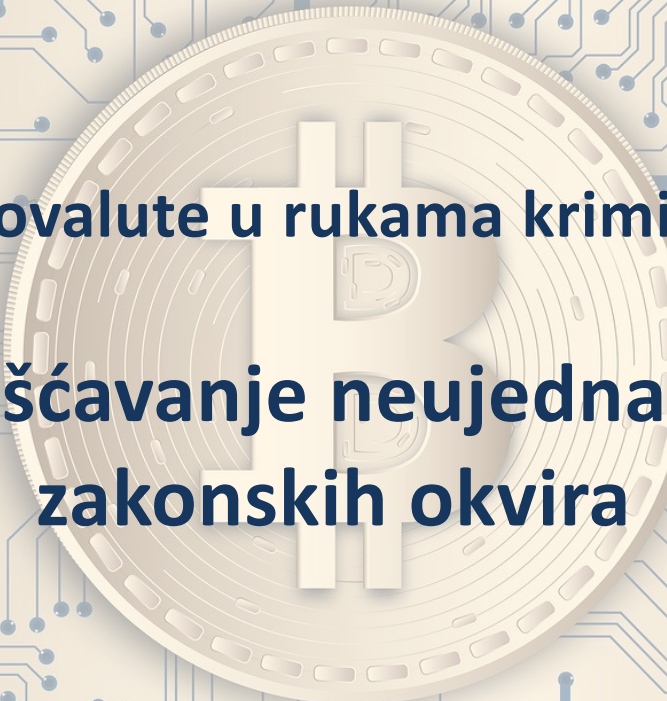




Kriptovalute u rukama kriminala: Iskorišćavanje neujednačenih zakonskih okvira

Autorka: mr Nina Vuksanović

Februar 2026. godine



Ova analiza je izrađena u okviru stipendije koju finansira Vlada Ujedinjenog Kraljevstva, kao dio programa međunarodnog razvoja, a sprovodi BIRN Crna Gora. Međutim, mišljenja i stavovi izneseni u ovoj analizi odražavaju perspektivu autora i ne predstavljaju nužno zvanične stavove britanske Vlade ili Britanske ambasade Podgorica.

Kriptovalute u rukama kriminala:

Iskorišćavanje neujednačenih zakonskih okvira

Autorka: mr Nina Vuksanović

Februar 2026. godine

Ova analiza je izrađena u okviru stipendije koju finansira Vlada Ujedinjenog Kraljevstva, kao dio programa međunarodnog razvoja, a sprovodi BIRN Crna Gora. Međutim, mišljenja i stavovi izneseni u ovoj analizi odražavaju perspektivu autora i ne predstavljaju nužno zvanične stavove britanske Vlade ili Britanske ambasade Podgorica.

Sažetak

Ovaj istraživački rad analizira načine na koje se kriptovalute zloupotrebljavaju za izvršavanje krivičnih djela, s posebnim fokusom na iskorišćavanje neujednačenih zakonskih i regulatornih okvira širom svijeta. Digitalna imovina, poput Bitcoina i tzv. stabilnih kriptovaluta (stablecoins), omogućava visok stepen pseudonimnosti i brze međunarodne transakcije, što je čini pogodnim alatom za pranje novca, finansiranje terorizma i druge oblike finansijskog kriminala. Neusklađenost regulatornih pristupa – od stroge kontrole u Evropskoj uniji do znatno labavijih pravila u pojedinim azijskim jurisdikcijama – stvara prostor za tzv. regulatornu arbitražu, u okviru koje kriminalne grupe preusmjeravaju aktivnosti u zemlje sa slabijim nadzorom.

Na osnovu analiza iz izvještaja Europol-a i Chainalysis-a, procjenjuje se da je manje od 1% ukupnog obima transakcija u kriptovalutama povezano s kriminalom, ali taj podatak obuhvata isključivo on-chain tokove i ne uključuje off-chain transakcije, OTC trgovinu ni privatne mreže. Stvarna izloženost vjerovatno je veća, naročito zbog sve češće upotrebe sofisticiranih tehnika prikrivanja porijekla imovine, kao što su mixing/tumbling servisi i chain-hopping.

U cilju ublažavanja rizika i jačanja integriteta tržišta digitalne imovine, rad ističe potrebu za globalnim usklađivanjem regulatornih standarda, produbljivanjem međunarodne saradnje i primjenom naprednih analitičkih alata za praćenje transakcija, uz istovremeno očuvanje inovativnog potencijala kripto-ekosistema.



Sadržaj

1. Uvod	5
2. Koncept kriptovaluta i njihove specifičnosti	6
3. Kriptovalute i kriminalne aktivnosti	8
4. Neujednačeni zakonski okviri	12
5. Kriminal u praksi: slučajevi zloupotrebe	14
6. Institucionalni odgovori	17
7. Policy preporuke	19
8. Zaključak	21
Literatura	23



1. Uvod

Digitalna transformacija globalne ekonomije donijela je brojne inovacije, ali sa njima i isto tako brojne rizike koji prevazilaze granice poznatog, tradicionalnog finansijskog sistema. Među njima, kriptovalute predstavljaju jedan od najdinamičnijih, ali i najkontroverznijih fenomena savremenog doba. Njihova decentralizovana priroda, tehnološka sofisticiranost i brzina transakcija učinile su ih, najprije, atraktivnim investicionim ulogom, a zatim i sredstvom razmjene i štednje. Međutim, upravo ove karakteristike čine ih pogodnim alatom za različite oblike zloupotreba, uključujući pranje novca, utaju poreza, finansiranje terorizma i sajber kriminal.

U posljednjoj deceniji, vrijednost i upotreba kriptovaluta su eksponencijalno porasle. Bitcoin, kao prva kriptovaluta, nastala 2008.-2009. godine, otvorio je vrata čitavom ekosistemu digitalnih sredstava i decentralizovanih finansijskih usluga (DeFi). Iako je razvoj ove tehnologije doprinio finansijskoj inkluziji i inovacijama, istovremeno predstavlja veliki izazov za regulatorne i bezbjednosne institucije. Nedostatak cjelovitih zakonskih rješenja, razlike u regulativi između država i ograničene insitucionalne i tehničke mogućnosti nadzora stvaraju prostor za zloupotrebe što ugrožava i ekonomske i bezbjednosne interese država i međunarodne zajednice kao cjeline.

Crna Gora, kao mala ekonomija u razvoju, nije izuzetak iz ovih globalnih trendova. Iako je prisutnost kriptovaluta u domaćem finansijskom sistemu još uvijek ograničena, njihova upotreba u regionu raste, a institucionalna spremnost za suočavanje sa rizicima ostaje nedovoljna. Posebno zabrinjava činjenica da, prema zvaničnim odgovorima crnogorskih organa na zahtjeve za slobodan pristup informacijama, ne postoje evidencije o slučajevima zloupotrebe kriptovaluta. Takvo stanje ukazuje na ozbiljan institucionalni deficit u oblasti nadzora, analitike i prevencije digitalnog kriminala.

Ovaj policy paper ima za cilj da pruži pregled ključnih aspekata odnosa između kriptovaluta i kriminalnih aktivnosti, uz fokus na izazove koji proizlaze iz neujednačenih zakonskih okvira. Poseban akcenat stavljen je na stanje u Crnoj Gori i regionu Zapadnog Balkana, kroz identifikovanje institucionalnih slabosti i formulaciju preporuka za unapređenje regulatornog i operativnog odgovora.



2. Koncept kriptovaluta i njihove specifičnosti

Kriptovalute su „digitalni oblici imovine koji se oslanjaju na šifrovane mreže za izvršavanje, verifikaciju i bilježenje transakcija, nezavisno od centralizovanih autoriteta poput vlada ili banaka“ (Britannica, 2023). Tehnički, kriptovalute se zasnivaju na *blockchain*-u – decentralizovanoj, distribuiranoj bazi podataka koja omogućava vjerodostojno, trajno i transparentno evidentiranje transakcija bez potrebe za posrednikom. Ključna ideja iza kriptovaluta jeste **povjerenje u kod, a ne u institucije** – što znači da se vjerodostojnost transakcija obezbjeđuje putem kriptografskih algoritama i konsenzusa mehanizama, a ne državnim garancijama zasnovanim na pravnim konstruktima.

2.1. Tehničke i funkcionalne osobine

Za razliku od klasičnog novca, koji izdaju centralne banke, kriptovalute nastaju kroz jedan od tri mehanizma: *Proof-of-Work* (PoW), tzv. „rudarenjem“, *Proof-of-Stake* (PoS) poznatiji kao „minting“ ili su već sve jedinice stvorene unaprijed, u ograničenoj količini („preminovane valute“). U prva dva slučaja se radi o procesu verifikacije i dodavanja novih transakcija u blockchain, za šta „rudari“ ili validatori (kod mintinga) dobijaju naknadu u vidu novih jedinica valute. Neke od kriptovaluta koje su u najširoj upotrebi su Bitcoin (BTC), Ethereum (ETH) i Tether (USDT), a u posljednjim godinama pojavile su se (i pojavljuju se) i brojne druge, uključujući tzv. *privacy coin*-e poput Monera (XMR) i Zcasha (ZEC), koji omogućavaju gotovo potpunu anonimnost učesnika. Prema jednoj od procjena iz 2024. godine (CoinMarketCap, 2024.) broj različitih valuta (i coina i tokena) bio je blizu 11 miliona, dok je broj **aktivnih i značajnih** valuta u 2025. nešto preko 17 hiljada (CoinGecko, 2025.).

Decentralizacija znači da ne postoji jedinstveni entitet koji kontroliše sistem, dok transparentnost blockchaina omogućava da svaka transakcija bude javno dostupna i provjerljiva, ali bez nužnog otkrivanja identiteta korisnika. Naime, anonimnost jeste bila jedno od osnovnih obilježja prvih kriptovaluta, ali je prestala biti inherentna (ugrađena u samu tehnologiju) oko 2013–2015. godine, kada su uvedene tehnologije, propisi i alati koji su omogućili pseudonimnost umjesto potpune anonimnosti.

2.2. Prednosti kriptovaluta

Kriptovalute svakako nude više prednosti:

- brze međunarodne transakcije,
- smanjenje troškova posredovanja,
- finansijsku inkluziju za stanovništvo bez pristupa bankama,
- otpornost na inflaciju i monetarne intervencije država.

Zahvaljujući tim karakteristikama, kriptovalute su postale privlačne i kao sredstvo plaćanja i kao investiciono sredstvo. U mnogim ekonomijama u razvoju, uključujući zemlje Zapadnog Balkana, građani ih vide i kao način zaštite od inflacije i političke nestabilnosti. Još uvijek, međutim, prednjači njihova upotreba kao investicionog instrumenta, dok je trenutno samo u jednoj zemlji na svijetu zakonsko sredstvo plaćanja.

2.3. Rizici i slabosti

Ipak, ono što kriptovalute čini inovativnim, istovremeno ih čini i rizičnim. Anonimnost, odnosno pseudonimnost, nepostojanje regulatornog nadzora i tehnička složenost stvaraju prostor za zloupotrebe. Kriptovalute se tako mogu koristiti za pranje novca i prikrivanje tragova nezakonitih transakcija, finansiranje ilegalnih aktivnosti, uključujući trgovinu narkoticima, oružjem i ljudima, izbjegavanje poreza i razne prevare i „*pump and dump*“ šeme.

Upravo zato, globalne finansijske i bezbjednosne institucije (FATF, 2023; Europol, 2024) upozoravaju da su kriptovalute istovremeno inovacija i prijetnja — inovacija u smislu demokratizacije finansija, a prijetnja zbog nepredvidivog broja mogućnosti zloupotrebe i globalnog dosega.

2.4. Crna Gora i region

U zemljama Zapadnog Balkana, koje nisu članice EU, među kojima je i Crna Gora, tržište kriptovaluta se razvija bez jasnog regulatornog okvira. Kripto-berze i platforme za razmjenu novim Zakonom o sprečavanju pranja novca i finansiranja terorizma stavljene su pod nadzor Komisije za tržište kapitala, kao jedan od više subjekata koje ova komisija nadzire, pa je pitanje koliko takav nadzor može biti djelotvoran i efikasan, a što su po FATF-ovoj Interpretativnoj napomeni uz preporuku 15 (2019.), glavne karakteristike koje adekvatan nadzorni mehanizam treba da ima. Još uvijek ne postoji centralizovani registar korisnika, iako je za njegovo uspostavljanje istim zakonom predviđen rok od devet mjeseci, koji je istekao u decembru. Ovakvom stanju imanentan je rizik od stvaranja „sive zone“ unutar finansijskog sistema, gdje se novac može kretati izvan regulisanih tokova, čime se otvara prostor da kriptovalute postanu instrument prikrivanja tokova nelegalno stečenih sredstava – naročito u kombinaciji sa *off-shore* kompanijama i pomoću platformi van domašaja lokalnih vlasti.

3. Kriptovalute i kriminalne aktivnosti

Kriptovalute su u osnovi **neutralna tehnologija**, ali njihova anonimnost, globalni karakter i neregulisanost čine ih posebno pogodnim sredstvom za različite kriminalne aktivnosti. Zbog toga su postale neizostavan segment savremenog finansijskog kriminala, a nerijetko i ključni alat za prikrivanje tragova nezakonitih aktivnosti.

Kriminalne aktivnosti koje uključuju kriptovalute mogu se grupisati u nekoliko osnovnih kategorija:

Pranje novca – pretvaranje nelegalno stečenog novca u „čist“ kapital koristeći se kompleksnim lancima transakcija preko digitalnih novčanika, kripto-mjenjačnica i „mixing“ servisa i drugih alata, kako bi se izgubili tragovi porijekla.

Finansiranje terorizma – terorističke organizacije koriste kriptovalute zbog mogućnosti da sredstva brzo i diskretno prebacuju preko granica, a zatim ih dalje koriste za potrebe organizacije svojih aktivnosti.

Prevare i finansijske piramide – zbog svoje investicione privlačnosti i entuzijazma investitora, kripto-tržište je plodno tlo za tzv. „*pump and dump*“ šeme, lažne investicione fondove i prevarne inicijalne ponude (ICO).

Ransomware napadi i sajber-kriminal – umjesto u FIAT novcu, hakeri sada traže isplate otkupnine u kriptovalutama jer se one teško prate, a zatim ih brzo konvertuju u druge oblike imovine.

Utaja poreza (i izbjegavanje sankcija u vezi sa tim) – zbog otežanog praćenja tokova kapitala i nepotpune ili neprecizne regulative, kriptovalute postaju sredstvo skrivanja prihoda i transfera sredstava ka jurisdikcijama sa blažim propisima (tzv. regulatorna arbitraža).

3.1. Mehanizmi prikrivanja tragova

Neograničene mogućnosti tehnološkog unapređivanja i modifikacije algoritama, softvera i infrastrukture, kriminalcima daju prednost u odnosu na istražne organe i organe gonjenja ali i otežavaju posao zakonodavca jer je teško unaprijed predvidjeti sve moguće načine i pravce u kojima se njihovi mehanizmi djelovanja, u ovoj sferi, mogu kretati i razvijati. Ipak, u dosadašnjoj praksi, kao najčešće korišćena tehnika izdvajaju se „*mixing*“ i „*tumbling*“ servisi, koji miješaju ili razlažu transakcije kako bi se sakrilo porijeklo sredstava i tako izgubio trag o izvornom vlasniku sredstava.

Ovi servisi su od strane EUROPOL-a i FATF-a označeni kao **visokorizični mehanizmi za pranje novca**, a neki su već zabranjeni poput *Tornado Cash*-a (Ethereum mixing servis), sankcionisan od strane SAD (OFAC) ili *Bitcoin Fog* i *ChipMixer* – ugašeni u međunarodnim policijskim akcijama. Samo korišćenje ovih servisa, uz dokaz da je svrha bila prikrivanje nezakonitog porijekla može predstavljati krivično djelo pranja novca.

Tradicionalni miks-servisi gube primat, dok se sve više koristi (samostalno ili u kombinaciji sa mixer-om) novija metoda - „*chain-hopping*“ – zasniva se na prebacivanju sredstava sa jedne blockchain mreže na drugu, putem *cross-chain-bridge*-a, a što do svega par godina unazad bilo nezamislivo (Merkle Science, 2023). Nadograđeni servis - *Cross-chain swapping* - zamjena tokena između različitih blockchain, razbija trag o porijeklu imovine, čime se dodatno otežava praćenje.

Pored ovih mehanizama, kriminalne grupe sve češće pribjegavaju upotrebi tzv. „**privacy coins**“, poput Monera (XMR), koji pružaju potpunu **transakcijsku netransparentnost**. Takve kriptovalute skrivaju ključne informacije o pošiljaocu, primaocu i iznosu transakcije, čineći ih gotovo nevidljivim za konvencionalne alate za blockchain analitiku. Time se postiže visok stepen zaštite identiteta korisnika, što predstavlja ozbiljan izazov za regulatorne i istražne organe.

Dodatni sloj složenosti uvodi i razvoj **decentralizovanih finansijskih platformi** (DeFi), koje funkcionišu bez centralnog posrednika. Ove platforme omogućavaju anonimno pozajmljivanje, ulaganje i trgovinu digitalnom imovinom, pri čemu korisnici zadržavaju potpunu kontrolu nad svojim sredstvima. Takva arhitektura otežava sprovođenje klasičnih mehanizama nadzora i usklađenosti, jer se transakcije odvijaju isključivo putem pametnih ugovora, bez identifikovanih subjekata koji bi mogli biti pravno odgovorni.

Navedeni modaliteti prikrivanja porijekla sredstava nisu u potpunosti neprobojni. Postoje brojni alati (*Chainanalysis*, *Elliptic Investigator*, *TRM Labs*, *Cellebrite Crypto Solutions*), koji su imali uspjeha u ulaženju u trag transakcija ali su njihov rad i rezultati neuporedivo sporiji u poređenju sa djelovanjem kriminalaca. Primjera radi, prosječna blockchain transakcija odvije se za 0.79 sekundi, dok je istraga jednog od najnovijih slučajeva koji je rezultirao hapšenjima i pravosnažnim presudama trajao sedam godina (Metropolitan Police, 2025).

3.2. Globalni trendovi

Prema izvještaju EUROPOL-a iz 2024. godine, vrijednost kripto-transakcija povezanih sa kriminalnim aktivnostima procjenjuje se na više od 1,8% ukupnog kripto prometa, što predstavlja desetine milijardi eura godišnje.

FATF-ove analize pokazuju da se preko 60% kripto-transakcija koje su predmet istrage odnosi na **pranje novca i ransomware napade**. Samo u prvoj polovini 2025. godine preko 2,17 milijardi dolara ukradeno je iz kripto-servisa, što je više nego za cijelu 2024. godinu. Od toga, oko 1,5 milijardi u vezi je sa samo jednim slučajem - hakom platforme *ByBit*, što pokazuje da ciljevi postaju vrlo veliki, a alati sve sofisticiraniji.

Procjena *ChainAnalysis*-a za 2024. godinu je da volumen kripto-transakcija povezanih sa kriminalom (različite kategorije) iznosi preko 51 milijarde dolara.

Sudeći po dosadašnjim rezultatima analiza, 2025. je na dobrom putu da zabilježi dvostruko više fizičkih napada nego prethodna godina sa najvećim brojem napada. Takođe je vrijedno napomenuti da, pošto mnogi napadi ostaju neprijavljeni, stvarni broj takvih incidenata je vjerovatno mnogo veći. Analiza *Chainanalysis*-a otkriva jasnu korelaciju između nasilnih incidenata i povećanje prosjeka cijene Bitcoina, što sugerise da bi buduće povećanje vrijednosti (i sama percepcija njenog budućeg uzlaznog kretanja) moglo motivisati još veći broj oportunističkih fizičkih napada na poznate vlasnike kriptovaluta.

Iako je privatnost inherentna kriptovalutama, Bitcoin i druge slične valute nisu anonimne već **pseudonimne**. *Privacy Coins* (anonimne kriptovalute) su dizajnirane da riješe problem pseudonimnosti koristeći naprednu kriptografiju. Cilj je osigurati zamjenjivost (*fungibility*) novca, tretiranjem svake jedinica valute jednako, bez obzira na njenu prethodnu istoriju (za razliku od Bitcoina, gdje se BTC povezan s kriminalom može označiti kao "toksičan" i biti odbijen od strane regulisanih mjenjačnica). Trend pokazuje porast korišćenja anonimnijih valuta poput Monera, Zcash-a i Dash-a, posebno u sferi „dark-web“ tržišta, zbog čega su regulisane mjenjačnice (poput Coinbase-a ili Binance-a u nekim jurisdikcijama) prinuđene da delistiraju anonimne coine kako bi ostale u skladu sa strogim AML propisima.

Veliki izazov predstavljaju *Over-The-Counter* transakcije (OTC) što bukvalno znači „preko šaltera“, a u kontekstu kriptovaluta to označava trgovinu van berze, direktno između dvije strane, bez posredstva javne platforme. Iako OTC deskovi spadaju pod KYC/AML, transakcija se sprovodi off-chain (nije vidljiva u order book-u) dok se ne izvrši prenos, a moguće je kombinovanje (u esrow međufazi) fiat i kripto valuta, što mijenja strukturu transakcije i otežava uspostavljanje veze između pošiljaoca i primaoca.

Ono što se iz brojnih izvještaja izvodi kao zajednički zaključak jeste da pravni okvir širom svijeta ne prati tempo tehnoloških promjena.

3.3. Kripto kriminal u regionu i Crnoj Gori

U regionu Zapadnog Balkana, iako se obim kripto-tržišta još uvijek smatra umjerenim, evidentni su slučajevi prevara i drugih oblika zloupotrebe. Ipak, Srbija i Hrvatska, nakon on-site posjeta ekspertske timova MONEYVAL-a (Komitet eksperata za procjenu mjera protiv pranja novca i finansiranja terorizma Savjeta Evrope) i revizije izvještaja, sada zadovoljavaju svih 40, odnosno 36 FATF preporuka.

S druge strane, Crna Gora, nema registrovane slučajeve zloupotreba kriptovaluta u zvaničnim evidencijama, što ne znači da takvi slučajevi ne postoje, već da institucije nemaju kapacitete za njihovo prepoznavanje i evidentiranje. U odgovorima koje su dostavili nadležni organi (Ministarstvo unutrašnjih poslova - Uprava policije, Ministarstvo pravde, Specijalno i Osnovno državno tužilaštvo), navodi se da ne posjeduju evidenciju o krivičnim djelima povezanim s korišćenjem kriptovaluta, međunarodnoj pomoći u vezi sa takvim predmetima odnosno druge evidencije, koje bi proizilazile iz njihovih nadležnosti. Ovo potvrđuje i izvještaj MONEYVAL-a, u kom se navodi da *“Crna Gora ... **nema praksu za identifikaciju, praćenje, zaplenu i upravljanje virtuelnom imovinom.** Zakonodavni i operativni okviri nikada nisu testirani u tom pogledu.”* Iako je izvještaj usvojen u decembru 2023., nakon čega su stupile izmjene i dopune Zakona o sprečavanju pranja novca i finansiranja terorizma (februar 2025.), situacija se u praksi nije značajno promijenila. U istom izvještaju se takođe ističe kako određeni nalazi ukazuju na to da članovi organizovanih kriminalnih grupa već poseduju određene količine kriptovaluta, koje se koriste za kupovinu nekretnina, podrivajući mogućnost praćenja porijekla imovine. Istraživanje BIRN-a (Balkan Investigative Reporting Network) iz juna 2025. godine, pokazalo je da kupovina nekretnina i automobila kriptovalutama nije registrovana u poreskom i pravnom sistemu države, što znači da ove transakcije i dalje prolaze “ispod radara”.

Ovakav institucionalni vakuum ukazuje na odsustvo analitičkog pristupa, nedostatak specijalizovanih kadrova i tehničkih alata za digitalnu forenziku, što može predstavljati ozbiljan problem u budućnosti.



4. Neujednačeni zakonski okviri

Kriminalne aktivnosti zasnovane na kriptovalutama ugrožavaju integritet finansijskog sistema, koji počiva na praćenju i izvještavanju transakcija. Njima se destabilizuje tržište i narušava povjerenje javnosti u digitalne tehnologije. Osim negativnih ekonomskih efekata, prisutan je i bezbjednosni rizik prvenstveno zato što transferi sredstava u kriptovalutama omogućavaju finansiranje ekstremističkih grupa i sajber-napada bez klasičnih tragova u bankarskom sistemu.

Pravni tretman kriptovaluta značajno varira među državama, što stvara globalnu pravnu fragmentaciju i brojne rupe koje kriminalne strukture uspješno koriste. Dok neke zemlje pokušavaju uvesti stroge regulatorne okvire, druge i dalje nemaju jasno definisane propise (neke zato što to ne šele, druge zato što nemaju institucionalne, kadrovske, tehničke i/ili finansijske mogućnosti), što otežava nadzor, međunarodnu saradnju i sprovođenje istraga, jer su kriminalne aktivnosti povezane sa kriptovalutama po prirodi međunarodnog dometa. Tako na primjer, s jedne strane, u Sjedinjenim Američkim Državama vlada fragmentisan i neujednačen pristup - nema jedinstvenog federalnog zakona, djeluje više regulatora (SEC, CFTC, FinCEN, IRS, OFAC i državne agencije) i svi oni različito definišu i tretiraju kripto-imovinu, a kao primarni cilj postavlja se razvoj i dominacija u ovoj industriji. Tako na primjer, Komisija za hartije od vrijednosti (SEC) smatra ih investicionim instrumentima, dok ih Poreska uprava (IRS) klasifikuje kao imovinu.

S druge strane, u Evropskoj uniji, slična situacija koja je postojala do 2023. godine (države članice imale su različite režime regulacije), promijenjena je usvajanjem Uredbe o tržištima kriptoimovine (MiCA), kojom je EU uvela jedinstveni okvir koji reguliše izdavanje, trgovinu i nadzor nad kripto-sredstvima. Cilj MiCA-e je integrisati kripto u finansijski sistem, ali pod istim standardima kontrole kao tradicionalne institucije, što podrazumijeva zaštitu potrošača, smanjenje rizika od pranja novca i uspostavljanje pravne sigurnosti za tržišne aktere. Ova kompleksna uredba predstavlja najnapredniji regulatorni pristup u svijetu, kojim se pokušava izbalansirati između afirmacije inovacija i bezbjednosnog standarda.

Slično, Singapur i Švajcarska imaju vrlo jasan pristup, zbog kog su stekle reputaciju "crypto-friendly", ali i izuzetno bezbjednih destinacija za kripto ulaganja, zbog strogih KYC i AML zahtjeva.

Kina je zauzela najrestriktivniji stav – zabranila je sve aktivnosti povezane sa kriptovalutama, navodeći kao razloge zaštitu finansijskog sistema i kontrolu kapitalnih tokova. Nasuprot tome, El Salvador je uveo Bitcoin kao zvanično sredstvo plaćanja, pokazujući suprotan, liberalni pristup.

Ovakva razlika u pristupu stvara konfuziju i pravne praznine, naročito u slučajevima koji uključuju međunarodne transakcije i digitalne tokove kapitala.

4.1. Posljedice pravne fragmentacije

Neujednačenost regulative omogućava pojavu tzv. regulatorne arbitraže — izbora jurisdikcija sa liberalnijom regulativom i slabim nadzorom, u cilju izbjegavanja strožih propisa i, na taj način, akumuliranja profita. Kriminalne grupe i nelegalne platforme često koriste *off-shore* zone (npr. Sejšeli, Belize, Panamska ostrva) gdje su zakoni nejasni, a pristup informacijama ograničen.

Ovaj fenomen ima domino-efekat: zemlje sa slabim nadzorom postaju privlačne destinacije za nelegalne tokove kapitala, dok zemlje sa strožim režimima gube mogućnost potpunog praćenja.

4.3. Crna Gora: regulatorni vacuum

Crna Gora se trenutno nalazi u posebno osjetljivoj poziciji. Kao država kandidat za članstvo u EU, dužna je da uskladi svoj pravni okvir sa evropskim propisima, što je, kako se može vidjeti iz iskustva pojedinih zemalja regiona, dugotrajan proces.

U praksi, niti jedan organ nema precizne podatke o obimu trgovine kriptovalutama, broju korisnika, niti o mogućim sumnjivim transakcijama. Na upite upućene u skladu sa Zakonom o slobodnom pristupu informacijama, Uprava policije, Ministarstvo pravde i Tužilaštvo, su zvanično odgovorili da ne posjeduju evidenciju o zloupotrebama kriptovaluta. Takav odgovor jasno pokazuje da država nema izgrađen sistem praćenja digitalnih finansijskih tokova, što predstavlja ozbiljnu slabost u borbi protiv pranja novca i finansiranja terorizma. Nedostatak proaktivnog institucionalnog pristupa znači da Crna Gora rizikuje da postane „siva zona“ za kriptotransakcije koje bi mogle biti povezane sa kriminalnim strukturama iz regiona.



5. Kriminal u praksi: slučajevi zloupotrebe

Iako se kriptovalute često promovišu kao simbol tehnološkog napretka i finansijske slobode, u praksi su one postale jedno od najznačajnijih oruđa kriminalnih struktura. Slučajevi iz međunarodne i regionalne prakse pokazuju kako se prednosti decentralizacije i anonimnosti pretvaraju u mehanizme za prikrivanje nezakonitih radnji.

5.1. Međunarodni primjeri

Silk Road (SAD, 2013)

Najraniji razotkriveni primjer zloupotrebe kriptovaluta je platforma *Silk Road* - ilegalno tržište na *dark web*-u, na kojem su se prodavali narkotici, oružje i ukradeni podaci. Transakcije su se obavljale isključivo u Bitcoinu, što je omogućilo visok stepen anonimnosti učesnika, s obzirom da je *know-your-client* (KYC) i *anti-money laundering* (AML) regulativa u to vrijeme bila daleko manje razvijena. Iako je 2013. godine platforma ugašena intervencijom FBI-a, a njen osnivač, Ross Ulbricht, uhapšen, ovaj slučaj je prvi pokazao kako kriptovalute mogu omogućiti globalne kriminalne operacije bez klasičnog bankarskog posrednika.

Mt. Gox (Japan, 2014)

Nekada najveća svjetska berza za trgovinu Bitcoinom propala je nakon što je nestalo više od 850.000 Bitcoina korisnika, u tom trenutku vrijednih 450 miliona dolara. Istraga je pokazala da su sredstva pronevjerena kroz kombinaciju hakerskih napada i unutrašnjih zloupotreba, da nisu postojale evidencije o depozitima i da su kritični serverski sistemi bili slabo zaštićeni. Ovaj slučaj ukazao je na potrebu za nadzorom i osiguranjem depozita korisnika na kripto-berzama, čime su se kripto-berze i mjenjačnice počele podvoditi pod regulativu donekle analognu onoj kojoj podliježu komercijalne banke.

PlusToken (Kina, 2019)

Rigorozan regulatorni okvir Kine odgovor je na jednu od najvećih kripto-prevara, u kojoj je više od dvije milijarde dolara kapitala prikupljeno od investitora pod izgovorom ulaganja u „inovativnu platformu“. Novac je zatim prebačen u više hiljada digitalnih novčanika i kasnije konvertovan u Bitcoin i Ethereum, čime se izgubio trag porijekla. Ovaj slučaj demonstrirao je kako nedostatak međunarodnog nadzora i koordinisane akcije omogućava da prevare prelaze granice i pogađaju desetine hiljada građana. Kineske vlasti su već 2020. godine uhapsila 109 osumnjičenih povezanih sa ovom prevaram i zaplijenile kripto-sredstva u vrijednosti od oko 4,2 milijarde dolara.

FTX (Bahami/SAD, 2022)

Jedan skoriji primjer - kolaps platforme FTX, jedne od najvećih svjetskih mjenjačnica, otkrio je kako monopolistički položaj u sistemu koji funkcioniše van okvira regulisanog tržišta, stvara usove za masovnu zloupotrebu sredstava korisnika i manipulaciju tržištem. Iako FTX formalno nije kriminalna organizacija, istrage su pokazale da su interni mehanizmi kontrole potpuno izostali, a korisnici ostali bez više milijardi dolara. Ovaj slučaj je postao globalni simbol potrebe za jasnim propisima i odgovornošću u digitalnim finansijama.

5.2. Regionalni i lokalni slučajevi

U regionu Zapadnog Balkana, iako ne postoje zvanične statistike, mediji, istraživački izvještaji i izvještaji pojedinih međuvladinih institucija ukazuju na sve češću upotrebu kriptovaluta u pranju novca i finansijskim prevarama.

Izvještaj istrage sprovedene u Srbiji, u saradnji sa Eurojust-om i EUROPOL-om, pokazuje da je u januaru 2023. obavljena koordinisana akcija protiv mreže koja je iz Srbije, Bugarske i Kipra djelovala sa lažnim kripto-platformama, na koje su korisnici sredstva uplaćivali u fiat valutama, da bi ih organizatori kasnije konvertovali u kriptovalute i potom prebacivali u inostranstvo.

U decembru 2024. MUP Srbije je objavio da je zaplijenjeno oko 500.000 EUR u kriptovalutama u akciji protiv organizovane kriminalne grupe osumnjičene za prodaju nedozvoljenih doping sredstava. U ovom slučaju nije riječ o "čistom" kripto kriminalu već krivičnom djelu neovlašćena proizvodnja, držanje i stavljanje u promet opojnih droga/ljekova, a u kom se kripto valute javljaju kao sredstvo plaćanja tj. korist stečena izvršenjem. Ovo je bitno s obzirom da su se kriminalne organizacije na prostoru Zapadnog Balkana decenijama unazad isprofilisale u vršenju određenih krivičnih djela (trgovina narkoticima, oružjem i td.) tako da je za očekivati da plaćanja koja su u vezi sa tim krivičnim djelima ubuduće izvršavaju u kriptovalutama. To bi, uz adekvatnu tehničku i kadrovsku spremnost, nadležnim organima zemalja regiona, moglo olakšati otkrivanje izvršilaca, u poređenju sa ulaženjem u trag plaćanjima izvršenim keš novcem.

U Hrvatskoj, najveća kripto prevara rezultirala je hapšenjem tri osobe zbog prevare 220 ulagača u kripto valute, pri čemu su ih oštetili za najmanje 4,6 miliona eura. Optuženi su u periodu od 2018. do 2023. pozivali investiture na ulaganje, primali od njih uloge u gotovom novcu, uplatom na račun i prenosom virtuelnih valuta na digitalne novčanike, iako su znali da *BitLucky*, njihova kompanija za trgovanje kriptovalutama, neće uopšte trgovati prenesenim sredstvima.

Kada je riječ o Crnoj Gori, situacija je specifična — zvanične institucije uopšte ne vode evidenciju o slučajevima kriptokriminala. To znači da eventualne zloupotrebe, ako i postoje, prolaze “ispod radara” sistema. Takvo stanje predstavlja ozbiljan institucionalni propust jer onemogućava detekciju rizika, praćenje trendova i izradu strategija za prevenciju.

5.3. Mehanizmi prikrivanja u praksi

Analize slučajeva pokazuju da se kriminalci najčešće koriste kombinovanim metodama:

- prenos sredstava između više digitalnih novčanika prije konverzije u fiat valute,
- korišćenje tzv. mixera i tumblera za „čišćenje“ tragova,
- korišćenje decentralizovanih mjenjačnica (DEX) koje ne zahtijevaju verifikaciju korisnika (KYC),
- ulaganje sredstava u NFT-ove i DeFi platforme (npr. kroz yield farming) kako bi se prikrilo porijeklo novca i tako kapitalizovali kriminalnu dobit.

Ovakve metode otežavaju rad istražnih organa, koji su u većini zemalja regiona još uvijek tehnički i kadrovski nedovoljno opremljeni da ih otkriju.



6. Međunarodni okviri i organizacije

Na globalnom nivou, vodeću ulogu u uspostavljanju standarda imaju FATF (Financial Action Task Force), Međunarodni monetarni fond (MMF), Svjetska banka, EUROPOL i INTERPOL.

FATF je još 2019. godine u svoje preporuke uključio termin „virtual assets“ i propisao obavezu implementacije tzv. **Travel Rule**, prema kojoj svi pružaoci usluga kriptotransfera moraju identifikovati pošiljaoca i primaoca. Ova mjera ima za cilj da poveže kriptotransakcije sa stvarnim identitetima, čime se smanjuje anonimnost i rizik od pranja novca.

Međutim, FATF okuplja 37 zemalja članica, što je manje od jedne četvrtine ukupnog broja članova međunarodne zajednice, te je nerealno očekivati da sumnjivi tokovi, posebno digitalnih valuta, budu promptno detektovani i zamrznuti.

EUROPOL, u saradnji sa INTERPOL-om i nacionalnim policijama, redovno sprovodi operacije praćenja i gašenja nelegalnih platformi, a MMF i Svjetska banka pružaju tehničku pomoć državama u izgradnji regulatornih i tehničkih kapaciteta.

Međutim, i pored tih napora, globalni mehanizmi nadzora ostaju ograničeni jer ne postoji univerzalni sistem razmjene podataka o kripto-transakcijama, što omogućava kriminalcima da se kreću između različitih jurisdikcija.

6.1. Evropska unija

Evropska unija je, nakon višegodišnjih konsultacija, uspostavila sveobuhvatan regulatorni okvir kroz Uredbu o tržištima kriptoomovine (MiCA) i novi AML paket (Anti-Money Laundering Package).

MiCA uvodi jasne definicije digitalne imovine, zahtjeve za licenciranje platformi, pravila o transparentnosti i zaštiti korisnika, te obavezu nadzora od strane nacionalnih regulatora.

U okviru AML paketa, predviđeno je i osnivanje Evropske agencije za borbu protiv pranja novca (AMLA), koja će koordinirati razmjenu informacija između država članica i nadzirati rizične transakcije, a počće sa radom od 2026. godine.

Ovaj sistem bi, kada se u potpunosti implementira, trebalo da postane najnapredniji model kontrole kriptotržišta u svijetu.

6.2. Regionalni pristupi

Na Zapadnom Balkanu, institucionalni odgovori su neravnomjerni.

Srbija i Albanija se izdvajaju kao najnaprednije u dijelu regulative digitalne imovine. Srbija je uvela registar pružalaca usluga povezanih s virtuelnim valutama, a Narodna banka Srbije ima nadležnost nad nadzorom i izdavanjem dozvola.

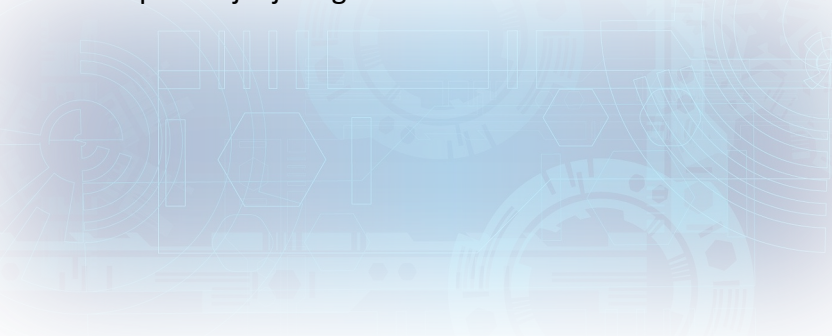
Hrvatska, kao članica EU, primjenjuje MiCA i AML direktive i, u skladu sa obavezama koje iz njih proizilaze, aktivno prati tržište kriptovaluta.

Bosna i Hercegovina i Sjeverna Makedonija još uvijek su u ranim fazama izgradnje regulatornih mehanizama.

Crna Gora, iako je članica Grupe država protiv korupcije (GRECO) i ima zakone o sprječavanju pranja novca, izdvojila se kao glavni evropski centar za korišćenje kriptovaluta na *darkweb*-u (GI-TOC, 2025). Još uvijek nije donijet sistemski zakon koji reguliše virtuelnu imovinu, pa samim tim nije uspostavljena ni adekvatna institucionalnu strukturu za nadzor kripto-sredstava, a odsustvo takvog sistema dovodi do situacije da potencijalno sumnjive transakcije ostaju potpuno nevidljive za nadležne organe. Bez sistemskog prikupljanja podataka, država ne može ni procijeniti obim rizika, niti razviti mehanizme prevencije. Ova situacija predstavlja institucionalni deficit koji ugrožava usklađivanje sa standardima EU i može negativno uticati na međunarodni kredibilitet zemlje.

Do sada, u regionu su realizovane samo tri zaplene digitalne imovine (GI-TOC, 2025), što ukazuje na potrebu za boljom koordinacijom i kooperacijom zemalja regiona. Kriptovalute ne poznaju granice, pa je saradnja među državama ključna. U regionu, međusobna razmjena informacija o sumnjivim transakcijama je minimalna, a ne postoje zajedničke baze podataka ni operativni mehanizmi.

Formiranje regionalne radne grupe pod okriljem Savjeta za regionalnu saradnju (RCC) ili inicijative „Otvoreni Balkan“ moglo bi biti prvi korak ka zajedničkom praćenju digitalnih finansijskih tokova i uspostavljanju regionalnih standarda.



7. Pravci akcije

7.1 Nacionalni nivo

Vlada bi najprije trebalo da usvoji document – nacionalnu strategiju, koji bi obuhvatio politike razvoja, bezbjednosti i regulacije digitalne imovine, definisati dugoročne ciljeve i vremenski okvir za njihovu realizaciju. Takva strategija je polazna osnova za zakonodavnu aktivnost, međutim, kako je već u zakašnjenjum, Crna Gora mora hitno usvojiti i zakon koji bi definisao pojam, pravni status i režim nadzora nad digitalnim sredstvima. Taj zakon treba biti usklađen sa Uredbom MiCA i drugim relevantnim direktivama EU. Zakonom treba jasno odrediti koje institucije su nadležne za nadzor, koje obaveze imaju pružaoci usluga (mjenjačnice, platforme, novčanici) i obaveze vezane za identifikaciju korisnika (KYC) i prijavu sumnjivih transakcija (AML).

Na institucionalnom planu, s obzirom na razuđenost crnogorske državne uprave i fragmentisanost nadležnosti u vezi sa istom odnosno srodnim oblastima, predlaže se uspostavljanje posebnog odjeljenja - centralne kontakt-tačke za virtuelnu imovinu, u okviru Ministarstva finansija ili Centralne banke Crne Gore koje bi bilo zaduženo za praćenje tržišta digitalne imovine i koordinaciju između institucija.

Takođe, registracija mjenjačnica i drugih servisa omogućila bi državi da zna ko posluje na njenoj teritoriji i pod kojim uslovima. Time bi se spriječilo djelovanje neregistrovanih i neregulisanih platformi.

Crna Gora mora uspostaviti sistem evidencije koji će omogućiti praćenje i analizu tokova digitalnih sredstava. Nedostatak takvih evidencija danas je najveći institucionalni propust. Svi nadležni državni organi moraju redovno objavljivati izvještaje o registrovanim slučajevima zloupotreba i sprovedenim istragama. Trenutna praksa — gdje organi navode da ne posjeduju podatke — mora biti zamijenjena sistemom obavezne evidencije i javnog izvještavanja, što će istovremeno pozitivno uticati na podizanje svijesti javnosti o ovom pitanju.

7.2. Regionalna i međunarodna dimenzija

Zapadni Balkan poznat je po interoperabilnosti kriminalnih aktera pojedinaca ili grupa, porijeklom iz različitih zemalja ovog područja. Shodno tome, neophodno je uspostaviti koordinisani sistem akcije u vidu regionalnog centra za analizu kripto-transakcija, u saradnji sa svim državama Zapadnog Balkana, odnosno, kao prvi korak, potpisati memorandume o razumijevanju sa susjednim zemljama radi razmjene informacija o sumnjivim korisnicima i platformama.

Kada se uspostavi zakonodavni i institucionalni okvir, Crnoj Gori, kao kandidatu za EU, stoji na raspolaganju više mehanizama za aktivno učešće u evropskim projektima za borbu protiv pranja novca i digitalnog kriminala (IPA fondovi, Twinning projekti), kojima bi se omogućila razmjena ekspertize, a što je uslov za potpunu funkcionalnost sistema i konkurentnost kriminalnim organizacijama.

Ovi koraci čine osnovu za izgradnju sveobuhvatne politike nadzora nad kriptotržištem i prevencije kriptokriminala. Njihova realizacija zahtijeva političku volju i konsenzus, institucionalnu koordinaciju i širu međunarodnu podršku, ali predstavljaju ključne komponente jačanju finansijske bezbjednosti, ali i nacionalne bezbjednosti uopšte.



8. Zaključak

Kriptovalute predstavljaju jedno od najznačajnijih i najdinamičnijih finansijskih i tehnoloških dostignuća savremenog doba, ali i izvor kompleksnih bezbjednosnih i regulatornih izazova. Njihova decentralizovana priroda, visok stepen anonimnosti i globalni domet stvaraju prostor za zloupotrebe koje mogu ozbiljno ugroziti stabilnost finansijskih sistema, povjerenje građana i bezbjednost država.

U posljednjoj deceniji, kriptovalute su od marginalnog fenomena postale sastavni dio globalne ekonomije. Međutim, dok su tehnološke inovacije napredovale ogromnom brzinom, pravni i institucionalni sistemi ostali su u zaostatku. Njihova međusobna neujednačenost stvorila je pravni vakuum koji kriminalne strukture efikasno koriste za pranje novca, utaju poreza, finansiranje ilegalnih aktivnosti i izbjegavanje međunarodnih sankcija.

Iskustva razvijenih država pokazuju da jedini efikasan pristup podrazumijeva kombinaciju adekvatnog regulatornog okvira, tehničkih kapaciteta i međunarodne saradnje. Evropska unija je Uredbom o tržištima kriptoimovine (MiCA) i novim AML paketom postavila model koji bi trebalo da posluži kao primjer i državama Zapadnog Balkana, pogotovo imajući u vidu njihovu namjeru da postanu njene članice.

Crna Gora se, međutim, suočava sa ozbiljnim institucionalnim nedostacima. Zvanične institucije ne vode evidenciju o upotrebi ni zloupotrebama kriptovaluta, ne postoji zakonski okvir koji bi omogućio praćenje i nadzor digitalne imovine, a saradnja između nadležnih organa je minimalna. Takvo stanje predstavlja visok rizik za finansijski sistem i potencijalno narušava međunarodni kredibilitet države u oblasti borbe protiv pranja novca i finansiranja terorizma.

Neophodno je preći sa reaktivnog na proaktivan pristup – kroz usvajanje Zakona o digitalnoj imovini, uspostavljanje centralne kontakt-tačke za nadzor, obuku službenika i kreiranje baze podataka o sumnjivim transakcijama. Paralelno, Crna Gora treba aktivno da se uključi u međunarodne mreže saradnje i razmjene informacija o kripto-kriminalu, čime bi ojačala svoju institucionalnu otpornost.

Kriptovalute ne moraju nužno biti prijetnja — uz adekvatan pravni okvir i institucionalni nadzor, one mogu postati dio savremene ekonomije i finansijskih inovacija, što bi

pozitivno uticalo na privredni razvoj. Međutim, bez kontrole i odgovornosti, one predstavljaju prostor za rast sivih i crnih tokova kapitala.

Zato je ključno da Crna Gora i region prepoznaju važnost ovog pitanja i uspostave sistem koji balansira između inovacije i bezbjednosti, privatnosti i odgovornosti, slobode tržišta i pravne sigurnosti.



Izvori:

- APML (2022) Nacionalna procjena rizika od pranja novca i finansiranja terorizma. Beograd: Uprava za sprečavanje pranja novca, Ministarstvo finansija Republike Srbije.
- Bank for International Settlements (BIS) (2022) CBDCs, Stablecoins and the Future of Money. Basel: BIS.
- Chainalysis (2023) Crypto Crime Report 2023. Chainalysis Inc. Dostupno na: <https://blog.chainalysis.com>.
- CipherTrace (2021) Cryptocurrency Crime and Anti-Money Laundering Report. Menlo Park, CA: CipherTrace.
- Elliptic (2023) The State of Cross-Chain Crime. London: Elliptic Enterprises Ltd.
- European Commission (2023) Markets in Crypto-Assets Regulation (MiCA) – Regulation (EU) 2023/1114. Brussels: European Union.
- Europol (2023) Cryptocurrency and Criminal Finances: Analysis and Trends 2023. Den Haag: Europol.
- FATF (2023) Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (VASPs). Paris: Financial Action Task Force.
- IMF (2023) Global Financial Stability Report – Digital Assets and Financial Integrity. Washington D.C.: International Monetary Fund.
- MONEYVAL (2022) Anti-money laundering and counter-terrorist financing measures: Montenegro Mutual Evaluation Report. Strasbourg: Council of Europe.
- Merkle Science (2023) Crypto Crime Trends 2023 Report. Singapore: Merkle Science.
- Metropolitan Police (2025) Two people convicted following world's largest crypto seizure. Dostupno na: <https://news.met.police.uk/news/woman-convicted-following-worlds-largest-seizure-501569>.
- TRM Labs (2024) Illicit Crypto Ecosystem Report. San Francisco: TRM Labs.
- UNODC (2023) Illicit Financial Flows and Cryptocurrency: Emerging Threats and Responses. Vienna: United Nations Office on Drugs and Crime.
- World Bank (2022) Crypto-Assets and Anti-Money Laundering: Policy Responses and Risks. Washington D.C.: World Bank.
- Zakon o sprječavanju pranja novca i finansiranja terorizma ("Službeni list Crne Gore", br. 110/23 od 12.12.2023, 065/24 od 05.07.2024, 024/25 od 12.03.2025).