулација. Дигитална имовина доступна је свим корисницима широм света, без географских или регулаторних ограничења која су често присутна код традиционалних финансијских инструмената.¹⁹ Трансакције са дигиталном имовином могу бити анонимне или псеудонимне, што ствара додатне изазове за праћење токова новца и откривање злоупотреба. За разлику од традиционалних инструмената који захтевају посреднике и централизоване процесе, трансакције са дигиталном имовином често су брже и јефтиније захваљујући директној размени између учесника. Цене дигиталне имовине често показују знатно већу волатилност у поређењу са традиционалним финансијским инструментима, што може представљати и ризик и прилику за инвеститоре. Трговина и коришћење дигиталне имовине захтевају техничко знање и разумевање блокчејн технологије, што може представљати препреку за поједине инвеститоре и регулаторе.

2.2. Трговина дигиталном имовином на тржишту капитала

2.2.1. Процес трговања дигиталном имовином

Трговина дигиталном имовином одвија се путем специјализованих платформи, познатих као берзе дигиталне имовине. Платформе попут Binance-а, Coinbase-а и Kraken-а омогућавају корисницима да једноставно и брзо купују, продају или размењују различите врсте дигиталне имовине, укључујући криптовалуте, токенизоване хартије од вредности и NFT-ове.

18 Hedera, "TradFi and DeFi: Key Differences", <https://hedera.com/learning/decentralized-finance/tradfi>, 10. април 2025.

19 J. Stojić Dabetiћ, P. Mirković, „Digitalna imovina – novo poglavlje u regulisanju imovinskih prava“, XXI међународни научни skup „Правнички дани – Prof. dr Slavko Carić“, Одговори правне науке на изазове савременог друштва, Нови Сад, 2024, 671–672.

Корисници приступају овим платформама коришћењем дигиталних новчаника, који служе за сигурно чување приватних кључева неопходних за одобравање и извршавање трансакција на блокчејн мрежама. Трансакције се обављају директно на децентрализованим мрежама, што омогућава већи степен сигурности и транспарентности, али и захтева техничку спремност и пажљиво управљање приватним кључевима од стране корисника.²⁰

2.2.2. Учесници на тржиштима дигиталне имовине

На тржишту дигиталне имовине делују различити субјекти који омогућавају њено функционисање:

- *Берзе дигиталне имовине:* Ове платформе пружају инфраструктуру за трговање и ликвидност. Поред Binance-а и Coinbase-а, значајну улогу имају и мање регионалне берзе које послују у складу са локалним законодавством.
- *Пружаоци услуга чувања:* Специјализовани субјекти који нуде сигурно складиштење дигиталне имовине за кориснике, попут Fireblocks-а и BitGo-а. Њихове услуге су кључне за минимизацију ризика од губитка или крађе дигиталне имовине.²¹
- *Инвестициониори и корисници:* Ова група укључује појединце и институције који улажу у дигиталну имовину ради остваривања профита или њене примене као средства размене. Институционални инвеститори, попут хеџ фондова и корпорација, постају све присутнији актери на овом тржишту.

У Републици Србији, пружаоци услуга повезаних с дигиталном имовином подлежу ЗДИ, који дефинише њихове обавезе и процедуре лиценцирања. Привредно друштво које намерава да пружа ову врсту услуга мора прибавити одговарајућу дозволу Народне банке Србије и/или Комисије за хартије од вредности.²²

2.2.3. Регулација тржишта капитала у вези с дигиталном имовином

Регулација тржишта капитала у вези са дигиталном имовином подразумева прилагођавање и развој законских оквира који регулишу активности на овом специфичном тржишту. У Србији, ЗДИ представља основни правни

20 S. Houy, P. Schmid, A. Bartel, "Security Aspects of Cryptocurrency Wallets – A Systematic Literature Review", *ACM Computing Surveys*, 1/2023, 1–31.

21 Пружаоце услуга чувања дигиталне имовине, који обезбеђују техничку инфраструктуру за складиштење дигиталних средстава (нпр. Fireblocks, BitGo), треба разликовати од пружалаца услуга чувања криптографских кључева у складу са ЗДИ, према којем ову услугу могу, уз испуњење законом прописаних услова, пружати и банке.

22 К. Трајковић, „Лиценцирање и надзор у области дигиталне имовине“, *Зборник радова Народне банке Србије*, 2/2022, Београд, 152–156.

акт који регулише статус дигиталне имовине, обавезе пружалаца услуга и услове пословања. Пружалац услуга дигиталне имовине мора имати одговарајућу лиценцу Народне банке Србије или Комисије за хартије од вредности, односно обе дозволе. На међународном нивоу, регулативе попут MiCA (Markets in Crypto-assets Regulation) у Европској унији и смернице FATF-a (Financial Action Task Force) представљају значајан корак ка унапређењу правне сигурности, спречавању злоупотреба и повећању транспарентности на тржишту дигиталне имовине. Ови регулаторни оквири дефинишу стандарде за KYC (Know Your Customer) и AML (Anti-Money Laundering) процедуре, уређују пословање берзи и пружалаца услуга, те доприносе бољој међународној сарадњи у овој области.

2.2.4. Ризици и изазови у љракси љрљовања дигиталним имовином

Трговање дигиталном имовином праћено је низом специфичних ризика и изазова који могу резултирати појавом озбиљних кривичноправних проблема. У наставку су наведени ризици и њихове практичне импликације: тржишта дигиталне имовине могу бити подложна значајним флукутацијама ликвидности, што може довести до наглих промена цена; ниска ликвидност олакшава манипулације тржиштем, као што су „pump-and dump“ шеме, где учесници вештачки подижу цену одређене имовине ради краткорочне добити на штету других инвеститора;²³ дигитална имовина је изложена сајбер нападима, укључујући крађе приватних кључева, хаковање платформи за трговање и новчаника. Ови сигурносни пропусти доводе до великих финансијских губитака и правних спорова, што наглашава потребу за јасном кривичноправном регулативом и ефикасним правосудним реакцијама; грешке у функционисању блокчејн технологије или технички кварови у инфраструктури могу узроковати прекид трговања и губитак средстава корисника. Ови инциденти често резултирају питањима правне одговорности, укључујући процену кривичне одговорности за немар или непоштовање безбедносних стандарда; недовољно јасна регулатива и правна несигурност у многим јурисдикцијама омогућавају простор за злоупотребе и отежавају истрагу и гођење учинилаца кривичних дела.

2.3. Правни оквир за дигиталну имовину

2.3.1. Национални закони и љројиси

У Републици Србији, правни оквир за дигиталну имовину успостављен је доношењем ЗДИ који је ступио на снагу 29. децембра 2020. године, а

23 За више вид. J. T. Hamrick *et al.*, „An examination of the cryptocurrency pump and dump ecosystem”, *Ecosystem*, 2019, 23–26.

примењује се од 30. јуна 2021. године. Овај закон пружа свеобухватну регулативу за издавање, трговину и пружање услуга повезаних с дигиталном имовином у Србији. ЗДИ дефинише дигиталну имовину као дигиталне записе вредности који се могу куповати, продавати, размењивати или преносити дигитално, а могу се користити као средство размене или улагања. Ова дефиниција обухвата, између осталог, виртуелне валуте и дигиталне токене. Поред ЗДИ, донети су и подзаконски акти који ближе уређују одређене аспекте дигиталне имовине. На пример, Народна банка Србије је донела Одлуку о условима и начину обављања плаћања, преноса и наплате у девизама у вези с трансакцијама с дигиталном имовином, која прецизира услове под којима се могу обављати ове трансакције.²⁴ Такође, Комисија за хартије од вредности је донела више правилника који регулишу пружање услуга повезаних с дигиталним токенима, укључујући услове за добијање дозволе, управљање информационо-комуникационим системом, вођење евиденције и друге аспекте пословања пружалаца ових услуга.²⁵

2.3.2. Међународни стандарди

Међународне организације су важан део за хармонизацију и успостављање глобално прихваћених правила за дигиталну имовину, што је од суштинске важности за смањење ризика и повећање правне сигурности:

- FATF (Financial Action Task Force): Ова међувладина организација поставља стандарде за борбу против прања новца и финансирања тероризма који су директно применљиви и на тржишту дигиталне имовине. Посебно је значајно правило „Travel Rule“, које обавезује пружаоце услуга дигиталне имовине да прикупљају и преносе информације о идентитету учесника у трансакцијама, чиме се омогућава ефикасније праћење сумњивих активности.
- ЕУ регулатива MiCA (Markets in Crypto-assets Regulation): Ова регулатива представља свеобухватни правни оквир Европске уније који дефинише јединствене стандарде за дигиталну имовину и пружаоце услуга у овој области. Њен циљ је обезбеђивање транспарентности, стабилности тржишта и јасне заштите инвеститора.
- Земље као што су Јапан, Сингапур и Швајцарска представљају примере успешних регулаторних приступа дигиталној имовини.²⁶ Ове државе имају свеобухватне и јасно дефинисане законе и регулативе

24 Одлука о обављању плаћања у девизама у вези с трансакцијама с дигиталном имовином, *Службени гласник РС*, бр. 49/2021.

25 Сви правилници су доступни на следећем линку: <https://shorturl.at/0E1ds>, 10. април 2025.

26 K. Werbach, “Digital Asset Regulation: Peering into the Past, Peering into the Future”, *William & Mary Law Review*, 4/2022–2023, 1275–1278.

које се посебно фокусирају на регулисање берзи, спречавање финансијских злоупотреба и обезбеђивање високих стандарда за заштиту инвеститора.

2.3.3. ФАТФ стандарди и препоруке за дигиталну имовину

ФАТФ је међународна организација која поставља стандарде за борбу против прања новца и финансирања тероризма.²⁷ Њен „Travel Rule“ налаже да пружаоци услуга дигиталне имовине (VASPs) прате и деле информације о трансакцијама које премашују одређени праг вредности. Овај стандард захтева идентификацију пошиљаоца и примаоца средстава, чиме се смањује ризик од злоупотреба повезаних са анонимним трансакцијама.²⁸ ФАТФ стандарди су основа за усклађивање националних регулаторних оквира. На пример, ЕУ је увела регулативу која интегрише „Travel Rule“ у своја правила о спречавању прања новца (AML), док су Сједињене Америчке Државе и Сингапур такође прилагодили своје законодавство према овим смерницама. Међутим, глобална имплементација и даље представља изазов због разлика у техничкој и регулаторној инфраструктури међу државама.

2.3.4. Улога ИНТЕРПОЛ-а, Еуропола и других тела

Међународне организације попут ИНТЕРПОЛ-а и Еуропола имају улогу у борби против злоупотреба повезаних са дигиталном имовином, нарочито у прекограничним случајевима. ИНТЕРПОЛ и Еуропол одржавају базе података о криминалним активностима и олакшавају размену обавештајних података међу државама чланицама. Организују специјализоване тренинге за полицијске и правосудне органе како би унапредили њихове капацитете за истраживање случајева злоупотреба дигиталне имовине. Ове организације помажу у усклађивању правних процедура и омогућавају заједничке операције за идентификацију и хапшење учинилаца. На пример, Еуропол је 2023. године координисао међународну акцију која је резултирала затварањем неколико платформи за прање новца путем криптовалута.²⁹ Поред ових тела, организације попут УН-а и Светске банке такође пружају подршку у развоју политика и стратегија за борбу против злоупотреба

27 Financial Action Task Force (FATF) Travel Rule, 2024, <https://www.sanctionsscanner.com/blog/financial-action-task-force-fatf-travel-rule-140>, 10. април 2025.

28 Financial Action Task Force (FATF), *Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers*, 2024, 18–23.

29 APNews, “German investigators take down crypto money laundering site”, <https://apnews.com/article/germany-cryptocurrency-money-laundering-darknet-4f0c402eddec3ffa57eb00df205a2ef4>, 10. април 2025.

дигиталне имовине. Њихов допринос укључује пружање техничке помоћи и спровођење истраживања о ризицима и трендовима у овој области.

3. КРИВИЧНОПРАВНИ АСПЕКТИ ТРГОВИНЕ ДИГИТАЛНОМ ИМОВИНОМ

3.1. Основни облици кривичних дела

3.1.1. Манипулације на тржишту

Манипулације на тржишту представљају један од најучесталијих облика злоупотреба у трговини дигиталном имовином. Једна од најпознатијих шема је тзв. *pump and dump*, где се цена одређене дигиталне имовине вештачки повећава ширењем лажних или обмањујућих информација. Након што цена достигне врхунац, организатори шеме продају своје уделе, што доводи до наглог пада вредности и значајних губитака за друге инвеститоре. Ове шеме су посебно присутне на тржишту криптовалута, где је регулатива често недовољна, а тржиште подложно манипулацијама. Овакве шеме могу узроковати значајне финансијске губитке за инвеститоре.³⁰ Осим „*pump-and-dump*“ шема, постоје и други облици манипулација на тржишту дигиталне имовине, као што су: ширење нетачних или обмањујућих информација с циљем утицаја на цену дигиталне имовине; коришћење поверљивих информација за стицање предности на тржишту дигиталне имовине; спуфинг и слојинг (енгл. *spoofing* и *layering*) – постављање лажних налога за куповину или продају с циљем обмане других учесника на тржишту. Ови облици манипулација нарушавају интегритет тржишта дигиталне имовине и могу довести до губитка поверења инвеститора

3.1.2. Прање новца у трговини дигиталном имовином

Дигитална имовина све више постаје алат за прање новца, захваљујући својој децентрализованој структури, могућности брзог трансфера и релативној анонимности корисника. Употреба криптовалута омогућава прикривање порекла илегално стечених средстава и њихово увођење у легалне финансијске токове без потребе за посредницима у традиционалном финансијском систему.³¹ Према извештају компаније Chainalysis за 2023. годину,³²

30 T. Li, D. Shin, B. Wang, “Cryptocurrency Pump-and-Dump Schemes”, *Journal of Financial and Quantitative Analysis*, 2025, 1–59.

31 Chainalysis, “DeFi Takes on Bigger Role in Money Laundering But Small Group of Centralized Services Still Dominate”, 2022, https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/?utm_, 10. април 2025.

32 Chainalysis, *The 2024 Crypto Crime Report*, 2024.

процењује се да је у току те године приближно 6 милијарди америчких долара прљавог новца опрано путем криптовалута, што представља смањење у односу на 8,6 милијарди долара из 2021. године, али и даље указује на висок ниво злоупотреба у овој области. Највећи део ових трансакција одвијао се преко децентрализованих берзи (DEX), миксера за криптовалуте и „приватних новчића“ попут Монеро-а, који користе напредне технике шифровања и замрачују траг трансакција. Употреба миксера, као што су Tornado Cash и Sinbad, омогућила је корисницима да трансформишу криптовалуте у друге облике без могућности праћења, што отежава рад истражних органа и финансијских регулатора. Примери из праксе показују да криминалне групе често користе више слојева трансакција, тзв. *layering*, ради прикривања извора средстава. Један од значајних случајева јесте истрага коју је координисао Еуропол 2022. године³³, која је обухватила више лица укључених у прање новца преко криптовалутних новчаника и DEX платформи, где је идентификовано више од 250 милиона евра у сумњивим трансакцијама.

3.1.3. Финансирање тероризма коришћењем дигиталне имовине

Дигитална имовина, посебно криптовалуте које пружају висок степен анонимности и могућност брзог трансфера преко граница, постала је инструмент у рукама терористичких организација за финансирање њихових активности. Према подацима Канцеларије УН-а за борбу против тероризма (UNOCT), број истрага у којима се јавља дигитална имовина као елемент финансирања тероризма је у порасту, посебно након пандемије COVID-19 када је повећана употреба онлајн платформи и децентрализованих мрежа.³⁴ Терористичке групе користе децентрализоване финансијске протоколе (DeFi), анонимне трансакције преко „приватних новчића“ и криптовалутне миксере за прикупљање донација, трансфер средстава и финансирање конкретних активности. Према наводима из извештаја ФАТФ-а из 2023. године, више група повезаних са блискоисточним екстремистичким мрежама користило је криптовалуте као што су Bitcoin и Tether за финансирање логистичке подршке, регрутацију и набавку опреме. Финансирање тероризма преко дигиталне имовине изазов је за органе безбедности, јер захтева истовремену примену мера финансијског надзора, техничких капацитета за анализу блокчејн трансакција и међународну координацију. Постоје примери успешних истрага, као што је заједничка операција америчког Министарства правде

33 Europol, “9 drug traffickers arrested and EUR 27 million in cryptocurrencies seized”, <https://www.europol.europa.eu/media-press/newsroom/news/9-drug-traffickers-arrested-and-eur-27-million-in-cryptocurrencies-seized>, 10. април 2025.

34 Subcommittee on Digital Assets, Financial Technology, and Inclusion Hearing: “Crypto Crime in Context Part II”, Memorandum, 2024, [HHRG-118-BA21-20240215-SD002.pdf](#), 10. април 2025.

и Израелске агенције за борбу против тероризма, у којој су идентификовани и заплењени крипто-новчаници повезани са организацијама Хамас и ИСИС у вредности од неколико милиона долара.³⁵

3.1.4. Преваре у вези са улажањем у дигиталну имовину

Преваре везане за дигиталну имовину представљају један од најраспрострањенијих облика злоупотреба у овој области и укључују различите облике криминалног деловања као што су лажне инвестиционе платформе, прева-рантски токени, нерегистровани ICO пројекти, фишинг напади и хаковање берзи. Један од најпознатијих случајева је „OneCoin“, пројекат који је функционисао као глобална Понзи шема, у којој је на стотине хиљада инвеститора обмануто широм света. Процењује се да је штета настала овом преваром износила више од 4 милијарде америчких долара. Организаторка пројекта, Ружа Игнатова, остала је недоступна органима гоњења више година, што је додатно указало на проблем недостатка међународне координације у борби против оваквих превара. Према подацима Комисије за хартије од вредности САД,³⁶ број случајева повезаних са Initial Coin Offerings (ICO) у којима су инвеститори доведени у заблуду у вези са високим приносима и нерегистрованим хартијама од вредности наставља да расте. У свом годишњем извештају за 2022. годину, SEC је навео да је више од 70% истражених ICO пројеката садржавало елементе преваре или непотпуне документације.

3.2. Одговорност физичких и правних лица

3.2.1. Правна лица

Правна лица која послују у домену дигиталне имовине – укључујући берзе дигиталне имовине, пружаоце услуга чувања и размене, платформе за почетне понуде токена (ICO),³⁷ као и DeFi протоколе под корпоративном управом – имају централну улогу у одржавању правне сигурности и спречавању злоупотреба на овом тржишту. Њихова кривичноправна и регулаторна одговорност произлази из више извора: пружаоци услуга морају да прикупе, обраде и чувају податке о идентитету корисника у складу са законом, а непоштовање ове обавезе може омогућити прање новца, финансирање тероризма и друге нелегалне активности; правна лица су у обавези да имплементирају системе за прање трансакција и идентификацију сумњивих

35 Chainalysis, “United States DOJ and FBI Seize Cryptocurrency in Major Disruption of Hamas Terrorist Financing Scheme”, 2025, *DOJ Seizes Crypto in Disruption of Hamas Terrorist Financing Scheme*, 10. април 2025.

36 SEC, *Reports and Publications*, <https://www.sec.gov/reports>, 10. април. 2025.

37 P. Mirković, *op. cit.*, 25.

активности, те да о истима обавештавају Управу за спречавање прања новца,³⁸ а непријављивање може довести до прекршајне, а у одређеним случајевима и кривичне одговорности; пружаоци услуга морају улагати у техничку и организациону заштиту инфраструктуре, а пропусти који доводе до губитка средстава или компромитације личних података корисника могу бити основ за одговорност због немара или чак саучесништва у кривичним делима ако се утврди свесна неактивност, одн. пропуштање. Према Регулациви MiCA, правна лица која пружају услуге повезане с дигиталном имовином морају добити дозволу надлежног регулаторног тела, поштовати обавезе транспарентности, водити евиденције и предузимати мере за заштиту потрошача. Непоштовање ових обавеза повлачи казне у висини до 12,5% укупног годишњег промета или 15 милиона евра, у зависности од тога шта је веће.

3.2.2. Физичка лица

Физичка лица која учествују у трговини дигиталном имовином подлежу кривичноправној одговорности уколико њихово поступање представља повреду важећих закона. Ова одговорност обухвата низ деликата који се могу јавити у контексту дигиталне имовине, како у погледу активности на тржишту, тако и у погледу злоупотреба технолошких механизма. Најчешћи облици кривичне одговорности физичких лица укључују: физичка лица која намерно шире лажне или обмањујуће информације с циљем подизања или обарања вредности дигиталне имовине, чиме себи или другима прибављају противправну имовинску корист, могу се теретити за кривична дела против привреде, као што су злоупотреба поверења у привреди или превара (чл. 223, 208 Кривичног законика – КЗ).³⁹ Особе које користе дигиталну имовину за прикривање или легализацију незаконито стечених прихода, подлежу санкцијама у складу са чл. 245 КЗ, који предвиђа казне затвора до 10 година, као и одузимање имовине. Појединци који организују лажне ICO пројекте, непостојеће криптовалуте или лажне платформе за улагање, могу одговарати за кривично дела преваре из чл. 208 КЗ, што подразумева затворску казну и накнаду штете оштећеним инвеститорима. У прекограничним случајевима, правна помоћ и међународна сарадња – кроз механизме као што су екстрадиција, међународни захтеви за податке, и рад преко INTERPOL-а или EUROJUST-а – омогућавају ефикасније гоњење осумњичених. Нарочито је значајна улога споразума о узајамној правној помоћи у кривичним стварима који Србија има са више од 30 држава.

38 Правилник о методологији за извршавање послова у складу са законом о спречавању прања новца и финансирања тероризма, *Службени љласник РС*, бр. 80/2020 и 18/2022.

39 *Службени љласник РС*, бр. 85/2005, 88/2005 – испр., 107/2005 – испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 и 94/2024.

3.3. Доказивање и специфичности поступка

3.3.1. Проблеми у прикупљању дигиталних доказа

Прикупљање доказа у вези са злоупотребама дигиталне имовине представља један од најсложенијих аспеката у области дигиталне форензике и кривичноправног гоњења. Главни проблеми произилазе из техничке природе дигиталне имовине, али и из недовољно развијеног правног оквира који не прати напредак технологије. Најчешће, трансакције на блокчејн мрежама се извршавају преко криптографски заштићених адреса, без директне везе са идентитетом корисника (псеудонимност). Ово значи да, чак и ако је трансакција јавно доступна у блокчејн евиденцији, идентификација стварне особе захтева додатне техничке и оперативне мере. Приватни новчићи као што је Monero (XMR) користе напредне технологије као што су RingCT (Ring Confidential Transactions) и stealth адресе, што онемогућава праћење трансакција чак и уз приступ јавном кључу. Ово практично чини традиционалне методе праћења бескорисним без приступа софистицираним аналитичким алатима и сарадње са пружаоцима услуга.⁴⁰ Други значајан проблем је недостатак стандардизованих правних процедура за прикупљање, верификацију и коришћење дигиталних доказа у кривичном поступку. У већини правних система не постоји јединствена регулатива која дефинише валидност доказа из блокчејн извора, што доводи до правне несигурности и потенцијалног искључивања доказа пред судом. Упоредна пракса показује да неке државе, попут Немачке и Естоније, уводе форензичке стандарде за блокчејн анализу, док у другим државама недостаје обучено особље и техничка опрема. На пример, у Србији још увек не постоји, у оквиру тужилачких структура, специјализована јединица за анализу криптовалутних трансакција, што додатно отежава праћење и документовање дигиталног криминала. Поред тога, правна заштита приватности и података често долази у конфликт са потребом државе за истрагом. Без адекватних механизма балансирања ових интереса, поједине активности истражних органа могу бити оспорене због кршења људских права.

3.3.2. Форензичке методе у праћењу трансакција на блокчејну

Форензичка анализа блокчејн технологије постала је незаменљив инструмент у истраживању и доказивању криминалних активности повезаних са дигиталном имовином. Иако је блокчејн по природи децентрализован и

40 S. Ali Turab, "Monero: The Cryptocurrency That Defies Forensic Analysis", *Medium*, *Monero: The Cryptocurrency That Defies Forensic Analysis | by Syed Ali Turab | Mar. 2025 | Medium*, 10. април 2025.

псеудониман, свака трансакција остаје трајно забележена на јавно доступној књизи, што омогућава ретроспективну анализу токова средстава. Употребом напредних форензичких алата, као што су Chainalysis, CipherTrace, Elliptic, и TRM Labs, истражни органи и надзорна тела могу: пратити токове дигиталне имовине кроз различите новчанике, чак и када се користе сложене технике замагљивања као што су миксери и тумблери; повезати трансакције са криминалним активностима, укључујући хаковања, рансомвер нападе, преваре и финансирање тероризма, идентификовањем „тагованих“ адреса повезаних са претходним инцидентима; идентификовати везе између учесника у трансакцијама, применом анализа мрежне топологије и кластерисањем адреса које припадају истом ентитету.⁴¹ Ове методе су већ примењене у неколико значајних случајева. На пример, у истрази напада на берзу Bitfinex из 2016. године, амерички органи за спровођење закона су 2022. године, уз помоћ форензичких анализа, идентификовали учиниоце и запленили више од 94.000 BTC (у вредности од преко 3,6 милијарди USD), што представља једну од највећих конфискација у историји крипто сектора.⁴² Поред тога, интеграција ових алата у рад финансијских институција и регулатора омогућава рано откривање ризичних активности и повећава капацитете за спречавање прања новца и финансирања тероризма. У неким државама, попут САД и Велике Британије, овакве технологије су већ институционализоване у оквиру агенција као што су FinCEN и NCA.

3.3.3. Улога међународне сарадње у гоњењу учинилаца

Прекогранична природа трговине дигиталном имовином представља изазов у области кривичноправног гоњења, јер већина активности повезаних са злоупотребама – укључујући прање новца, финансирање тероризма и хакерске нападе – обухвата више држава, различите правне системе и техничке режиме. Ефективан одговор на ове изазове захтева развијену, континуирану и институционализовану међународну сарадњу. Елементи ове сарадње су различити: међународне организације као што су INTERPOL и EUROPOL играју кључну улогу у координацији активности између националних агенција. Оне омогућавају брз пренос података, техничку подршку и приступ међународним базама података о крипто-новчаницима повезаним са криминалним активностима. На пример, у оквиру програма EUROPOL's EC3 (European Cybercrime Centre), успостављена је специјализована јединица за прањење и анализу трансакција дигиталне имовине. У случајевима када се осумњичени или осуђени налазе у државама које нису место извршења дела, екстрадициони споразуми постају кључан

41 Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, Publications Office of the European Union, Luxembourg, 2023.

42 D. Nelson, N. De, "US Officials Seize \$3.6B in Bitcoin From 2016 Bitfinex Hack", *CoinDesk*, 2022, [US Officials Seize \\$3.6B in Bitcoin From 2016 Bitfinex Hack](#), 10. април 2025.

инструмент за спровођење правде. Србија је потписница више од 30 билатералних и мултилатералних споразума о правној помоћи и екстрадицији, укључујући и Европску конвенцију о екстрадицији (1957). Разлике у дефиницијама дигиталне имовине, различитим процедурама за прикупљање и употребу дигиталних доказа, као и различитим стандардима одговорности, могу значајно успорити правосудну сарадњу. Због тога је од суштинске важности усклађивање националних закона са међународним стандардима – као што су препоруке FATF-а, MICA регулатива у ЕУ, и иницијативе UNODC.⁴³ Према извештају EUROPOL-а из 2023. године, више од 80% криминалних активности повезаних са криптовалутама укључује трансакције у више од једне јурисдикције, што додатно наглашава неопходност појачане сарадње међу државама у области размене података, идентификације учинилаца, прикупљања доказа и извршења судских одлука.⁴⁴

3.4. Изазови у прекограничном гоњењу кривичних дела

3.4.1. Негоспољак јединствене јурисдикције за дигиталну имовину

Један од изазова у борби против прекограничних злоупотреба дигиталне имовине представља одсуство јасно дефинисане и униформне јурисдикције. Дигитална имовина – као што су криптовалуте, токени или дигитални уговори – оперише на глобалним децентрализованим мрежама које не познају физичке или административне границе. Трансакције на блокчејну могу обухватати више актера из различитих држава: иницијатор трансакције може бити у једној земљи, дигитална платформа у другој, а пријемник средстава у трећој. Поред тога, сама инфраструктура (нпр. чворови блокчејна) често је распоређена на више континената, што додатно усложњава идентификацију надлежности за конкретан случај. У складу са принципима класичног међународног кривичног права, примена јурисдикције заснива се на локацији учињеног дела, националности учиниоца или жртве, или интересима државе. У случају дигиталне имовине, ови критеријуми често нису лако применљиви, што доводи до проблема у утврђивању надлежности, почетка истраге и правног гоњења. Додатни изазов представља чињеница да значајан број држава још увек нема уређене прописе који препознају дигиталну имовину као предмет права или као основу за изрицање кривичне санкције. У многим јурисдикцијама, криптовалуте нису дефинисане ни као имовина, ни као средство плаћања, што онемогућава примену традиционалних механизма кривичне одговорности.

43 Europol, *op. cit.*, UNDOC, *Manual on Mutual Legal Assistance and Extradition*, UN, New York, 2012.

44 Sirius EU electronic evidence situation report, The Hague, 2023.

3.4.2. Проблеми у екстрадицији и координацији истрага

Екстрадиција осумњичених за злоупотребе дигиталне имовине представља озбиљан правни и политички изазов у контексту међународне сарадње. Основна препрека произилази из недостатка правне усаглашености у погледу дефинисања кривичних дела која укључују дигиталну имовину. Док једне државе класификују одређене облике понашања као кривична дела (нпр. нерегистровани ICO, коришћење анонимних криптовалута), друге их не третирају као кажњиве радње или уопште не препознају дигиталну имовину као предмет регулисања. У складу са принципом „двоструке инкриминације“ који се примењује у већини екстрадиционих уговора, лице се може изручити само ако је дело за које се терети кажњиво и у земљи тражиоцу и у земљи која извршава екстрадицију. Овај услов често представља препреку у предметима дигиталног криминала, јер не постоји јединствени глобални стандард о кривичноправном третману дигиталне имовине. Координација истрага такође је веома сложен процес из следећих разлога. Праћење трансакција које обухватају више држава захтева сарадњу међу техничким тимовима, приступ глобалним блокчејн анализаторима и форензичким платформама, као и интеграцију националних информационих система. Примери као што су операције „Operation Disruptor“ (коју су заједно водили Europol и FBI) показују да успех зависи од нивоа технолошке усклађености.⁴⁵ Неусаглашеност у правилима о купувању, верификацији и прихватању дигиталних доказа доводи до проблема у њиховој употребљивости у судским поступцима. У неким земљама није дозвољено коришћење података добијених без судске наредбе, док друге допуштају ширу примену истражних овлашћења. Упоредна анализа показује да механизми као што су Европска истражна наредба (ЕИО), Европска конвенција о узајамној правној помоћи и платформе за заједничке истраге (Joint Investigation Teams – JITs) доприносе побољшању сарадње, али нису доступни свим државама, нити обухватају све облике дигиталног криминала. Потребно је да се развије систем брзог реаговања за истраге повезане са дигиталном имовином, укључујући: увођење униформних правила о дигиталним доказима; ажурирање екстрадиционих споразума ради укључивања нових кривичних дела; специјализована обука истражних органа и тужилаштва.

45 Операција „Disruptor“ из 2020. године представља значајан пример успешне међународне сарадње у борби против трговине дрогом на дарк вебу. Координирана од стране америчког Министарства правде, ФБИ-а, DEA, ICE, и у сарадњи са Europol-ом, ова операција резултирала је хапшењем 179 особа широм света, запленом 500 килограма дрога и конфискацијом 6,5 милиона долара у готовини и криптовалутама. Успех операције био је омогућен захваљујући заједничком раду техничких тимова, употреби напредних форензичких алата за анализу блокчејн трансакција и интеграцији информационих система различитих држава.

4. ПРЕПОРУКЕ ЗА УНАПРЕЂЕЊЕ РЕГУЛАТИВЕ И ПРАКСЕ

4.1. Регулотива на националном нивоу

4.1.1. Предлози за унајређење законских оквира за дигиталну имовину у Србији

Постојећи законски оквир у Републици Србији, утврђен ЗДИ, представља значајан корак ка институционализацији тржишта дигиталне имовине. Ипак, у пракси су уочене бројне празнине и недоумице које указују на потребу за даљим унапређењем и прецизирањем појединих одредби. Закон би требало допунити јасним обавезама за све категорије VASP-а – укључујући оператере берзи, кастодијалне новчанике и пружаоце саветодавних услуга – у погледу одговорности за безбедност трансакција, чување средстава клијената, и обавештавање о сумњивим активностима. Предложено је доношење посебног подзаконског акта који би детаљно уредио техничке и организационе стандарде за ове субјекте. Иако је Закон о спречавању прања новца и финансирања тероризма⁴⁶ примењив и на дигиталну имовину, потребно је ускладити процедуре идентификације (KYC), праћења трансакција и извештавања с новим облицима дигиталних услуга, укључујући децентрализоване финансије (DeFi) и неконвенционалне токене. Примена FATF препорука у пракси треба бити ревидирана кроз извештај о ефикасности мера. Потребно је увести обавезу јавног регистра свих лиценцираних пружалаца услуга дигиталне имовине, као и успостављање механизма за надзор и објављивање података о трговању, ликвидности и примењеним безбедносним протоколима. Регулаторна тела као што су Комисија за хартије од вредности и Народна банка Србије треба да добију проширена овлашћења за инспекцијски надзор над овим сектором. Потребно је увести одредбе које предвиђају обештећење инвеститора у случајевима доказаних превара, хаковања платформи или кршења дужне пажње од стране VASP-ова. Такође, требало би размотрити могућност успостављања гарантног фонда за кориснике лиценцираних платформи. Регулаторни оквир у Србији треба динамичније усклађивати са прописима Европске уније, посебно у светлу имплементације MiCA регулативе. Потребно је дефинисати прелазне рокове и процедуре за признавање страних лиценци и сарадњу са регулаторима других држава

4.1.2. Јачање сарадње између регулаторних и правосудних органа

Ефикасна и правовремена борба против злоупотреба у области дигиталне имовине захтева развијен механизам институционалне сарадње

46 Службени гласник РС, бр. 113/2017, 91/2019, 153/2020, 92/2023, 94/2024 и 19/2025.

између регулаторних тела и правосудних органа. У Републици Србији, улоге у овом процесу имају Комисија за хартије од вредности, Народна банка Србије, Управа за спречавање прања новца, Министарство унутрашњих послова, јавна тужилаштва и судови.⁴⁷ Међусобна координација ових тела тренутно је недовољно формализована, што доводи до кашњења у обради предмета и смањене ефикасности у истрагама. Мере за јачање сарадње могу бити: успоста-вљање формалног механизма за редовне координационе састанке између представника регулаторних и правосудних институција, са фокусом на иден-тификацију ризика, размену оперативних података и процену појавних облика нових злоупотреба. Поред тога, потребно је организовати специјализоване обуке за судије, тужиоце и инспекторе у области финансијске форензике, блокчејн технологија и примене криптографије у истражним радњама. Неопходно је формирати заједничке радне групе сачињене од представника Комисије за хартије од вредности, Управе за спречавање прања новца, Јавног тужилаштва за организовани криминал и Министарства унутрашњих послова. Ови тимови би били задужени за брзу идентификацију високори-зичних субјеката и пројеката, иницирање истрага, као и за правовремену реакцију у случају инцидента као што су хаковања берзи, нерегистровани ИСО или прање новца преко децентрализованих платформи. Неопходно је дефинисати јединствене интеринституционалне протоколе за размену пода-така, прикупљање доказа и извештавање о сумњивим активностима.⁴⁸ Ово би омогућило ефикаснији рад и смањило ризик од дуплирања надлежности или пропуста у комуникацији. Регулаторна и правосудна тела у Србији треба да интензивније учествују у међународним радним групама и иницијативама попут Европске банкарске агенције (ЕБА), Европске мреже за финансијску форензику и UNODC форума за дигиталну безбедност.⁴⁹

4.1.3. Успешни примери регулативе из иностранства применљиви у Србији

Искуства других држава које су раније приступиле регулисању тржишта дигиталне имовине могу представљати значајан извор смерница за унапређење српског законодавства. Примери успешне регулативе у ино-странству указују на важност флексибилности, технолошке неутралности и јасно дефинисаних надлежности регулаторних тела.

- *Евројска унија – Регулатива MiCA*: Овај свеобухватни правни оквир дефинише лиценцирање, транспарентност, обавезе према инвеститорима и управљање ризицима у области дигиталне имовине. Србија

47 Стратегија за борбу против прања новца и финансирања тероризма у Републици Србији (2020–2024), *Службени гласник РС*, бр. 14/2020.

48 FATF, *Best Practices on Combating the Abuse of Virtual Assets*, 2023.

49 European Banking Authority, *Guidelines on cooperation between competent authorities*, 2022.

би могла применити концепт јединствене дозволе за пружаоце услуга дигиталне имовине, као и обавезу издавања белих књига за сваки токен који се нуди јавности.

- *Јапан – Закон о илајним услујама (Payment Services Act)*: Јапан је рано увео лицензирање крипто берзи и обавезне мере чувања средстава клијената. Поред тога, агенција за финансијске услуге (FSA) редовно врши надзор и издаје упозорења. Србија би могла применити модел обавезне сегрегације клијентских и оперативних средстава као средство заштите инвеститора.⁵⁰
- *Сингапур – Закон о илајним услујама (Payment Services Act 2019)*: Сингапур нуди флексибилан режим лицензирања са више нивоа, који се прилагођава ризичности активности. Такође, Сингапурска монетарна управа (MAS) снажно подстиче иновације кроз Sandbox програм, што је модел који би могао бити примењен и у Србији за контролисано тестирање нових производа и услуга.⁵¹
- *Швајцарска – FINMA смернице за ICO и дигиталну имовину*: Швајцарска је применила правну категоризацију токена на три врсте: платни, имовински и кориснички. Такав модел олакшава одређивање регулативе која се примењује. У Србији би било корисно увести сличну категоризацију ради прецизнијег регулаторног третмана појединих облика дигиталне имовине.⁵²
- *САД – SEC/CFTC надлежности и преседани*: Иако правни режим у САД није унификован, искуства SEC-а у санкционисању нерегистрованих ICO-а, као и пресуде у предметима попут SEC v. Ripple, указују на значај судске праксе као извора права. Србија би могла развити базу административне и судске праксе у вези са дигиталном имовином као инструмент правне сигурности.⁵³

4.2. Унапређење међународне сарадње

С обзиром на глобалну природу тржишта дигиталне имовине и све чешће прекограничне злоупотребе, неопходно је успоставити уједначене међународне правне стандарде који ће омогућити ефикасније спречавање и гоњење кривичних дела, као и већи ниво заштите инвеститора и финансијског система. Међународна заједница треба да усагласи терминологију и правне дефиниције кривичних дела као што су манипулација на тржишту, прање новца и финансирање тероризма у контексту дигиталне имовине. Недостатак хармонизације често доводи до правних празнина и омогућава

50 Payment Services Act (Japan).

51 Payment Services Act (Singapore).

52 FINMA, *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, 2018.

53 SEC v. Ripple Labs Inc., No. 20 Civ. 10832 (S.D.N.Y.).

учиниоцима да искористе регулаторне разлике између држава. Потребно је развити униформне протоколе за прикупљање, анализу и дељење података о трансакцијама. Ово обухвата примену „Travel Rule“ стандарда ФАТФ-а, развој универзалних формата за размену информација и поступке за пријаву сумњивих активности (Suspicious Transaction Reports – STR). Успостављање нових мултилатералних споразума који конкретно обухватају дигиталну имовину омогућило би бржу екстрадицију и примену заједничких истрага. У том смислу, улога УН-а, Групе седам (G7) и Међународног монетарног фонда (ММФ) је кључна у иницирању консензуса међу државама. Неопходно је обезбедити платформе за обуку, размену знања и технолошку подршку мање развијеним државама како би могле ефикасно да учествују у међународним истрагама.

Ефикасно сузбијање криминалних активности повезаних са дигиталном имовином у великој мери зависи од способности држава да координисано делују у прекограничним истрагама. Различити регулаторни оквири, недовољна размена података и ограничене могућности екстрадиције често омогућавају учиниоцима да избегну одговорност користећи јурисдикцијске празнине.⁵⁴ Неопходно је унапредити коришћење постојећих међународних платформи као што су INTERPOL-ова база података I-24/7 и EUROPOL-ов Систем за анализу криминалних података (SIENA). Ове мреже омогућавају правовремену и безбедну размену обавештајних и оперативних података о трансакцијама, осумњиченим лицима и повезаним платформама. Србија би требало да убрза закључивање споразума о правној помоћи у кривичним стварима са земљама у којима делују главни пружаоци услуга дигиталне имовине. Поред тога, потребно је активно учешће у иницијативама као што је Будимпештанска конвенција о сајбер-криминалу, као и формирање заједничких истражних тимова (Joint Investigation Teams – JITs) у сарадњи са ЕУ и другим партнерским државама. Предлаже се оснивање националне контакт тачке за дигитални криминал у оквиру Министарства унутрашњих послова или Управе за спречавање прања новца, која би била задужена за координацију захтева за међународну правну помоћ, екстрадицију и имплементацију заједничких акција. Кроз споразуме би требало уградити механизме који обавезују државе потписнице да у одређеним роковима доставе податке или изврше одређене истражне радње, чиме се смањују кашњења у поступку.

4.3. Превентивне мере

4.3.1. Едукација инвеститора о ризицима цифровине дигиталном имовином

Подизање свести о ризицима и комплексностима улагања у дигиталну имовину представља основу превентивне стратегије у борби против

54 Financial Markets Law Committee, *Digital Assets: Governing Law and Jurisdiction*, 2024, 16–17.

злоупотреба на тржишту. Недовољна информисаност грађана, као и лакоћа приступа дигиталним платформама, чине инвеститоре посебно рањивим на манипулације, преваре и незаконите шеме.⁵⁵ Регулаторна тела попут Комисије за хартије од вредности, у сарадњи са образовним институцијама и организацијама цивилног друштва, треба да организују редовне кампање усмерене на информисање јавности о ризицима, правним последицама и начинима заштите приликом трговања дигиталном имовином. Ови програми би обухватили теме као што су препознавање инвестиционих превара, основних безбедносних принципа и процена поузданости платформи. Припрема прегледних и јасних водича који ће објашњавати основне концепте дигиталне имовине, ризике улагања, правне обавезе и заштитне механизме такође може бити од користи. Материјали би требало да буду доступни у електронској и штампаној форми, као и кроз кратке видео-формате на друштвеним мрежама и веб-платформама државних институција. Увођење теме дигиталне финансијске писмености у средњошколске и универзитетске програме из економије, права и информационах технологија, с циљем развоја критичког приступа и раног препознавања финансијских ризика међу младима може бити више него корисна. Од значаја је и сарадња са медијима и друштвеним мрежама ради идентификације и уклањања лажних инвестиционих огласа и промоције проверених информација.⁵⁶

4.3.2. Јачање контроле над берзама дигиталне имовине и пружаоцима услуга

Како би се обезбедила већа правна сигурност и заштита инвеститора, неопходно је унапредити надзорни и регулаторни режим у погледу деловања пружалаца услуга дигиталне имовине (VASPs), са посебним фокусом на берзе, кастодијалне платформе и посреднике у трансакцијама. Потребно је утврдити виши праг техничких, финансијских и организационих услова за добијање и одржавање лиценце. То укључује проверу стручности руководства, присуство одговарајућих безбедносних протокола, као и способности у управљању ризицима. Надлежни треба да редовно спроводе инспекције и ванредне контроле. Пружаоци услуга треба да подлежу редовним ревизијама усклађености са прописима о спречавању прања новца, заштити података и безбедности система. Такође, потребно је да постоји обавеза подношења периодичних извештаја о активностима, обиму трговања и примени KYC/AML мера. Од значаја може бити и увођење независне процене сајбер-безбедности платформи, са сертификатима који

55 Вид. F. Eigelshoven, U. André, P. Douglas, "Cryptocurrency Market Manipulation: A Systematic Literature Review", *Forty-Second International Conference on Information Systems*, Austin, 2021, 4–10.

56 IOSCO, *Investor Education and Financial Literacy: Guidance on Good Practices*, 2020.

потврђују усклађеност са међународним безбедносним стандардима (нпр. ISO/IEC 27001). Платформе би требало да јавно објављују податке о на-
кнадама, условима трговања, правилима о ликвидацији и управљању сред-
ствима клијената.

4.3.3. Улога и одговорност медија у превенцији злоупотреба

Медији имају улогу у подизању јавне свести и превенцији злоупотреба у вези са дигиталном имовином. Њихова способност да брзо и масовно информишу јавност омогућава благовремено реаговање на појаву превара, манипулација и других нерегуларности.⁵⁷ Медији треба да се уздрже од сензационализма и објављивања непроверених инвестиционих савета. Уместо тога, пожељно је заснивати извештавање на подацима из званичних извора и стручних анализа, што би помогло у формирању реалних очекивања инвеститора. Објављивањем едукативних текстова, интервјуа са стручњацима и анализа регулативе, медији могу допринети бољем разумевању дигиталне имовине, њених предности, али и ризика. Истраживачко новинарство усмерено на откривање лажних шема, нерегистрованих платформи и манипулативних пракси игра важну улогу у превенцији губитака и заштити грађана. Медији би требало да сарађују са државним органима у објављивању упозорења, јавних саопштења и спискова нерегистрованих или потенцијално ризичних субјеката.⁵⁸

5. ЗАКЉУЧАК

Дигитална имовина, као нова класа актива на тржишту капитала, доноси значајне иновације, али истовремено отвара простор за нове облике злоупотреба које постојећи правни и регулаторни оквири често не успевају адекватно да обухвате. Изазови као што су манипулације на тржишту, прање новца, финансирање тероризма, као и сложеност прикупљања дигиталних доказа и прекограничног кривичног гоњења, указују на потребу за свеобухватним приступом који интегрише тржишну регулативу и кривичноправне механизме. Налази овог рада показују да је ефикасна борба против злоупотреба могућа само кроз синергију између регулаторних мера и примене кривичног права, где регулатива обезбеђује транспарентност и заштиту инвеститора, а кривично право делотворно санкционисање незаконитих активности. Правна сигурност, поверење учесника на тржишту и

57 OECD, *The Role of the Media in Promoting Financial Education and Consumer Protection*, 2022.

58 Савет за штампу Републике Србије, *Прейоруке за извештавање о финансијским шемама*, 2020.

превенција злоупотреба могу се остварити једино уколико ова два система делују усклађено и међусобно се допуњују и подржавају.

У том контексту, будућа истраживања треба да буду усмерена на развој глобалних стандарда за дигиталну имовину, укључујући усклађивање правних оквира, анализу утицаја нових технологија попут децентрализованих финансија и приватних блокчејн мрежа, као и на систематску обраду упоредноправних примера из праксе. Само кроз овакве анализе могуће је развити ефикасне и отпорне правне механизме који ће одговорити на ризике и изазове савременог дигиталног тржишта капитала.

ЛИТЕРАТУРА

- Werbach K., "Digital Asset Regulation: Peering into the Past, Peering into the Future", *William & Mary Law Review*, 4/2022–2023.
- Eigelshoven F., André U, Douglas P., "Cryptocurrency Market Manipulation: A Systematic Literature Review", *Forty-Second International Conference on Information Systems*, Austin, 2021.
- Јованић Т., „Крипто-имовина као пример утицаја дигитализације на право и праксу регулаторних органа“, *Међународна научна конференција „Право и дигитализација“*, *Зборник радова*, Правни факултет Универзитета у Нишу, Ниш, 2021.
- Lehmann M., "Digital Assets in The Conflict of Laws: A Comparative Search for The Ideal Rule", *Singapore Journal of Legal Studies*, Online Edition, 2024.
- Li T., Shin D., Wang B., "Cryptocurrency Pump-and-Dump Schemes", *Journal of Financial and Quantitative Analysis*, 2025.
- Mirković P., "Digital assets – a legal approach to the regulation of the new property law institute", *LAW – theory and practice*, 40/2023.
- Поповић У., „Дисруптивни потенцијал блокчејн технологије за унапређење међународне правне сарадње у кривичним стварима“, *Зборник радова са међународне научне конференције „Однос међународној кривичној и националној кривичној права“*, Том II, Београд, 2024.
- Stojić Dabetić J, Mirković P., „Digitalna imovina – novo poglavlje u regulisanju imovinskih prava“, *XXI međunarodni naučni skup „Pravnički dani – Prof. dr Slavko Carić“*, *Odgovori pravne nauke na izazove savremenog društva*, Novi Sad, 2024.
- Stojić Dabetić J., Mirković P., *Ugovaranje i ugovorno pravo u digitalnom društvu*, Правни факултет за привреду и правосудје у Новом Саду, Нови Сад, 2022.
- Трајковић К., „Лиценцирање и надзор у области дигиталне имовине“, *Зборник радова Народне банке Србије*, 2/2022, Београд.
- Hamrick J. T. et al. "An examination of the cryptocurrency pump and dump ecosystem", *Ecosystem*, 2019.
- Houy S., Schmid P., Bartel A., "Security Aspects of Cryptocurrency Wallets – A Systematic Literature Review", *ACM Computing Surveys*, 1/2023.

ИНТЕРНЕТ ИЗВОРИ

- Ali Turab S., “Monero: The Cryptocurrency That Defies Forensic Analysis”, *Medium*, *Monero: The Cryptocurrency That Defies Forensic Analysis | by Syed Ali Turab | Mar, 2025 | Medium*, 2025.
- APNews, “German investigators take down crypto money laundering site”, <https://apnews.com/article/germany-cryptocurrency-money-laundering-darknet-4f0c402eddec3ffa57eb00df205a2ef4>.
- Binance News, “Global Cryptocurrency Market Value Surpasses \$3.37 Trillion, Bitcoin Dominates with 56.8% Share”, https://www.binance.com/en/square/post/12-27-2024-global-cryptocurrency-market-value-surpasses-3-37-trillion-bitcoin-dominates-with-56-8-share-18126760852378?utm_.
- Chainalysis, “DeFi Takes on Bigger Role in Money Laundering But Small Group of Centralized Services Still Dominate”, 2022, https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/?utm_.
- Chainalysis, “United States DOJ and FBI Seize Cryptocurrency in Major Disruption of Hamas Terrorist Financing Scheme”, 2025, *DOJ Seizes Crypto in Disruption of Hamas Terrorist Financing Scheme*.
- Europol, “9 drug traffickers arrested and EUR 27 million in cryptocurrencies seized”, <https://www.europol.europa.eu/media-press/newsroom/news/9-drug-traffickers-arrested-and-eur-27-million-in-cryptocurrencies-seized>.
- Financial Action Task Force (FATF) Travel Rule, 2024, <https://www.sanctions Scanner.com/blog/financial-action-task-force-fatf-travel-rule-140>.
- Grace Garnett A., “Digital tokens: 8 types of crypto coins”, *Britannica Money*, 2024, <https://www.britannica.com/money/what-are-stablecoins>.
- Hedera, “TradFi and DeFi: Key Differences”, <https://hedera.com/learning/decentralized-finance/tradfi>.
- Investopedia, “Digital Asset: Meaning, Types, and Importance”, 2024, https://www.investopedia.com/terms/d/digital-asset-framework.asp?utm_.
- Nelson D., De N., “US Officials Seize \$3.6B in Bitcoin From 2016 Bitfinex Hack”, *CoinDesk*, 2022, *US Officials Seize \$3.6B in Bitcoin From 2016 Bitfinex Hack*.
- SEC, *Reports and Publications*, <https://www.sec.gov/reports>.
- Stojadinović M., „Koliko su podaci korisnika na Blockchainu zaista privatni?“, *Webmind*, 2023, https://web-mind.rs/blokcejn/koliko-su-podaci-korisnika-na-blockchainu-zaista-privatni/?utm_.
- Šmirmaul M., „Kriptot tržište se hladi – je li sad vrijeme za kupovinu?“, *Bloomberg Adria*, 2025, https://hr.bloombergadria.com/trzista/crypto/72147/kriptotrziste-se-hladi-je-li-sad-vrijeme-za-kupovinu/news?utm_.

ПРАВНИ ИЗВОРИ, ИЗВЕШТАЈИ, ПРАВИЛНИЦИ

- European Banking Authority, *Guidelines on cooperation between competent authorities*, 2022.

Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, Publications Office of the European Union, Luxembourg, 2023.

Закон о алтернативним инвестиционим фондовима, *Службени гласник РС*, бр. 73/2019 и 94/2024.

Закон о дигиталној имовини, *Службени гласник РС*, бр. 153/2020.

Закон о спречавању прања новца и финансирања тероризма, *Службени гласник РС*, бр. 113/2017, 91/2019, 153/2020, 92/2023, 94/2024 и 19/2025.

Закон о тржишту капитала, *Службени гласник РС*, бр. 129/2021.

IOSCO, *Investor Education and Financial Literacy: Guidance on Good Practices*, 2020.

Кривични законик, *Службени гласник РС*, бр. 85/2005, 88/2005 – испр., 107/2005 – испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 и 94/2024.

Национална процена ризика, *Процена ризика од прања новца*, Министарство финансија, Управа за спречавање прања новца, 2024.

Одлука о обављању плаћања у девизама у вези с трансакцијама с дигиталном имовином, *Службени гласник РС*, бр. 49/2021.

OECD, *The Role of the Media in Promoting Financial Education and Consumer Protection*, 2022.

Правилник о методологији за извршавање послова у складу са законом о спречавању прања новца и финансирања тероризма, *Службени гласник РС*, бр. 80/2020 и 18/2022.

Payment Services Act (Japan).

Payment Services Act (Singapore).

Савет за штампу Републике Србије, *Прейоруке за извештавање о финансијским темама*, 2020.

Sirius EU electronic evidence situation report, The Hague, 2023.

Стратегија за борбу против прања новца и финансирања тероризма у Републици Србији (2020–2024), *Службени гласник РС*, бр. 14/2020.

Subcommittee on Digital Assets, Financial Technology, and Inclusion Hearing: “Crypto Crime in Context Part II”, Memorandum, 2024, [HHRG-118-BA21-20240215-SD002.pdf](#).

UNDOC, *Manual on Mutual Legal Assistance and Extradition*, UN, New York, 2012.

Financial Action Task Force (FATF), *Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers*, 2024.

Financial Action Task Force (FATF), *Best Practices on Combating the Abuse of Virtual Assets*, 2023.

Financial Markets Law Committee, *Digital Assets: Governing Law and Jurisdiction*, 2024.

FINMA, *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, 2018.

Chainalysis, *The 2024 Crypto Crime Report*, 2024.

Chainalysis, *The 2025 Crypto Crime Report*, 2025.

Uroš Popović*

CRIMINAL LIABILITY IN THE TRADE OF DIGITAL ASSETS ON THE CAPITAL MARKET

Summary

This paper analyzes criminal liability in the field of digital asset trading on the capital market, with a focus on the increasingly frequent abuses such as money laundering, market manipulation, terrorism financing, and investment fraud. It highlights the insufficient normative alignment of existing criminal and capital market regulations, both in the Republic of Serbia and in the broader international context. Special emphasis is placed on the role of regulatory authorities and international institutions, as well as the challenges related to the implementation of existing legal provisions. The aim of this paper is to identify, through systematic legal analysis and a comparative approach, the critical shortcomings in the current system of market protection and sanctioning of abuses. Particular attention is devoted to the role of institutions such as the Securities Commission, the National Bank of Serbia, judicial authorities, as well as international bodies such as INTERPOL and Europol. This study is intended for experts in the fields of criminal and financial law, regulators, policymakers, and the academic community, with the goal of providing a systematic insight and encouraging concrete measures for a timely and effective response to the risks associated with digital assets.

Keywords: Digital Assets, Criminal Liability, Market Manipulation, Regulatory Framework, Money Laundering.

* Master of Laws and Head of the Market Participants Department at the Securities Commission of the Republic of Serbia, uros.popovic@sec.gov.rs.