2024

# EVALUARE SECTORIALĂ PENTRU FURNIZORII DE SERVICII DE SCHIMB ÎNTRE MONEDE VIRTUALE ȘI MONEDE FIDUCIARE ȘI FURNIZORII DE PORTOFELE DIGITALE DIN ROMÂNIA


www.onpcsb.ro

# CUPRINS

# Oficiul Național de Prevenire și Combatere a Spălării Banilor

+40 213 155 207

onpcsb@opcsb.ro

Bulevardul Tudor Vladimirescu, nr. 22, clădirea Green Gate, etajul 7, sector 5, București

# Definiții și cuvinte cheie

| | |
|---|---|
| CRIPTOACTIVE | Forme de valori digitale, care utilizează criptografia pentru a securiza tranzacțiile și a controla crearea de unități suplimentare (criptomonede, diverse tipuri de token-uri, NFT-uri, etc.) |
| CRIPTOMONEDĂ | Subcategorie distinctă de criptoactive, tip de monedă digitală, virtuală, nebancară, folosită ca mijloc de plată (ex: Bitcoin, Ethereum, Ripple, Avalanche). Criptomonedele au propriul blockchain și utilizează criptografia pentru a securiza tranzacțiile și a controla generarea de noi unități. |
| FATF (FINANCIAL ACTION TASK FORCE) | Organism internațional care stabilește standarde globale pentru prevenirea spălării banilor și finanțării terorismului |
| FT (FINANȚAREA TERORISMULUI) | Actul de furnizare a fondurilor necesare pentru sprijinirea activităților teroriste sau a organizațiilor teroriste. |
| SB (SPĂLAREA BANILOR) | Procesul prin care fondurile obținute din activități ilegale sunt transformate în active legitime |
| VASP (VIRTUAL ASSETS SERVICE PROVIDER - FURNIZOR DE ACTIVE VIRTUALE) | Furnizori de servicii legate de activele virtuale (cripomonedele) și includ platformele de schimb (exchanges), furnizorii de portofele digitale, intermediari financiari și alte entități care oferă servicii de administrare și transfer de criptoactive. Aceste entități își desfășoară activitatea în conformitate cu reglementările incidente în vigoare. |

I

# Introducere

## 1.1. Scopul evaluării

Evaluarea riscurilor în sectorul furnizorilor de servicii pentru active virtuale (VASP) are drept scop analizarea oportunităților și riscurilor semnificative asociate cu acest domeniu, în special în contextul spălării banilor (SB) și finanțării terorismului (FT). Dezvoltarea rapidă a acestui sector, atât la nivel global, cât și în România, impune o evaluare detaliată a vulnerabilităților specifice pentru a implementa măsuri adecvate de supraveghere și conformitate.

În octombrie 2018, Financial Action Task Force (FATF), dezvoltatorul internațional de standarde pentru combaterea SB/FT, a adoptat un nou standard și a emis îndrumări privind reglementarea și supravegherea activelor virtuale (VA) și a furnizorilor de servicii de active virtuale (VASP). FATF recomandă țărilor să identifice, să evalueze și să înțeleagă riscurile de SB/FT, să dezvolte și să implementeze un regim național bazat pe riscuri. Recomandarea 15 modificată de FATF cere ca acest sector să fie reglementat în scopuri de combatere a SB/FT, respectiv VASP să fie autorizate sau înregistrate și să fie supuse unor sisteme eficiente de monitorizare sau supraveghere [1].

[1] FATF - Updated Guidance for a Risk-Based Approach – Virtual Assets and Virtual Asset Service Providers - October 2021

Deși unele jurisdicții au introdus reglementări, implementarea globală este relativ slabă, iar conformitatea rămâne în urma majorității celorlalte sectoare financiare. Pe baza a 98 de rapoarte de evaluare reciprocă și de urmărire, aproximativ 75% dintre jurisdicții sunt doar parțial sau nu sunt conforme cu cerințele FATF. Sondajul FATF din martie 2023 a relevat că 34% dintre respondenți nu au efectuat o evaluare a riscurilor privind VA și VASP, semnalând lipsa de date fiabile și îndrumări limitate ca principale provocări [2].

În septembrie 2022, Oficiul Național pentru Prevenirea și Combaterea Spălării Banilor, în colaborare cu Banca Națională a României, Autoritatea de Supraveghere Financiară, Ministerul Justiției, Ministerul Afacerilor Interne, Parchetul de pe lângă Înalta Curte de Casație și Justiție și Serviciul Român de Informații, a întocmit primul raport referitor la Evaluarea Națională a Riscurilor de Spălare a Banilor și Finanțare a Terorismului. Acest raport a vizat perioada 2018-2020 și a evidențiat faptul că sectorul economic în care activează furnizorii de servicii de criptoactive prezintă un nivel ridicat de risc, caracterizat prin anonimatul tranzacțiilor, rapiditatea acestora și lipsa limitărilor privind volumul fondurilor transferate.

Conform Evaluării Naționale a Riscurilor, analiza cazurilor a identificat 52 de situații în care criptomonedele au fost folosite pentru a spăla fonduri obținute din activități infracționale. Cele mai frecvente infracțiuni asociate au fost corupția, infracțiunile informatice, înșelăciunea, fraudele de tip phishing și skimming, precum și evaziunea fiscală. Încasările externe s-au dovedit a fi principalul mecanism prin care fondurile provenite din aceste infracțiuni au fost introduse în sistemul bancar, iar transferurile externe și retragerile de numerar au constituit principalele metode de externalizare a banilor spălați.

Pe baza recomandărilor FATF și a concluziilor Evaluării Naționale a Riscurilor, Comitetul de experți pentru evaluarea măsurilor de combatere a spălării banilor și finanțării terorismului (Moneyval) a subliniat, în raportul său de evaluare reciprocă din mai 2023, că autoritățile române au inițiat câteva măsuri importante în direcția reglementării și supravegherii furnizorilor de servicii de active virtuale (VASP). Totuși, nu a fost efectuată încă o evaluare exhaustivă a riscurilor asociate activităților de active virtuale (VA) și de VASP, iar cerințele pentru VASP sunt în prezent limitate la burse și deținătorii de portofele.

Această evaluare sectorială are ca scop analiza detaliată a riscurilor asociate cu activitățile VASP în România, având în vedere legislația națională existentă, reglementările internaționale, constatările din Evaluarea Națională a Riscurilor și constatările din Raportul Moneyval (2023), care a subliniat nevoia de a realiza o evaluare completă a riscurilor.

[2] FATF - Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers – June 2023

Acest raport va conține recomandări și măsuri de atenuare, iar acțiunile specifice vor fi monitorizate și evaluate în funcție de evoluțiile reglementărilor naționale și europene, inclusiv implementarea Regulamentului MiCA și alte norme aplicabile până la finalul anului 2024.

## 1.2. Obiectivele evaluării

Obiectivele evaluării sectoriale a riscurilor asociate activităților furnizorilor de servicii de active virtuale (VASP) sunt esențiale pentru a asigura o înțelegere cuprinzătoare a provocărilor și oportunităților pe care le prezintă acest sector emergent. În acest context, evaluarea își propune să identifice și să evalueze riscurile specifice de spălare a banilor (SB) și finanțare a terorismului (FT), luând în considerare cele mai recente standarde internaționale stabilite de Financial Action Task Force (FATF), evaluarea supranațională a riscurilor (SNRA) realizată de Comisia Europeană în anul 2022, constatările din Evaluarea Națională a Riscurilor (ENR), precum și a Raportului Moneyval (2023).

Un obiectiv central este corelarea riscurilor specifice VASP cu cele evidențiate în Supranational Risk Assessment (SNRA). Această corelare va permite o abordare mai bine fundamentată, având în vedere măsurile de risc și vulnerabilitate identificate atât la nivel național, cât și internațional. Evaluarea va lua în considerare toți factorii relevanți, inclusiv tipurile de servicii și produse oferite, riscurile clienților, precum și factorii geografici care influențează activitatea VASP în România.

Un alt aspect important este ajustarea măsurilor de reglementare. Evaluarea își propune să dezvolte măsuri de reglementare adaptate pe baza riscurilor identificate, asigurând o aliniere eficientă cu cele mai bune practici internaționale. Această ajustare va include formularea de recomandări specifice care să abordeze riscurile, în special în ceea ce privește activitățile care permit relații de afaceri fără prezența fizică a clientului și tranzacțiile anonime sau cu pseudonime.

Un alt obiectiv esențial este de a propune măsuri adecvate de atenuare a riscurilor. Aceasta va include identificarea soluțiilor puternice de identitate digitală pentru a contracara anonimatul tranzacțiilor și asigurarea unui sistem eficient de identificare și verificare a clienților. Evaluarea va lua în considerare și riscurile asociate cu utilizarea crypto-ATM-urilor, care pot oferi infractorilor o poartă de acces pentru a introduce fonduri ilicite în ecosistemul cripto.

În plus, evaluarea va contribui la dezvoltarea unui sistem de monitorizare și evaluare continuă a riscurilor, alături de eficiența măsurilor de reglementare și de combatere

a SB/FT. Această monitorizare va ține cont de evoluțiile sectorului VASP și de implementarea viitoare a Regulamentului MiCA, asigurând astfel un cadru de reglementare dinamic și adaptabil.

În final, evaluarea va promova conștientizarea și educația în rândul furnizorilor de servicii de active virtuale și al utilizatorilor acestora, urmărindu-se creșterea gradului de conștientizare cu privire la riscurile asociate și la măsurile de prevenire a SB/FT, contribuind astfel la un mediu mai sigur și mai transparent. Prin realizarea acestor obiective, evaluarea sectorială își propune să contribuie la construirea unui cadru eficient de reglementare și monitorizare, care să răspundă provocărilor actuale și viitoare ale sectorului VASP în România, aliniindu-se la standardele internaționale și cerințele Uniunii Europene.

## 1.3. Metodologia de evaluare a riscurilor

Metodologia utilizată pentru evaluarea riscurilor în sectorul furnizorilor de servicii de schimb între monede virtuale și monede fiduciare (VASP) din România, a fost elaborată cu respectarea recomandărilor internaționale ale FATF și a metodologiilor adoptate la nivel internațional pentru combaterea spălării banilor și a finanțării terorismului (CSB/CFT). FATF recomandă țărilor să efectueze evaluări ale riscurilor în fiecare sector supus acestor cerințe, având ca scop identificarea, evaluarea și înțelegerea riscurilor asociate, precum și adoptarea de măsuri preventive proporționale.

Procesul de evaluare a riscurilor pentru sectorul VASP a fost structurat pe mai multe etape esențiale, incluzând colectarea și analizarea datelor, identificarea surselor de informații relevante și evaluarea riscurilor asociate spălării banilor și finanțării terorismului. Printre etapele principale ale procesului s-au numărat analiza contextului general al sectorului VASP, ce a avut în vedere numărul de entități active, volumul tranzacțiilor și nivelul de adopție a criptoactivelor la nivel național, precum și identificarea caracteristicilor cheie specifice sectorului VASP, inclusiv riscurile, amenințările, vulnerabilitățile, probabilitatea apariției unor evenimente negative și consecințele acestora.

Cercetarea surselor naționale și internaționale de informare, adaptarea modulelor de colectare a datelor la specificul contextului național, formularea de solicitări către autoritățile implicate și colectarea de informații de la entitățile din sector prin instrumente precum chestionare adresate sectorului VASP, solicitări către autoritățile competente în materie, fișe statistice privind profilul utilizatorilor, precum și analiza cazurilor de utilizare abuzivă a serviciilor VASP, au constituit pași esențiali în realizarea evaluării sectoriale.

Comisia responsabilă pentru evaluarea sectorială a VASP-urilor, numită la nivelul Oficiului Național de Prevenire și Combatere a Spălării Banilor, a gestionat colectarea, analiza și interpretarea datelor din surse naționale și internaționale, asigurându-se că metodologia respectă standardele internaționale. Evaluarea riscurilor asociate sectorului VASP din România a inclus o analiză detaliată a contextului geografic, economic și legal pentru a înțelege dimensiunea, caracteristicile și vulnerabilitățile specifice sectorului.

Evaluarea a acoperit și analiza cazurilor de spălare a banilor independente de alte infracțiuni, sursele de fonduri provenite din activități ilegale naționale și internaționale asociate sectorului VASP, precum și modul în care veniturile din infracțiuni principale intră în sistemul financiar prin intermediul acestui sector. De asemenea, a fost evaluată legătura cu alte sectoare economice cu care VASP-urile interacționează.

Raportul sintetizează evaluarea riscurilor asociate sectorului VASP, evidențiind principalele riscuri de spălare a banilor și finanțare a terorismului, descriind vulnerabilitățile identificate, nivelul general de expunere la riscuri și eficacitatea măsurilor de gestionare aplicate. Această sinteză oferă o imagine clară asupra stării de conformitate și a capacității sectorului de a preveni și combate activitățile de spălare a banilor și finanțare a terorismului, furnizând recomandări pentru îmbunătățirea măsurilor de supraveghere, colaborare și implementare a politicilor CSB/CFT, în conformitate cu standardele internaționale.

## 1.4. Surse de date și informații

Informația joacă un rol esențial în dezvoltarea unei evaluări sectoriale, având un impact direct asupra calității și rezultatelor finale. Un pas important în evaluarea riscurilor asociate sectorului furnizorilor de servicii de active virtuale (VASP) din România, a constat în utilizarea unor instrumente și proceduri eficiente pentru a identifica sursele relevante de informații și a colecta atât date cantitative, cât și calitative. Pentru a obține o imagine clară asupra riscurilor de spălare a banilor (SB) și finanțare a terorismului (FT), au fost valorificate informațiile provenite dintr-o varietate de surse. Printre acestea, informațiile oferite de entitățile din sectorul VASP au fost deosebit de valoroase, deoarece operatorii din acest domeniu dispun de experiență practică în ceea ce privește măsurile de prevenire și combatere a SB/FT. Colaborarea cu aceste entități a permis obținerea unor perspective relevante asupra riscurilor și provocărilor cu care se confruntă sectorul.

Entitățile din sectorul VASP au constituit o sursă principală de informații, având în vedere expertiza și cunoștințele lor în prevenirea și combaterea spălării banilor și a finanțării terorismului. Colectarea datelor de la aceste entități a fost realizată prin chestionare, elaborate cu scopul de a obține informații specifice despre tipologiile de activitate, riscurile percepute și măsurile de conformitate implementate. Aceste chestionare au permis o evaluare detaliată a modului în care VASP-urile își gestionează riscurile și reacționează la amenințările identificate, oferind o bază solidă pentru analiza ulterioară.

Colaborarea cu autoritățile competente în aplicarea legii a fost de asemenea esențială. Acestea au furnizat date statistice relevante, incluzând informații despre cazurile asociate acestui sector. Aceste date, împreună cu observațiile privind tipologiile și tendințele în activitatea de prevenire a SB/FT, au contribuit la obținerea unei imagini clare asupra riscurilor existente și a intervențiilor necesare.

Oficiul Național de Prevenire și Combatere a Spălării Banilor (ONPCSB) a avut un rol central în procesul de evaluare, fiind responsabil de primirea și analiza rapoartelor de tranzacții suspecte. Informațiile furnizate din baza de date ONPCSB au fost cruciale în identificarea amenințărilor și vulnerabilităților din sectorul VASP, precum și în descoperirea tendințelor emergente care ar putea afecta acest domeniu.

Pe lângă aceste surse interne, au fost integrate informații provenite din organizații internaționale și forumuri specializate, cum ar fi FATF, MONEYVAL. Acestea au oferit studii și rapoarte valoroase despre tipologiile de SB/FT, promovând standardele internaționale relevante pentru sectorul VASP. De asemenea, evaluările supranaționale ale riscurilor (SNRA) realizate de Comisia Europeană în 2022 au oferit un cadru de referință important pentru analiza națională.

Raportul privind Evaluarea Națională a Riscurilor de SB/FT, publicat în 2022, a constituit o altă sursă fundamentală de informații, aducând date și concluzii relevante pentru sectorul VASP. În plus, ghidul elaborat de Oficiul Național de Prevenire și Combatere a Spălării Banilor a inclus indicatori de suspiciune și tipologii de spălare a banilor în domeniul criptoactivelor, oferind un instrument util pentru înțelegerea riscurilor specifice.

Rezultatele activităților de supraveghere efectuate de Oficiul Național de Prevenire și Combatere a Spălării Banilor au completat analiza, oferind o viziune clară asupra conformității și posibilelor vulnerabilități din sector. De asemenea, sursele deschise credibile au fost folosite pentru a completa informațiile obținute din sursele mai formale, asigurând astfel o evaluare cât mai bine fundamentată.

Instrumentele de colectare a datelor au avut un impact semnificativ în procesul de evaluare, facilitând identificarea priorităților în gestionarea riscurilor. Acestea au inclus stabilirea unor arii de concentrare pentru evaluare, analiza contextului general al sectorului VASP, precum și identificarea caracteristicilor cheie relevante pentru evaluarea riscurilor de SB/FT. Aceasta a presupus o examinare detaliată a amenințărilor și vulnerabilităților asociate, precum și a probabilității apariției unor evenimente negative.

Colectarea datelor și informațiilor relevante a fost o activitate crucială pentru finalizarea evaluării. Aceasta a inclus cercetarea surselor naționale și internaționale de informare, adaptarea modulelor de colectare a datelor la specificul contextului național, formularea de solicitări către autoritățile implicate și colectarea de informații de la entitățile din sector prin aceste instrumente. În plus, analiza răspunsurilor primite de la autoritățile de aplicare a legii și de alte autorități competente implicate, inclusiv ONPCSB, a asigurat o evaluare riguroasă și bine fundamentată a riscurilor.

În contextul dimensiunii relativ mici a sectorului VASP în România, datele colectate nu s-au limitat la un număr restrâns de cazuri cunoscute. Evaluarea a fost concepută pentru a capta tendințele emergente, vulnerabilitățile și amenințările mai ample, inclusiv cele care nu s-au manifestat încă în mod evident în țară. De asemenea, s-a realizat o comparare a utilizării abuzive a serviciilor VASP din România cu cele din alte jurisdicții, pentru a obține o înțelegere mai profundă a tendințelor globale și a riscurilor transfrontaliere. Această abordare a inclus integrarea informațiilor din surse internaționale de încredere, cum ar fi rapoartele sectoriale ale altor țări și studii specifice privind riscurile asociate sectorului VASP. Aceasta a fost o necesitate, mai ales în contextul în care România nu a dispus de suficiente cazuri interne pentru a construi o bază de analiză solidă.

## 1.5. Structura raportului

### Introducere

Acest capitol are rolul de a contura cadrul general al evaluării riscurilor asociate spălării banilor și finanțării terorismului, în conformitate cu standardele internaționale stabilite de Grupul de Acțiune Financiară (FATF) și cerințele naționale specifice. Se evidențiază scopul fundamental al evaluării, care constă în identificarea și analiza riscurilor inerente sectorului VASP, esențial pentru formularea unor politici eficiente de prevenire. Metodologia de evaluare este detaliată, oferind o descriere a procesului utilizat pentru colectarea și analiza datelor. Sursele de informații incluse sunt variate, cuprinzând entități raportoare, autorități de reglementare, organe de aplicare a legii, Oficiul Național de Prevenire și Combatere a Spălării Banilor, precum și surse deschise și ghiduri relevante.

## Profilul Sectorului VASP

Acest capitol se dedică explorării profilului sectorului VASP, începând cu o definiție clară a acestuia și a rolului său fundamental în economia națională. Se analizează importanța economică a sectorului, evidențiind contribuțiile sale semnificative. Factorii contextuali care influențează evoluția sectorului sunt, de asemenea, examinați, inclusiv tendințele globale și reglementările emergente. Se detaliază cadrul juridic relevant, subliniind reglementările naționale în vigoare, precum și noul cadru juridic armonizat la nivel de UE.

## Evaluarea Riscurilor de SB/FT

Acest capitol se concentrează asupra evaluării riscurilor de SB/FT specifice sectorului VASP. Sunt prezentate diverse tipologii de riscuri asociate, bazându-se pe date statistice și rapoarte elaborate de instituții internaționale. Evaluarea riscurilor pe baza caracteristicilor clienților este realizată prin intermediul chestionarelor și analizelor provenite din rapoarte internaționale. De asemenea, se examinează riscurile asociate produselor și serviciilor oferite de VASP-uri, în baza informațiilor colectate de la entități prin intermediul chestionarelor. Capitolul se încheie cu o analiză amănunțită a amenințărilor externe și interne, evidențiind vulnerabilitățile sectorului în fața diverselor forme de criminalitate financiară.

## Amenințări și Vulnerabilități

Acest capitol investighează în profunzime tipologiile de spălare a banilor care se manifestă în cadrul sectorului VASP, fundamentându-se pe ghiduri și resurse elaborate la nivel național și internațional. Se abordează magnitudinea și natura fenomenului finanțării terorismului, subliniind implicațiile asupra securității naționale și internaționale. Analiza vulnerabilității sectorului VASP este realizată printr-o examinare a legăturilor cu alte sectoare economice, identificând sinergiile și riscurile asociate cu acestea.

## Gestionarea Riscurilor

În acest capitol sunt discutate măsurile de prevenire și atenuare a riscurilor de SB/FT, bazându-se pe reglementările stabilite de legislația națională și europeană. Se analizează în detaliu strategiile de răspuns și managementul riscurilor, evidențiind modalitățile prin care sectorul VASP poate adopta practici de conformitate eficace. Criteriile pentru stabilirea profilului de risc sunt discutate, incluzând dezvoltarea unei matrice de risc care să indice nivelul de risc asociat sectorului VASP din România.

## Concluzii și Recomandări

Capitolul final sintetizează principalele constatări rezultate din evaluare, punând în evidență riscurile semnificative identificate în cadrul sectorului VASP. Se formulează o serie de recomandări concrete pentru autorități și entitățile din sector, menite să sprijine implementarea unor măsuri eficiente de prevenire și combatere a SB/FT. Aceste recomandări sunt fundamentate pe analizele și constatările anterioare, având ca obiectiv consolidarea integrității și securității sectorului financiar în ansamblu.

II

# Profilul sectorului

Evaluarea sectorului VASP din România implică o analiză complexă a contextului geografic, economic și legal pentru a înțelege atât dimensiunea, cât și vulnerabilitățile acestui sector. Poziția strategică a României în Europa de Sud-Est și statutul său de stat membru al Uniunii Europene facilitează fluxuri transfrontaliere semnificative, care, deși oferă oportunități economice, cresc riscul de expunere la spălarea banilor (SB) și finanțarea terorismului (FT).

În ultimii ani, adopția criptoactivelor a crescut considerabil, susținută de un interes public tot mai mare pentru aceste active digitale. Aceasta se reflectă în numărul tot mai mare de cripto-ATM-uri instalate și în creșterea semnificativă a căutărilor online legate de criptomonede.

În acest context, evaluarea sectorului VASP va examina rolul său, importanța economică și cadrul legal aplicabil, cu scopul de a identifica riscurile de SB/FT și măsurile necesare pentru gestionarea acestora la nivel național.

## 2.1. Definiția și rolul sectorului VASP

Sectorul furnizorilor de servicii de schimb între monede virtuale și monede fiduciare include o gamă variată de entități care facilitează schimbul, stocarea și gestionarea criptoactivelor. Aceste entități joacă un rol esențial în ecosistemul criptoactivelor, oferind servicii care permit utilizatorilor să tranzacționeze și să dețină monede virtuale.

### Ce este o monedă virtuală?

*„o reprezentare digitală a valorii care nu este emisă sau garantată de o bancă centrală sau de o autoritate publică, nu este în mod obligatoriu legată de o monedă instituită legal și nu deține statutul legal de monedă sau de bani, dar este acceptată de către persoane fizice sau juridice ca mijloc de schimb și care poate fi transferată, stocată și tranzacționată în mod electronic" [3]*

Această definiție subliniază mai multe aspecte cheie ale monedelor virtuale, care le diferențiază de monedele fiduciare tradiționale. În primul rând, monedele virtuale sunt **reprezentări digitale ale valorii**. Acest lucru înseamnă că ele nu au o formă fizică, cum ar fi bancnotele sau monedele metalice, și există exclusiv în mediul electronic.

Un alt aspect important este că monedele virtuale **nu sunt emise sau garantate de o bancă centrală sau de o autoritate publică**. Spre deosebire de monedele fiduciare, cum ar fi dolarul sau euro, care sunt emise și susținute de guverne și bănci centrale, monedele virtuale nu au un garant guvernamental care să le susțină valoarea. Acest lucru le face mai vulnerabile la fluctuațiile de preț și la incertitudinile pieței. Cu toate acestea, datorită lipsei de legături directe cu o autoritate publică, ele pot funcționa independent de sistemele financiare tradiționale, oferind o alternativă descentralizată.

De asemenea, acestea nu au statut legal de monedă. Acest lucru înseamnă că, spre deosebire de monedele naționale care trebuie acceptate în mod obligatoriu în cadrul tranzacțiilor dintr-un stat (cum ar fi obligativitatea acceptării euro în zona euro), monedele virtuale nu au o astfel de obligație legală.

[3] Directiva (UE) 2018/843 a Parlamentului European și a Consiliului

Cu toate acestea, monedele virtuale sunt **acceptate voluntar** de multe persoane și organizații, atât fizice, cât și juridice, ca mijloc de schimb în tranzacții. Această acceptare voluntară a contribuit la creșterea utilizării monedelor virtuale în tranzacțiile comerciale și financiare internaționale.

Monedele virtuale sunt atractive pentru utilizatori datorită faptului că pot fi **transferate, stocate și tranzacționate în mod electronic**, eliminând nevoia de intermediari tradiționali precum băncile. Acest lucru facilitează **transferurile rapide de valoare** între utilizatori, indiferent de distanța geografică sau de fusul orar, la costuri reduse în comparație cu metodele tradiționale de transfer bancar. Astfel, monedele virtuale au devenit un mijloc preferat pentru tranzacții transfrontaliere și plăți internaționale.

## Ce este un furnizor de portofel digital?

*„o entitate care oferă servicii de păstrare în siguranță a unor chei criptografice private în numele clienților săi, pentru deținerea, stocarea și transferul de monedă virtuală" [4]*

Această definiție subliniază importanța furnizorilor de portofele digitale în ecosistemul criptoactivelor, evidențiind rolul lor central în protejarea accesului utilizatorilor la fondurile virtuale. Cheile criptografice private, care sunt esențiale pentru autorizarea și realizarea tranzacțiilor în siguranță, sunt gestionate de aceste entități. Prin păstrarea în siguranță a acestor chei, furnizorii de portofele digitale nu doar că asigură securitatea utilizatorilor, dar contribuie și la facilitarea unor tranzacții rapide și eficiente

Pe măsură ce utilizarea criptoactivelor se extinde la nivel global, furnizorii de portofele digitale devin piloni esențiali ai securității tranzacțiilor, având responsabilitatea de a preveni accesul neautorizat și atacurile cibernetice. În contextul reglementărilor legale privind combaterea spălării banilor și finanțării terorismului, acești furnizori joacă un rol crucial, implementând măsuri riguroase de securitate și verificare a identității clienților (KYC), contribuind astfel la prevenirea abuzurilor și asigurând conformitatea cu normele legale în vigoare.

[4] Directiva (UE) 2018/843 a Parlamentului European și a Consiliului de modificare a Directivei (UE) 2015/849 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, precum și de modificare a Directivelor 2009/138/CE și 2013/36/UE

## Care este rolul VASP-urilor?

Furnizorii de servicii de schimb între monede virtuale și monede fiduciare (VASP-uri) reprezintă o componentă esențială a ecosistemului criptoactivelor. Aceste entități facilitează conectarea între lumea monedelor virtuale și cea a finanțelor tradiționale, asigurând astfel puntea necesară pentru tranzacții eficiente și sigure între cele două sisteme.

VASP-urile au o importanță crucială într-un sistem financiar digital în plină expansiune, deoarece permit utilizatorilor să acceseze lichidități prin conversia criptoactivelor în monede fiduciare, oferind astfel flexibilitate pentru utilizatori, investitori și companii. În plus, VASP-urile contribuie la securitatea tranzacțiilor și a fondurilor prin gestionarea portofelelor digitale și oferirea de soluții de custodie securizate, protejând criptoactivele utilizatorilor de riscurile cibernetice și fraude. Acestea facilitează o serie de servicii, cum ar fi:

### Schimb între monede virtuale și monede fiduciare

VASP-urile permit utilizatorilor să convertească monedele virtuale în monede fiduciare (precum EUR, USD sau RON) și invers, oferind acces la lichidități și conectând piețele financiare digitale cu cele tradiționale.

### Furnizarea și administrarea portofelelor digitale

VASP-urile oferă servicii de custodie și gestionare a portofelelor digitale, asigurând stocarea securizată a criptoactivelor.

### Tranzacții rapide și transferuri transfrontaliere

VASP-urile facilitează transferuri rapide de fonduri între utilizatori la nivel global, cu costuri mai reduse decât metodele tradiționale de transfer bancar

## De ce sunt importante VASP-urile în economia digitală?

VASP-urile joacă un rol fundamental în susținerea și extinderea economiei digitale, facilitând utilizarea criptoactivelor în tranzacții comerciale, investiții și transferuri financiare. Acestea creează o legătură între piețele tradiționale și economia emergentă bazată pe criptoactive, oferind posibilitatea utilizatorilor de a accesa și utiliza monede virtuale în mod eficient și securizat. Dezvoltarea rapidă a sectorului criptoactivelor a contribuit semnificativ la diversificarea economiei digitale.

De asemenea, creșterea adopției criptomonedelor și a utilizării blockchain-ului a generat un val de investiții noi, atât din partea companiilor tehnologice, cât și a investitorilor privați, care văd un potențial uriaș în această industrie. Sectorul VASP joacă un rol important în acest proces, oferind infrastructura necesară pentru a facilita conversia criptoactivelor în monede fiduciare și invers, astfel încât utilizatorii să poată accesa lichidități și să participe activ pe piețele financiare digitale

## Cum contribuie VASP-urile la combaterea riscurilor de SB/FT?

VASP-urile joacă un rol esențial în combaterea riscurilor de spălare a banilor și finanțare a terorismului prin implementarea reglementărilor stricte de conformitate cu cerințele CSB/CFT. Deși sectorul VASP facilitează transferuri rapide și poate oferi un anumit grad de anonimitate, aceste entități au obligația de a implementa măsuri care să contribuie la prevenirea utilizării criptoactivelor în scopuri ilicite. Pentru a combate riscurile de SB/FT, VASP-urile sunt obligate să adopte și să aplice mecanisme eficiente de cunoaștere a clientelei (KYC), prin care să identifice și să verifice identitatea utilizatorilor. Aceste măsuri sunt esențiale pentru a reduce anonimitatea tranzacțiilor cu criptoactive și pentru a împiedica utilizarea acestora în disimularea provenienței fondurilor obținute din activități infracționale.

De asemenea, VASP-urile trebuie să implementeze **sisteme de monitorizare a tranzacțiilor**, pentru a identifica tranzacțiile suspecte și a le raporta autorităților competente. Aceste rapoarte de tranzacții suspecte (STR) sunt instrumente esențiale în detectarea activităților ilicite, contribuind la supravegherea eficientă a sectorului.

Prin aplicarea acestor măsuri și prin cooperarea cu autoritățile de reglementare și de supraveghere, VASP-urile contribuie activ la prevenirea și combaterea spălării banilor și finanțării terorismului. În acest context, conformitatea cu reglementările CSB/CFT nu doar că reduce riscurile de SB/FT, dar protejează și integritatea pieței financiare digitale și a utilizatorilor săi. Astfel, deși VASP-urile sunt expuse unor riscuri semnificative prin natura activităților lor, adoptarea unor mecanisme eficiente de supraveghere și prevenire contribuie la reducerea vulnerabilităților sectorului și la asigurarea conformității cu cerințele legale.

## 2.2. Importanța economică și factorii contextuali

România, situată în sud-estul Europei, are o poziție strategică care o plasează la intersecția unor importante rute comerciale și financiare. Aceasta facilitează un volum ridicat de tranzacții transfrontaliere, mai ales în relațiile comerciale cu statele membre ale Uniunii Europene și cu cele din regiunea balcanică. Poziția sa geografică îi oferă acces la piețe globale și la fluxuri financiare internaționale, însă expune sectorul VASP la riscuri suplimentare, în special în ceea ce privește spălarea banilor și finanțarea terorismului prin criptoactive.

România a înregistrat o creștere semnificativă a interesului față de criptoactive în ultimii ani. În conformitate cu raportul Crypto-Ready Index din anul 2021 [5], România ocupă locul 33 la nivel global în ceea ce privește pregătirea pentru adopția criptoactivelor, dar se remarcă prin prezența în top 10 țări din lume cu cele mai multe ATM-uri de criptoactive.

[5] https://cryptohead.io/research/crypto-ready-index

Potrivit acestui raport, în anul 2021, în România a fost identificat un număr de 86 de ATM-uri cripto, ceea ce echivalează cu un ATM pentru fiecare 157.379 de locuitori. Acest fapt indică o accesibilitate tot mai mare la infrastructura cripto, facilitând utilizarea criptomonedelor și sporind integrarea acestora în economia digitală. Această creștere a accesibilității sugerează că piața românească este din ce în ce mai deschisă la inovațiile din sectorul criptoactivelor și reflectă un interes sporit al publicului față de aceste tehnologii emergente.

În plus, interesul public față de criptoactive a crescut semnificativ, reflectat de o creștere anuală de 331,3% în căutările online legate de criptomonede, ceea ce sugerează o adopție tot mai largă a acestor tehnologii în rândul populației. De asemenea, cu 7.635 de căutări anuale pe Google per 100.000 de persoane, România este una dintre țările cu cel mai mare interes pentru criptoactive.

Cu toate că România are una dintre cele mai rapide conexiuni la internet din lume în mediul urban, există disparități regionale majore în ceea ce privește accesul la tehnologii digitale. În marile orașe, precum București, Cluj-Napoca și Timișoara, accesul la internet de mare viteză și la servicii digitale este bine dezvoltat. În contrast, în zonele rurale, accesul la internet și la infrastructura digitală este limitat, ceea ce afectează adopția criptoactivelor și accesul populației la această piață. Această discrepanță digitală creează provocări în ceea ce privește uniformitatea accesului la noile tehnologii și servicii digitale, inclusiv criptoactive.

## 2.3. Cadrul legal aplicabil

În România, cadrul juridic principal în contextul prevenirii și combaterii spălării banilor și finanțării terorismului (SB/FT) este reglementat prin Legea nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului, precum și pentru modificarea și completarea unor acte normative.

Legea nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului a fost publicată în Monitorul Oficial al României, Partea I, la data de 18 iulie 2019, prevederile sale au transpus Directiva (UE) 2015/849 a Parlamentului European și a Consiliului privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, de modificare a Regulamentului (UE) nr. 648/2012 al Parlamentului European și al Consiliului și de abrogare a Directivei 2005/60/CE a Parlamentului European și a Consiliului și a Directivei 2006/70/CE a Comisiei, publicată în Jurnalul Oficial al Uniunii Europene la data de 05 iunie 2015.

Potrivit legislației naționale, respectiv în conformitate cu prevederile art. 5 alin. (1), lit. $g^1$ și $g^2$ din Legea nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului, precum și pentru modificarea și completarea unor acte normative, furnizorii de servicii de schimb între monede virtuale și monede fiduciare, precum și furnizorii de portofele digitale sunt considerați entități raportoare, supravegheate de Oficiul Național de Prevenire și Combatere a Spălării Banilor, respectiv acestora le revin toate obligațiile incidente în contextul prevenirii și combaterii spălării banilor și finanțării terorismului (SB/FT).

Ulterior adoptării acestui act normativ, în vederea asigurării unei supravegheri și monitorizări eficiente a categoriilor de entități raportoare, s-a impus necesitatea identificării celor care desfășoară efectiv activitățile care intră sub incidența Legii nr. 129/2019 pentru prevenirea şi combaterea spălării banilor şi finanțării terorismului.

În acest sens, a fost adoptată Ordonanța de urgență a Guvernului nr. 53/2022 privind modificarea şi completarea Legii nr. 129/2019 pentru prevenirea şi combaterea spălării banilor şi finanțării terorismului, precum și pentru modificarea și completarea unor acte normative. Astfel, au fost stabilite în sarcina entităților raportoare prevăzute la art. 5 alin. (1) lit. g) - k) din Legea nr. 129/2019, implicit furnizorilor de servicii de schimb între monede virtuale și monede fiduciare, precum și furnizorilor de portofele digitale, a obligației de a notifica Oficiul, exclusiv electronic, cu privire la începerea/suspendarea/încetarea activității care intră sub incidența acestei legi.

România, în calitate de stat membru al Organizației Națiunilor Unite și al Uniunii Europene și-a asumat angajamente internaționale, context în care subliniem faptul că actele cu forță juridică obligatorie ale acestor organizații stabilesc în sarcina statelor membre obligația de a adopta anumite măsuri legislative pentru punerea în aplicare a sancțiunilor internaționale instituite de Consiliul de Securitate al Organizației Națiunilor Unite, în baza art. 41 din Carta Națiunilor Unite, și de Uniunea Europeană în cadrul Politicii externe și de securitate comune. În acest sens, cadrul național de implementare a sancțiunilor internaționale este reglementat prin Ordonanța de Urgență a Guvernului nr. 202/2008 și Hotărârea Guvernului nr. 603/2011, prevederi legale ce impun obligații suplimentare entităților reglementate în ceea ce privește aplicarea sancțiunilor internaționale stabilite de ONU și Uniunea Europeană.

Astfel, furnizorii de servicii de schimb între monede virtuale și monede fiduciare, precum și furnizorii de portofele digitale sunt obligați să identifice tranzacțiile care implică persoane sau entități desemnate ori bunuri aflate sub sancțiuni, conform Ordonanța de Urgență a Guvernului nr. 202/2008.

În prezent, în România, accesul pe piață a furnizorilor de servicii de schimb între monede virtuale și monede fiduciare, precum și furnizorilor de portofele digitale (VASP) nu este condiționată de obținerea unei licențe sau autorizări, entitățile fiind constituite în conformitate cu prevederile Legii nr. 31/1990 privind societățile comerciale. Totuși, a fost inițiat un proiect legislativ în curs de elaborare, care necesită adaptarea la noul cadru juridic emergent.

La nivel european, în contextul reglementării criptoactivelor și al furnizorilor de servicii aferente, a fost creat pentru prima dată un cadru juridic armonizat prin adoptarea unor acte legislative esențiale, astfel:

| | |
|---|---|
| **Regulamentul privind piețele criptoactivelor (MiCA):** | REGULAMENTUL (UE) 2023/1114 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 31 mai 2023 privind piețele criptoactivelor și de modificare a Regulamentelor (UE) nr. 1093/2010 și (UE) nr. 1095/2010 și a Directivelor 2013/36/UE și (UE) 2019/1937 |
| **Regulamentul TFR:** | REGULAMENTUL (UE) 2023/1113 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 31 mai 2023 privind informațiile care însoțesc transferurile de fonduri și anumite criptoactive și de modificare a Directivei (UE) 2015/849 (reformare) |

Noul cadru juridic comun completează cadrul normativ prin specificarea cerințelor suplimentare aplicabile VASP-urilor. Aceste regulamente impun obligații privind transparența tranzacțiilor, păstrarea registrelor și identificarea clienților în cazul tranzacțiilor cu active virtuale, armonizând astfel standardele de conformitate la nivelul Uniunii Europene. Regulamentul TFR, aplicabil începând cu data de 30 decembrie 2024, introduce o schimbare semnificativă prin clasificarea furnizorilor de servicii de criptoactive (VASP-uri) drept instituții financiare, supuse astfel unui set de obligații similare celor aplicabile instituțiilor financiare tradiționale. În sensul Regulamentului MiCA, VASP-urile vor fi obligate să obțină o licență sau o autorizație pentru a putea continua să opereze pe piața europeană.

Acest regulament vizează protecția investitorilor prin sporirea transparenței și stabilirea unui cadru de reglementare cuprinzător pentru emitenți și furnizorii de servicii de criptoactive, inclusiv în ceea ce privește respectarea normelor SB/FT.

Acest pachet elimină o lacună din legislația existentă a UE, garantând faptul că actualul cadru juridic nu creează obstacole în calea utilizării noilor instrumente financiare digitale și, în același timp urmărește să sprijine inovarea și adoptarea de noi tehnologii financiare, oferind, în același timp, un nivel adecvat de protecție a consumatorilor și a investitorilor.

- **conform noilor reglementări, fiecare VASP va trebui să dețină o licență sau o autorizație obținută în urma unei proceduri taxabile.**

- **potrivit noilor reglementări, entitățile care furnizează servicii de criptoactive în conformitate cu legislația națională aplicabilă înainte de 30 decembrie 2024 pot continua să facă acest lucru până la 1 iulie 2026 sau până când obțin sau li se refuză o autorizație MiCA.**

În prezent, la nivel național au fost demarate măsuri legislative care vizează adaptarea legislației naționale la cerințele cadrului de reglementare armonizat la nivelul Uniunii Europene, aceste măsuri fiind esențiale pentru a asigura o tranziție lină către noul cadru juridic, protejând astfel investitorii și stabilitatea financiară.

Adoptarea noului cadru juridic, care adaptează legislația națională la reglementările europene MiCA și TFR, marchează o etapă importantă în reglementarea sectorului criptoactivelor. Aceste măsuri contribuie la asigurarea conformității cu standardele SB/FT, protejând astfel atât investitorii, cât și stabilitatea financiară, și oferind un cadru adecvat pentru inovare și dezvoltare în sectorul VASP din România.

III

# Evaluarea riscurilor de SB/FT

## 3.1. Supravegherea sectorului VASP la nivel național

Autoritatea competentă pentru supravegherea sectorului privind furnizorii de servicii de schimb între monede virtuale și monede fiduciare, precum și furnizorii de portofele digitale, este Oficiul Național de Prevenire și Combatere a Spălării Banilor – UIF România. Această instituție își desfășoară activitatea printr-o abordare sistematică, centrată pe evaluarea riscurilor, având ca obiectiv principal protejarea integrității sistemului financiar. Prin implementarea normelor legale naționale în materia prevenirii spălării banilor și a finanțării terorismului, se urmărește asigurarea unui mediu operațional sigur și transparent pentru toate entitățile implicate.

Supravegherea se realizează atât prin metode *off-site*, cât și prin acțiuni de control *on-site*. În cadrul activităților *off-site*, supravegherea se realizează prin analizeazarea datelor și informațiilor relevante cu privire la entitățile raportoare, utilizând un instrument analitic prestabilit. Această analiză permite evaluarea expunerii fiecărei entități la riscurile de spălare a banilor și de finanțare a terorismului, ceea ce contribuie la o mai bună înțelegere a contextului operațional al acestora.

Ca urmare a evaluării, în cadrul procesului analitic, a gradului de expunere la riscul de spălare a banilor si finanțare a terorismului, pe baza datelor și informațiilor existente la nivelul ONPCSB, sunt obținute rezultate în baza cărora sunt inițiate acțiuni de verificare

și control (on-site), care implică verificări directe la sediul entităților raportoare, prin care se monitorizează modul în care entitățile din acest sector respectă reglementările legale și aplică măsurile necesare pentru prevenirea activităților ilegale. Totodată, de menționat este și faptul că prin componenta supravegherii on-site se urmărește și creșterea nivelului de conștientizare și conformare a entităților raportoare cu obligațiile legale din domeniul prevenirii și combaterii spălării banilor și a finanțării terorismului.

Responsabilitatea Oficiului de a supraveghea entitățile raportoare, implicit furnizorii de servicii de schimb între monede virtuale și monede fiduciare, precum și furnizorii de portofele digitale este fundamentată pe cadrul juridic național, care îi conferă atribuții specifice. Supravegherea se realizează printr-un sistem operațional dedicat, care evaluează în mod constant riscurile asociate activităților entităților monitorizate. Acest proces analitic permite stabilirea frecvenței și intensității activităților de supraveghere, în funcție de rezultatele obținute în cadrul evaluărilor de risc.

Activitatea de supraveghere se realizează printr-un sistem operațional specific abordării pe bază de risc, ce implică procese analitice de evaluare a unor indicatori de risc, stabilind astfel nivelul de expunere la riscurile de SB/FT ale entităților raportoare. Frecvența și intensitatea activității de supraveghere sunt determinate pe baza evaluărilor Raportului de Evaluare Națională a Riscurilor de Spălare a Banilor și Finanțare a Terorismului (2022). Având în vedere dimensiunea redusă a sectorului VASP în România, unde conform evaluării naționale a riscurilor (ENR) [6] din 2022 s-a evidențiat că există între 5 și 6 entități active, este esențial să ne concentrăm asupra metodelor de supraveghere și control utilizate de Oficiului Național de Prevenire și Combatere a Spălării Banilor. În anul 2022, au fost efectuate supravegheri off-site pentru un număr de 11 entități raportoare din categoria VASP, iar în baza rezultatelor obținute au fost realizate controale on-site la 2 entități. Aceste controale au avut ca scop evaluarea conformității cu normele legale și identificarea eventualelor deficiențe în gestionarea riscurilor de spălare a banilor și finanțare a terorismului [7]. De asemenea, în cadrul acțiunilor de control on-site efectuate de ONPCSB, a fost evaluat statutul de "fit and proper" (potrivit și competent) al persoanelor din conducerea de nivel superior a societății, persoane care trebuie să dețină cunoștințele, experiența și expertiza necesare pentru a gestiona riscurile de spălare a banilor și finanțare a terorismului.Totodată, rezultatele controalelor efectuate nu au relevat deficiențe semnificative, ceea ce sugerează un grad de conformitate rezonabil în rândul entităților supravegheate. Cu toate acestea, este important de menționat că nu au fost impuse acțiuni, ci s-a stabilit un plan de măsuri pentru remedierea deficiențelor identificate. Aceste constatări sunt relevante pentru evaluarea riscurilor, dar trebuie interpretate cu prudență, având în vedere dimensiunea mică a sectorului și numărul limitat de controale.

[6] Raport privind Evaluarea Națională a Riscurilor de Spălare a Banilor și Finanțare a Terorismului - 2022
[7] Raport de activitate a Oficiul Național de Prevenire și Combatere a Spălării Banilor- 2022

Pe lângă acest context, este crucial să subliniem că Legea nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului a fost modificată în anul 2020, reglementând și furnizorii de servicii de schimb între monede virtuale și monede fiduciare, precum și furnizorii de portofele digitale în categoria entităților raportoare. Acest aspect adaugă un strat suplimentar de complexitate la supravegherea sectorului, având în vedere că aceste reglementări sunt relativ noi.

Evaluarea sectorială a riscurior în materie de SB/FT pentru domeniul VASP s-a realizat pe baza informațiilor colectate de la un număr de 10 entități care au transmis informațiile solicitate în timp util pentru finalizarea evaluării.

Având în vedere dimensiunea redusă a sectorului, se ridică întrebarea în ce măsură rezultatele obținute oferă o imagine completă asupra riscurilor de spălare a banilor și finanțare a terorismului în sectorul VASP. Deși supravegherea efectuată de ONPCSB este esențială pentru identificarea și gestionarea riscurilor, dimensiunea mică a sectorului și numărul limitat de controale pot duce la o evaluare parțială a acestora. Controalele on-site, realizate doar la entitățile considerate cu risc ridicat, reflectă doar o fracțiune din activitățile din sector, lăsând loc pentru potențiale riscuri nedeclarate sau neidentificate în cadrul entităților cu risc mai scăzut sau nesupravegheate direct.

Chiar și în acest context, informațiile obținute din supravegherea ONPCSB reprezintă un punct de referință important pentru evaluarea riscurilor reziduale și inerente. Chiar dacă nu s-au identificat deficiențe majore, este posibil ca, în cazul unui număr mai mare de controale sau în contextul extinderii sectorului, riscurile să evolueze sau să devină mai evidente. Supravegherea trebuie să continue și să se adapteze pe măsură ce sectorul crește și devine mai complex, având în vedere că, din perspectiva evaluării riscurilor, o dimensiune mică nu înseamnă automat riscuri scăzute.

**Concluzie**

**Informațiile obținute din supravegherea realizată de Oficiul Național de Prevenire și Combatere a Spălării Banilor oferă o bază valoroasă pentru evaluarea riscurilor de spălare a banilor și finanțare a terorismului în sectorul VASP. Totuși, aceste informații sunt limitate de dimensiunea redusă a sectorului și implicit de numărul mic de controale efectuate. Este esențial ca evaluarea riscurilor să fie un proces continuu și dinamic, care să țină cont de evoluția sectorului și de posibilele amenințări emergente, pentru a asigura un sistem eficient de prevenire și combatere a spălării banilor și finanțării terorismului.**

## 3.2. Dimensiunea sectorului VASP în România

În prezent, accesul pe piața din România al furnizorilor de servicii de schimb între monede virtuale și monede fiduciare, precum și al furnizorilor de portofele digitale, nu este condiționat de un cadru specific de autorizare sau de licențiere. În lipsa unei reglementări specifice de autorizare pentru accesul pe piață, obligația de notificare impusă prin Ordonanța de urgență nr. 53/2022 servește ca o măsură de atenuare parțială. Aceasta impune ca fiecare VASP să informeze Oficiul Național de Prevenire și Combatere a Spălării Banilor cu privire la începerea, suspendarea sau încetarea activităților. Deși această cerință permite o monitorizare a sectorului, eficiența sa este limitată.

Între 2021 și 2024, ONPCSB a primit 36 de notificări cu privire la desfășurarea activității în acest sector. În urma colectării datelor prin chestionare, s-a confirmat că doar 12 dintre cele 31 de entități care au răspuns desfășoară activități specifice VASP. Evaluarea sectorială a riscurilor s-a bazat în principal pe informațiile primite de la 10 dintre acestea, care au furnizat datele necesare în timp util. Cu toate acestea, este posibil ca pe piață să existe și alte entități care operează în acest sector, dar care nu au fost confirmate în cadrul acestei evaluări.

Dimensiunea redusă a sectorului VASP în România, marcată de o bază de entități limitată, face ca modificările din piață să fie semnificative și să poată influența rapid datele generale. Chiar și înregistrarea unei singure entități noi poate schimba structura sectorului, având impact asupra evaluărilor și măsurilor de gestionare a riscurilor. Din acest motiv, este important ca analiza să aibă în vedere nu doar situația actuală a sectorului, ci și tendințele globale și potențialul de creștere a pieței, sectorul criptoactivelor având o dinamică puternic influențată de inovațiile tehnologice și de reglementările emergente la nivel internațional.

| | **2021 (RON)** | **2022 (RON)** | **2023 (RON)** |
|---|---|---|---|
| **VASP 1** | ≈ 8.5 mil. | ≈ 12 mil. | ≈ 4.5 mil. |
| **VASP 2** | ≈ 6.5 mil. | ≈ 3 mil. | ≈ 2 mil. |
| **VASP 3** | ≈ 1.1 mil. | ≈ 1.5 mil. | ≈ 1.7 mil. |

*Top 3 VASP-uri din România potrivit cifrei de afaceri. Sursa: Ministerul Finanțelor*

Potrivit situațiilor financiare pentru anii 2021, 2022 și 2023, fluctuațiile în cifrele de afaceri ale principalelor VASP-uri din România, în perioada 2021-2023 indică o piață instabilă, sensibilă la factori economici și de reglementare. În prezent, cifrele de afaceri ale principalelor VASP-uri din România includ și veniturile obținute din activități desfășurate sub coduri CAEN care nu sunt specifice sectorului VASP. Această combinare a veniturilor provenite din diverse activități reduce claritatea asupra performanțelor strict legate de sectorul VASP, complicând astfel procesul de supraveghere și evaluare a riscurilor specifice acestuia. Pentru a asigura o monitorizare adecvată și o evaluare precisă a riscurilor asociate, este necesar ca VASP-urile să desfășoare exclusiv activități încadrate sub un cod CAEN specific, fără implicarea în alte activități economice.

Astfel, deși sectorul VASP din România este relativ mic, numărând doar 12 entități confirmate, potențialul său de creștere și evoluțiile internaționale impun o monitorizare atentă și o analiză continuă. Având în vedere ritmul rapid de dezvoltare a tehnologiei blockchain și a pieței criptoactivelor la nivel global, acest sector prezintă un risc crescut de expunere la amenințările de spălare a banilor și finanțare a terorismului. Odată cu adoptarea de reglementări tot mai stricte pe plan internațional, cum ar fi implementarea cadrului juridic armonizat la nivelul Uniunii Europene, este esențial ca analiza riscurilor să fie realizată dinamic, adaptându-se constant la noile tendințe și vulnerabilități.

Pentru a se alinia acestor cerințe internaționale și pentru a preveni riscurile transfrontaliere asociate cu activitățile VASP, este necesară implementarea unui cadru de reglementare flexibil și adaptabil, care să includă măsuri de evaluare a riscurilor, precum și mecanisme eficiente de raportare și control. În plus, având în vedere creșterea potențială a acestui sector, monitorizarea activităților VASP trebuie să fie susținută de o cooperare sporită între autoritățile naționale și internaționale, pentru a identifica și a contracara în mod proactiv eventualele vulnerabilități.

**Concluzie**

**Deși dimensiunea sectorului VASP în România este deocamdată redusă, dinamica sa promite o extindere viitoare semnificativă. Acest potențial de creștere, corelat cu tendințele internaționale, subliniază importanța unui cadru robust de analiză și gestionare a riscurilor, pentru a asigura conformitatea cu cerințele naționale și internaționale în materie de prevenire și combatere a spălării banilor și finanțării terorismului.**

### 3.3. Riscurile identificate în contextul global

În cadrul evaluării riscurilor asociate sectorului furnizorilor de servicii de active virtuale, diverse evaluări sectoriale și rapoarte internaționale au evidențiat riscuri fundamentale legate de anonimatul utilizatorilor, reglementările incomplete sau ineficiente și utilizarea noilor tehnologii financiare descentralizate.

Un risc general major în acest sector este anonimatul clienților, care afectează capacitatea autorităților de a detecta și preveni activitățile de spălare a banilor și finanțarea terorismului. Raportul FATF din anul 2023 subliniază că, deși anumite jurisdicții au făcut progrese în implementarea reglementărilor stricte KYC, multe VASP-uri permit în continuare tranzacții cu anonimat parțial sau complet, ceea ce facilitează activitățile ilicite. Platformele care nu implementează măsuri robuste de conformitate se confruntă cu riscul de a deveni vehicule pentru spălarea fondurilor provenite din activități criminale [8].

Conform evaluărilor FATF, există o întârziere semnificativă în implementarea efectivă a reglementărilor din materia combaterii spălării banilor și finanțării terorismului pentru VASP-uri la nivel global. Aproximativ 75% din jurisdicții nu au implementat sau au implementat parțial standardele FATF privind VASP-urile, ceea ce expune acest sector la vulnerabilități semnificative legate de spălarea banilor și finanțarea terorismului. În multe cazuri, lipsește o evaluare națională a riscurilor (ENR) care să identifice în mod corespunzător riscurile asociate acestui sector [9].

Tranzacțiile peer-to-peer (P2P) reprezintă un alt risc semnificativ, conform raportului Chainalysis din 2024. Lipsa unui intermediar centralizat în aceste tranzacții face ca fondurile să fie mai dificil de urmărit, ceea ce deschide oportunități pentru infractorii cibernetici să ascundă originea fondurilor ilicite. Chainalysis arată că aceste tranzacții au devenit un canal favorizat de grupările criminale, în special de entități asociate cu țări aflate sub sancțiuni internaționale, cum ar fi Coreea de Nord [10].

În plus, tehnologiile descentralizate precum platformele descentralizate (DeFi) sunt considerate o provocare pentru supravegherea eficientă a fluxurilor financiare. FATF subliniază că lipsa unui punct centralizat de control și dificultatea urmăririi fondurilor în aceste ecosisteme descentralizate cresc riscul de utilizare a VASP-urilor pentru spălarea banilor și alte activități ilicite [11].

[8] FATF (June, 2023) - Targeted Update On Implementation Of The FATF Standards On Virtual Assets And Virtual Asset Service Providers
[9] FATF(2024)-Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs
[10] Chainalysis Crypto Crime Report 2024
[11] FATF (June 2023)-Targeted Update On Implementation Of The Fatf Standards On Virtual Assets And Virtual Asset Service Providers

Totodată, și din raportul Moneyval (2023) cu privire la riscurile de spălare a banilor și finanțare a terorismului asociate sectorului VASP reiese necesitatea unor îmbunătățiri majore în ceea ce privește conformitatea statelor membre cu standardele FATF în domeniul activelor virtuale și al furnizorilor de servicii aferente. Raportul constată că, deși unele progrese au fost înregistrate, majoritatea statelor membre se confruntă în continuare cu deficiențe semnificative în implementarea măsurilor preventive și în supravegherea eficientă a sectorului VASP. Printre provocările majore se numără evaluarea riscurilor, detectarea platformelor neînregistrate, îmbunătățirea calității raportărilor de tranzacții suspecte și gestionarea riscurilor asociate anonimității și tehnologiilor descentralizate. De asemenea, raportul subliniază importanța intensificării cooperării internaționale pentru a combate infracțiunile transfrontaliere legate de activele virtuale și a crește eficiența măsurilor de combatere a spălării banilor și finanțării terorismului [12].

Evaluările naționale recente cu privire la acest sector, realizate de alte state membre ale Uniunii Europene, au evidențiat riscuri semnificative în utilizarea VASP-urilor pentru activități de spălare a banilor prin conversia rapidă a criptomonedelor în active fiat, precum și riscurile asociate cu serviciile de off-ramping. Conform Chainalysis, peste 71,7% din fondurile ilicite au fost convertite în monede fiduciare prin intermediul unui număr redus de platforme de off-ramping, ceea ce indică vulnerabilități ridicate în cadrul acestor entități [10].

De asemenea, rapoartele privind evaluările sectoriale efectuate de diverse jurisdicții, au subliniat necesitatea unei cooperări internaționale sporite pentru a combate riscurile asociate acestui sector, dat fiind că tranzacțiile VASP au o natură transfrontalieră, iar supravegherea eficientă a acestora necesită mecanisme comune și instrumente de cooperare la nivel global.

**Concluzie**

**Riscurile asociate sectorului VASP în contextul global includ anonimatul tranzacțiilor, vulnerabilitățile geografice, utilizarea noilor tehnologii financiare descentralizate și concentrarea activităților ilicite în jurul anumitor platforme specifice. Implementarea completă a recomandărilor FATF și adoptarea unor măsuri stricte de reglementare și conformitate, rămân esențiale pentru atenuarea acestor riscuri.**

[12] Moneyval (2023)-Money Laundering And Terrorist Financing Risks In The World Of Virtual Assets

### 3.4. Riscurile identificate la nivel național

Identificarea și analiza riscurilor din sectorul VASP din România joacă un rol central în cadrul evaluării naționale. Această analiză se bazează pe răspunsurile furnizate de VASP-uri prin intermediul chestionarelor, axându-se pe patru categorii esențiale de riscuri, după cum urmează:

#### RISCUL PRIVIND CLIENȚII

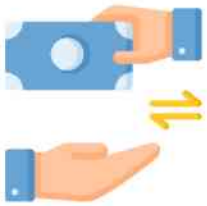
Vizează identificarea și evaluarea tipologiilor de clienți, jurisdicțiile de proveniență și structurile juridice complexe care pot prezenta un risc ridicat de spălare a banilor și finanțare a terorismului.

#### RISCUL PRIVIND PRODUSELE ȘI SERVICIILE

Se referă la riscurile asociate tipurilor de servicii oferite de VASP-uri, cum ar fi schimbul de criptoactive, portofelele digitale și alte produse care pot facilita tranzacții anonime sau greu de urmărit.

#### RISCUL DE CONFORMITATE

Include măsurile și procedurile implementate de VASP-uri pentru a se conforma reglementărilor naționale și internaționale privind prevenirea spălării banilor și finanțării terorismului.



#### RISCUL PRIVIND TRANZACȚIILE

Această categorie analizează riscurile asociate tranzacțiilor financiare efectuate prin intermediul criptoactivelor, în special cele transfrontaliere, care pot facilita transferuri anonime sau suspecte.

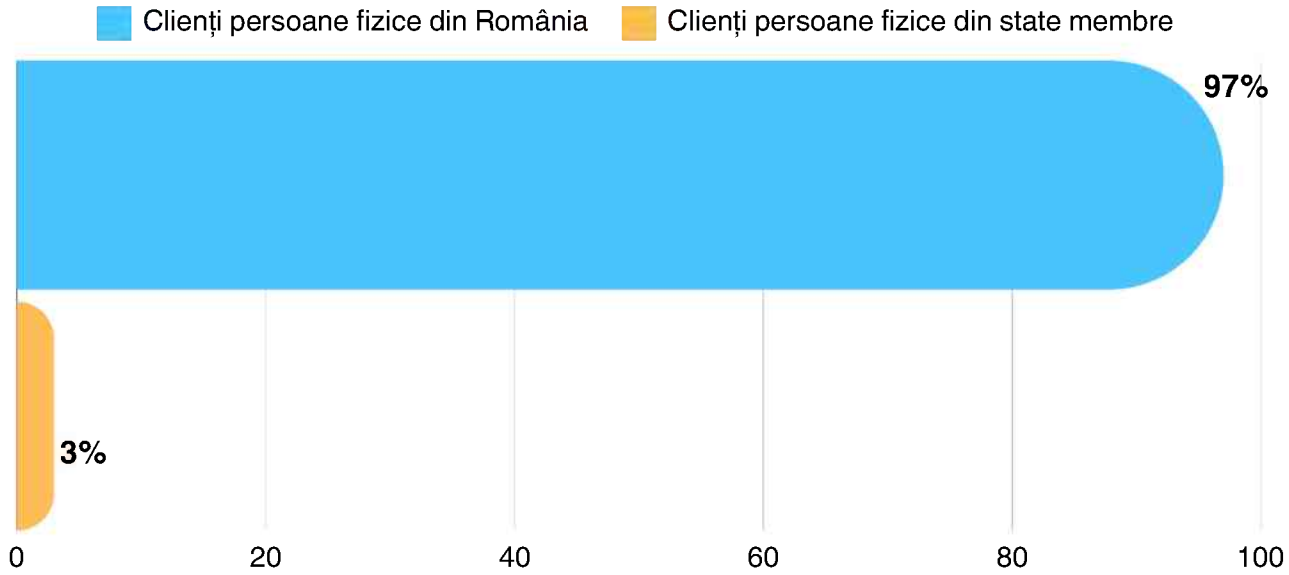
Aceste domenii de risc sunt considerate critice pentru identificarea vulnerabilităților sectorului, având în vedere că acestea afectează aspecte fundamentale ale activităților VASP-urilor, de la tipologia și profilul clienților, până la respectarea reglementărilor legale și monitorizarea tranzacțiilor. În continuare, vom explora fiecare dintre aceste riscuri în detaliu, pe baza datelor colectate prin chestionare, oferind o imagine cuprinzătoare asupra expunerii sectorului la potențialele amenințări în ceea ce privește spălarea banilor și finanțarea terorismului.

## Riscul privind clienții

Analiza riscurilor asociate clienților în sectorul VASP din România a evidențiat o serie de factori de risc specifici, care sunt esențiali pentru înțelegerea vulnerabilităților sectorului în ceea ce privește spălarea banilor și finanțarea terorismului. Răspunsurile din chestionar furnizate de VASP-uri au oferit date semnificative despre tipologia clienților, jurisdicțiile de proveniență și activitățile economice ale acestora. În cele ce urmează, sunt prezentate datele și riscurile relevante.

Toate VASP-urile care au completat chestionarul au indicat că desfășoară activități preponderent în România. Totuși, pentru entitățile care desfășoară tranzacții transfrontaliere cu clienți din alte jurisdicții, acest aspect necesită o monitorizare atentă, având în vedere că anumite jurisdicții pot fi mai vulnerabile la activități ilicite din cauza lipsei de reglementări stricte sau a standardelor mai scăzute de supraveghere financiară.

Proporția clienților din România este semnificativă, reprezentând majoritatea pentru toate entitățile (peste 97% pentru majoritatea VASP-urilor), potrivit figurii de mai jos. Totuși, există clienți și din Uniunea Europeană (UE), cu o pondere mai mică (de exemplu, între 2% și 3%), iar în unele cazuri, există o mică proporție de clienți din jurisdicții non-UE, în special țări din regiunea balcanică și Republica Moldova. Aceasta indică un risc moderat datorat tranzacțiilor internaționale, mai ales în contextul implicării unor jurisdicții cu potențial risc crescut.




*Proporția clienților persoane fizice ai VASP-urilor din România*

Răspunsurile VASP-urilor indică faptul că majoritatea clienților sunt persoane fizice, aceștia reprezentând peste 90% din totalul clienților. Acest fapt indică un risc ridicat de tranzacții de valoare mică și frecventă, care sunt utilizate adesea pentru a fragmenta transferurile și a evita raportarea, mai ales în contextul unei monitorizări insuficiente. Persoanele fizice prezintă un risc ridicat în evaluarea sursei fondurilor și în monitorizarea comportamentului tranzacțional.

Clienții persoane juridice reprezintă între 0% și 10% din portofoliul clienților, iar unele VASP-uri au indicat că aceștia provin din sectoare economice considerate de risc ridicat. Un risc suplimentar vine din partea structurilor juridice complexe, utilizate de unele entități juridice pentru a ascunde adevărații beneficiari ai tranzacțiilor.

Un risc semnificativ identificat în chestionare este reprezentat de clienții proveniți din jurisdicții cu risc ridicat, care au fost menționați de câteva VASP-uri. În general, ponderea acestor clienți este scăzută (sub 1% pentru majoritatea entităților), însă aceștia sunt foarte vulnerabili la utilizarea criptoactivelor în scopuri de spălare a banilor sau finanțare a terorismului. Exemplele de jurisdicții cu risc ridicat menționate includ țări non-UE din regiuni geopolitic instabile, precum Iran, Afghanistan, Coreea de Nord, Siria, Yemen, Burkina Fasso, etc.

Un alt risc notabil îl reprezintă clienții Persoane Expuse Public (PEP). Deși ponderea PEP în rândul clienților VASP este relativ scăzută (sub 1%), aceștia prezintă un risc ridicat de SB/FT din cauza potențialelor legături cu acte de corupție. VASP-urile au implementat măsuri suplimentare pentru verificarea și monitorizarea acestor clienți, conform legislației, însă numărul redus de clienți PEP nu elimină riscul asociat.

O altă categorie de clienți de risc ridicat este reprezentată de entitățile juridice care activează în sectoare economice vulnerabile, conform Evaluării Naționale a Riscurilor de SB/FT. Chestionarele arată că acești clienți au o prezență minoră în rândul clienților VASP (în general sub 2%), dar activitățile acestor sectoare, cum ar fi jocurile de noroc sau agențiile imobiliare, cresc riscul de utilizare a criptoactivelor pentru activități ilicite.

Un risc suplimentar este dat de utilizarea structurilor juridice complexe, care a fost identificată la un procent mic de clienți ai VASP-urilor (în general sub 0.5%). Aceste structuri sunt utilizate adesea pentru a ascunde beneficiarii reali ai tranzacțiilor și pot fi un semnal de alarmă în ceea ce privește activitățile de spălare a banilor. În cazurile în care VASP-urile au identificat companii paravan, acestea au aplicat măsuri suplimentare de due diligence și au investigat în profunzime structura de proprietate a entităților respective, reducând astfel riscurile asociate activităților financiare ilicite.

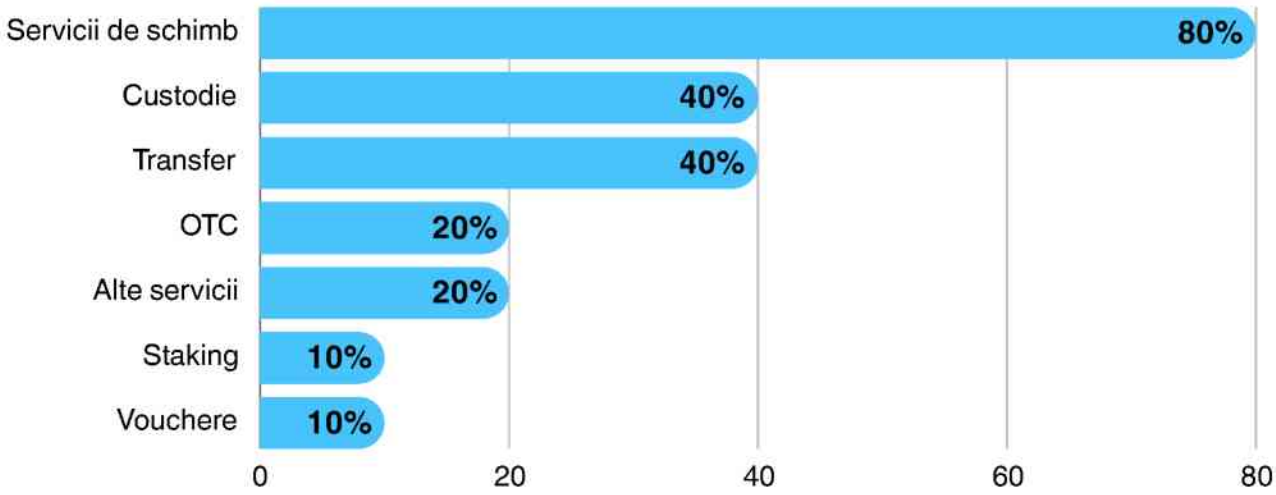
**Concluzie**

**Răspunsurile VASP-urilor la întrebările privind clienții relevă o serie de riscuri semnificative, inclusiv riscurile asociate clienților din jurisdicții cu risc ridicat, clienților PEP și celor care activează în sectoare economice vulnerabile. Chiar dacă majoritatea clienților provin din România și UE, există o expunere moderată la riscurile transfrontaliere și la structurile juridice complexe. Este necesară aplicarea continuă a măsurilor stricte de cunoaștere a clientelei (KYC) și de due diligence pentru a reduce vulnerabilitățile și a preveni activitățile ilicite în sectorul VASP din România.**

## Riscul privind produsele și serviciile

Analiza riscurilor asociate produselor și serviciilor oferite de VASP-uri este crucială pentru înțelegerea expunerii sectorului la vulnerabilitățile legate de spălarea banilor și finanțarea terorismului. O analiză detaliată a răspunsurilor din chestionare indică faptul că VASP-urile din România oferă o gamă diversă de servicii, printre care se numără schimbul între monede virtuale și monede fiduciare, furnizarea de custodie pentru criptoactive, și în unele cazuri, servicii OTC și tranzacții realizate prin intermediul ATM-urilor de criptoactive.

Conform datelor colectate și prezentate în figura de mai jos, 80% dintre VASP-uri oferă servicii de schimb între monede virtuale și monede fiduciare, acestea fiind printre cele mai frecvente servicii.




*Distribuția în procente a produselor și serviciilor oferite de VASP-urile din România*

Schimbul între monede virtuale și monede fiduciare implică o serie de vulnerabilități, întrucât permite convertirea rapidă a activelor digitale în monede tradiționale și invers, facilitând astfel posibilitatea disimulării provenienței fondurilor ilicite. Din această perspectivă, aceste VASP-uri trebuie să aplice măsuri stricte de cunoaștere a clientelei și de monitorizare a tranzacțiilor pentru a preveni utilizarea platformelor lor în scheme de spălare a banilor.

În privința serviciilor de custodie pentru criptoactive, doar aproximativ 30% dintre entități oferă aceste servicii. Custodia criptoactivelor prezintă riscuri semnificative deoarece implică păstrarea și gestionarea fondurilor clienților, ceea ce poate facilita accesul neautorizat sau activități frauduloase în cazul unor sisteme de securitate cibernetică inadecvate.

De asemenea, un aspect important al evaluării riscurilor este legat de tranzacțiile prin intermediul ATM-urilor de criptoactive. Din datele obținute, doar câteva entități au raportat utilizarea ATM-urilor în perioada 2021-2024. Unul dintre VASP-uri a indicat operarea a 85 de ATM-uri pe teritoriul României, ceea ce reprezintă o proporție semnificativă față de celelalte entități care fie nu dețin ATM-uri, fie au înregistrat un număr redus. De exemplu, un alt VASP a raportat operarea a 5 ATM-uri pe teritoriul României și alte 6 deținute de terți. Aceste entități sunt expuse riscurilor asociate tranzacțiilor anonime sau cu identitate falsificată, în special în absența unor controale stricte KYC.

O altă entitate a raportat faptul că, deși a operat ATM-uri în trecut, activitatea sa a fost încheiată în ianuarie 2024, subliniind că utilizarea acestor aparate trebuie monitorizată atent pentru a preveni utilizarea lor în activități suspecte de spălare a banilor. În plus, există și VASP-uri care, deși nu au deținut ATM-uri în perioada evaluată, au oferit alte servicii conexe, cum ar fi intermedierea plăților cu criptoactive. În ceea ce privește măsurile de cunoaștere a clientelei pentru tranzacțiile realizate prin ATM-uri, răspunsurile VASP-urilor au variat. De exemplu, un VASP care operează ATM-uri a aplicat măsuri simplificate de KYC pentru tranzacțiile mai mici de 15.000 RON, în timp ce pentru tranzacțiile de peste acest prag au fost necesare verificări suplimentare, inclusiv confirmarea identității prin verificarea documentelor oficiale și verificarea clientului pe listele de sancțiuni internaționale.

Serviciile OTC reprezintă o altă categorie importantă în analiza riscurilor asociate produselor și serviciilor oferite de VASP-uri. Acestea au fost menționate de aproximativ 20% dintre VASP-uri, indicând că oferă astfel de servicii. Tranzacțiile OTC sunt tranzacții private între două părți, fără utilizarea unei platforme de schimb publice. Deși aceste servicii pot oferi avantaje în termeni de flexibilitate și posibilitatea de a gestiona volume mari de tranzacții, ele prezintă riscuri semnificative, în special în ceea ce privește anonimitatea și evitarea măsurilor stricte de cunoaștere a clientelei.

Tranzacțiile OTC sunt deseori preferate de investitorii mari datorită faptului că pot negocia prețuri mai favorabile în afara piețelor deschise. Însă, tocmai din acest motiv, există riscul ca tranzacțiile OTC să fie utilizate pentru a evita controalele și cerințele de raportare impuse de reglementările SB/FT.

**Concluzie**

**Riscul asociat produselor și serviciilor oferite de VASP-uri este considerat a fi unul ridicat, în special din cauza anonimității și complexității tranzacțiilor, cum ar fi schimburile între monede virtuale și monede fiduciare, custodia criptoactivelor și operarea ATM-urilor de criptoactive. Aceste activități prezintă provocări majore în ceea ce privește conformitatea cu reglementările SB/FT. De asemenea, serviciile OTC contribuie la acest risc ridicat, datorită naturii private a tranzacțiilor, care necesită o monitorizare mai strictă și aplicarea măsurilor de cunoaștere a clientelei.**

## Riscul de conformitate

Riscul de conformitate reprezintă un aspect esențial în activitatea VASP-urilor, având în vedere cerințele riguroase impuse de legislația națională și internațională privind prevenirea spălării banilor și finanțarea terorismului.

În acest context, respectarea reglementărilor și aplicarea măsurilor adecvate pentru cunoașterea clientelei, monitorizarea tranzacțiilor și raportarea activităților suspecte sunt factori critici în gestionarea riscului de conformitate. Analiza datelor obținute din chestionarele completate de VASP-uri oferă o imagine detaliată asupra gradului de conformitate și a practicilor implementate de aceste entități.

Răspunsurile VASP-urilor indică faptul că majoritatea acestora (80%) au obținut venituri constante din activități legate de criptoactive în perioada 2021-2024, în timp ce doar 20% nu au înregistrat venituri. Acele 20% din VASP-uri care nu au înregistrat venituri în această perioadă sunt fie entități nou înființate, fie se află în faza incipientă a activității lor. Această activitate economică intensă subliniază importanța aplicării unor măsuri de conformitate stricte pentru a preveni riscurile asociate cu tranzacțiile de criptoactive și cu clienții implicați.

În ceea ce privește procedurile de identificare a clientelei, toate VASP-urile analizate au implementat astfel de măsuri, însă metodele aplicate variază. Aproximativ 20% dintre entități folosesc verificarea în persoană, în timp ce majoritatea optează pentru verificarea online sau prin platforme digitale. Un aspect notabil este faptul că 70% dintre VASP-uri utilizează verificări suplimentare pentru clienții PEP, iar 60% aplică verificări suplimentare pentru clienții din jurisdicții cu risc ridicat. Un alt element esențial este utilizarea inteligenței artificiale (AI) pentru verificarea documentelor de identitate – o tehnologie adoptată de 70% dintre entități. Această abordare modernă oferă o mai mare eficiență și precizie în identificarea potențialelor riscuri și în asigurarea conformității cu cerințele legale.

Mai mult de jumătate dintre VASP-urile chestionate au implementat sisteme automate pentru monitorizarea și detectarea tranzacțiilor suspecte, un element cheie în gestionarea riscului de conformitate și prevenirea activităților de spălare a banilor și finanțare a terorismului. Aceste sisteme utilizează tehnologii avansate, precum GBCAS, Chainalysis și alte soluții personalizate, care permit analiza datelor în timp real și identificarea rapidă a tranzacțiilor neobișnuite sau potențial suspecte. Implementarea acestor soluții oferă VASP-urilor capacitatea de a seta reguli configurabile, scoruri de risc și alerte automate, astfel încât să poată identifica tranzacții care depășesc anumite praguri valorice sau care provin din jurisdicții cu risc ridicat.

Cu toate acestea, deși sistemele sunt disponibile și utilizate, numărul de tranzacții suspecte raportate la Oficiul Național de Prevenire și Combatere a Spălării Banilor rămâne scăzut. Acest aspect sugerează fie că tranzacțiile suspecte sunt rar întâlnite în cadrul acestor entități, fie că există o posibilă sub-raportare cauzată de dificultăți în identificarea și evaluarea riscurilor. În unele cazuri, VASP-urile au recurs la soluții personalizate dezvoltate intern, care includ monitorizarea frecvenței tranzacțiilor, analiza comportamentului clientului și verificarea automată a adreselor cripto pe listele de sancțiuni.

De asemenea, VASP-urile care au utilizat sisteme avansate de tip SaaS (Software as a Service) au beneficiat de capabilități suplimentare, cum ar fi analiza datelor blockchain și detectarea riscurilor în timp real. Aceste soluții pot juca un rol crucial în îmbunătățirea eficienței sistemelor de conformitate și în creșterea gradului de detecție a tranzacțiilor suspecte.

În ceea ce privește raportarea/sesizarea altor autorități în afară de ONPCSB, aceasta este rară. Doar o mică parte dintre VASP-uri au menționat că au efectuat raportări sau sesizări către autorități precum Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism, Poliția Română sau Agenția Națională de Administrare Fiscală. Numărul raportărilor variază, fiind de obicei între 0 și 8 cazuri pe an, ceea ce indică faptul că expunerea la riscuri semnificative este limitată.

Principalii indicatori de suspiciune identificați de VASP-uri includ tranzacțiile nejustificate de activitatea clientului, tranzacțiile frecvente către jurisdicții cu risc ridicat și refuzul clienților de a furniza informațiile necesare pentru conformarea la cerințe. De asemenea, o proporție semnificativă a VASP-urilor a identificat tranzacții legate de PEP și tranzacții care evită limitele de raportare prin fragmentarea transferurilor.

În ceea ce privește măsurile de cunoaștere a clientelei la ATM-urile de criptoactive, aproximativ 30% dintre VASP-urile care operează ATM-uri aplică măsuri simplificate de cunoaștere a clientelei pentru tranzacțiile de valori mici, în general sub 15.000 RON. În aceste cazuri, verificările includ confirmarea adresei de portofel a clientului prin intermediul unor software-uri avansate de informații blockchain care oferă o monitorizare rapidă, precisă și de risc a tranzacțiilor și adreselor de portofele virtuale, cât și verificarea acestora pe listele de sancțiuni internaționale. Pentru tranzacțiile de valori mai mari, măsurile devin mai complexe pentru a asigura conformitatea și gestionarea eficientă a riscurilor.

Un operator de ATM-uri de criptoactive menționează că pentru sume tranzacționate între 15.000 și 30.000 RON pe zi, solicită verificări suplimentare, cum ar fi confirmarea numărului de telefon printr-un cod trimis prin SMS. În situațiile în care tranzacțiile depășesc pragul de 30.000 RON pe zi, măsurile de KYC sunt intensificate. Acestea includ atât verificarea manuală, cât și cea automată a documentelor de identitate, folosind tehnologii avansate bazate pe inteligența artificială. Procesul de verificare poate implica scanarea cărții de identitate sau a pașaportului și realizarea unei verificări video în timp real în care clientului i se cere să facă un selfie sau să își miște capul, pentru a confirma că este aceeași persoană cu cea din documentul prezentat.

Pentru clienții considerați cu risc mai ridicat, măsurile devin și mai riguroase. În aceste situații, se efectuează verificări ale adresei de domiciliu pe baza unor documente, cum ar fi facturi de utilități sau extrase bancare. De asemenea, clienții trebuie să completeze o declarație pe propria răspundere, prin care să confirme că sunt beneficiarii reali ai tranzacțiilor și să declare sursa fondurilor utilizate. În cazurile în care este necesar, VASP-urile solicită documente justificative suplimentare pentru a verifica originea fondurilor.

Pentru a preveni eventualele abuzuri sau încercări de fragmentare a tranzacțiilor, ATM-urile unui operator au stabilit o limită zilnică de 48.000 RON, atât pentru cumpărare, cât și pentru vânzare. Dacă un client dorește să efectueze o tranzacție care depășește această limită, acesta trebuie să contacteze VASP-ul pentru a solicita ridicarea limitei, după ce identitatea sa a fost verificată suplimentar. În toate cazurile, clienții sunt întrebați pe ecran dacă sunt PEP și dacă achiziționează Bitcoin în propriul portofel electronic. Dacă clienții sunt PEP sau dacă portofelul electronic nu le aparține, tranzacția este automat refuzată deoarece VASP-ul nu acceptă clienți PEP sau achizițiile în portofele străine.

Un aspect important de evidențiat în cazul schimburilor între monede virtuale și monedele fiduciare prin intermediul ATM-urilor de criptoactive, este caracterul extrem de riscant al acestor servicii din perspectiva SB/FT, din cauza utilizării numerarului, a lacunelor din legislația națională, cât și a faptului că nu sunt aplicate întotdeauna măsuri de cunoaștere a clientelei, iar în unele cazuri, monitorizarea tranzacțiilor se efectuează manual.

**Concluzie**

**Riscul de conformitate în sectorul VASP din România este un element de importanță majoră, dat fiind că neconformitatea poate atrage sancțiuni semnificative sau poate expune platformele la riscuri legale și reputaționale. Deși majoritatea VASP-urilor au implementat măsuri de conformitate, inclusiv proceduri KYC și soluții automate de monitorizare, rămân provocări legate de uniformitatea aplicării acestora, de identificarea și raportarea activităților suspecte, cauzată de cunoașterea insuficientă a tipologiilor de SB/FT în domeniul VASP. Monitorizarea atentă și aplicarea constantă a măsurilor de prevenire sunt esențiale pentru a asigura integritatea acestui sector în continuă creștere.**

## Riscul privind tranzacțiile

Riscul de tranzacții reprezintă o dimensiune esențială în evaluarea vulnerabilităților sectorului VASP din România, fiind strâns legat de volumul, frecvența și natura tranzacțiilor desfășurate de entitățile care oferă servicii în domeniul criptoactivelor. În cadrul analizei, au fost evidențiate mai multe aspecte relevante pe baza răspunsurilor primite la întrebările din chestionar.

În ceea ce privește volumul anual al tranzacțiilor, majoritatea VASP-urilor au raportat un volum semnificativ de tranzacții cu criptoactive în perioada 2021-2024. De exemplu, unul dintre VASP-uri a înregistrat tranzacții de peste 133 de milioane de euro în 2021, în timp ce alte entități au raportat volume între câteva milioane și zeci de milioane de euro. Această activitate intensă indică faptul că VASP-urile sunt implicate activ în facilitarea tranzacțiilor cu criptoactive și subliniază importanța implementării măsurilor de prevenire a riscurilor legate de spălarea banilor și finanțarea terorismului. Totuși, există și entități care nu au raportat activitate semnificativă în această perioadă, fie din cauza faptului că au fost recent înființate, fie pentru că nu au avut o activitate intensă.

Nouă din zece VASP-uri au raportat că dețin și utilizează conturi bancare deschise în România, subliniind astfel integrarea majorității acestor entități în sistemul bancar național, cu excepția a două VASP-uri. Astfel, un VASP care a avut conturi în România, dar din 2022 a transferat operațiunile bancare în Lituania, această decizie poate fi motivată de considerente strategice, cum ar fi accesul mai facil la piețele internaționale sau optimizarea costurilor operaționale sau de căutarea unui cadru de reglementare mai flexibil.

Datele colectate pentru perioada 2021-2024 indică o ușoară scădere a numărului anual de clienți care tranzacționează la ATM-urile de criptoactive, conform raportărilor VASP-urilor. Un exemplu notabil este un VASP care a înregistrat o creștere considerabilă în 2022, cu 1.618 clienți, dar numărul acestora a scăzut la 1.337 în 2023 și dramatic la doar 7 clienți în 2024 (până în luna octombrie). În alte cazuri, unele VASP-uri au început să raporteze activitate la ATM-uri doar în anii mai recenți, în timp ce altele nu au înregistrat deloc tranzacții la ATM-uri în perioada analizată.

În ceea ce privește volumul tranzacțiilor, se observă un model similar de scădere treptată. De exemplu, un VASP a înregistrat un volum de 3,561,802 EUR în 2021, cu o ușoară creștere în 2022 (3,643,262 EUR), însă volumul a scăzut ușor la 3,455,444 EUR în 2023 și la 3,146,485 EUR în 2024 (până în luna octombrie). De asemenea, un alt VASP a înregistrat o scădere semnificativă a volumului tranzacțiilor la ATM-uri, de la 1,501,019 EUR în 2023 la doar 4,915 EUR în 2024 (până în octombrie). Această evoluție reflectă o ușoară diminuare a activității la ATM-urile de criptoactive, care poate fi atribuită unor factori diverși, inclusiv schimbărilor în comportamentul clienților și ajustările reglementărilor din domeniu. Chiar dacă scăderile nu sunt considerabile, tendințele actuale indică o stabilizare sau chiar o reducere a activității în unele cazuri, ceea ce sugerează necesitatea monitorizării atente a evoluției pieței și a adaptării strategiilor de conformitate și operare pentru a răspunde noilor realități din sectorul criptoactivelor.

**Concluzie**

**Riscul de tranzacții în sectorul VASP din România reflectă o ușoară scădere a activității, atât la ATM-uri, cât și în volumul general al tranzacțiilor, conform datelor colectate pentru perioada 2021-2024. Deși unele VASP-uri au înregistrat volume semnificative de tranzacții, tendința generală arată o diminuare treptată. Unul dintre motivele acestei scăderi poate fi considerat evoluția pieței criptoactivelor, care, după vârful din 2021, a intrat într-o fază de corecție (scădere a prețului criptoactivelor). Această scădere evidențiază importanța monitorizării continue și a adaptării măsurilor de conformitate pentru a gestiona eficient riscurile asociate tranzacțiilor cu criptoactive în contextul fluctuațiilor pieței.**

## 3.5. Criminalitate și tendințe emergente în sectorul VASP din România

În cadrul evaluării riscurilor asociate sectorului VASP, au fost colectate date și informații reprezentând contribuții relevante de la organele de aplicare a legii și de la alte autorități competente în domeniu. Aceste contribuții au oferit o perspectivă cuprinzătoare asupra tipologiilor asociate sectorului VASP, *modus operandi* și riscurile identificate, evidențiind vulnerabilitățile pe care infractorii le pot exploata la nivel național.

La nivel național a fost identificat un număr redus de cazuri în care s-a săvârşit o infracțiune de spălare a banilor care au avut la bază infracțiuni predicat asociate sectorului VASP, complexitatea acestora și tehnicile sofisticate de disimulare a fondurilor utilizate făcându-le deosebit de periculoase. Utilizarea criptoactivelor conferă infractorilor un grad ridicat de anonimitate, ceea ce complică monitorizarea și urmărirea fluxurilor financiare, în special în cazurile care implică jurisdicții multiple. Tendințele globale indică o creștere a utilizării platformelor VASP pentru transferuri rapide și anonime de fonduri, deseori implicate în structuri complexe de tip „layering", menite să ascundă proveniența fondurilor ilicite.

Datele și informațiile colectate de la organele de aplicare a legii indică faptul că infracțiunile economice, informatice și cele de înșelăciune sunt cele mai frecvent întâlnite activități ilicite asociate sectorului VASP, subliniind riscurile majore pe care le implică utilizarea acestui sector de către infractori. În ceea ce privește infracțiunile economice și de înșelăciune, sectorul VASP din România este mai expus la scheme de tip Ponzi, fraude de investiții și tranzacții fictive. Infractorii utilizează serviciile oferite de VASP-uri pentru a direcționa fonduri obținute în mod fraudulos, atrăgând victimele prin promisiuni de câștiguri rapide și substanțiale din investiții în criptomonede. Ulterior, aceste fonduri sunt transferate rapid între conturi și platforme de schimb de criptomonede, complicând astfel procesul de urmărire a fluxurilor financiare și ascunzând proveniența ilicită a acestora.

Schemele de fraudă economică din sectorul VASP sunt facilitate de reglementările incomplete și cerințele slabe privind verificarea identității clienților. Platformele care impun cerințe minime de cunoaștere a clientului (KYC) oferă infractorilor posibilitatea de a acționa cu un grad înalt de anonimitate, favorizând astfel utilizarea lor pentru activități ilicite. În plus, având în vedere riscurile asociate tranzacțiilor prin crypto-ATM-uri, informațiile furnizate de autorități au scos la iveală un număr semnificativ de activități infracționale.

În sfera infracțiunilor informatice și a atacurilor cibernetice, portofelele digitale și platformele de tranzacționare sunt adesea vizate de atacuri de tip „phishing" și „hacking". Infractorii folosesc tehnici avansate pentru a obține acces neautorizat la fonduri prin aplicații de control la distanță, permițându-le să efectueze tranzacții frauduloase în numele victimelor. De asemenea, atacurile de tip „ransomware" reprezintă o amenințare

semnificativă asociată sectorului VASP, criptomonedele fiind preferate pentru plata răscumpărărilor datorită nivelului ridicat de anonimitate pe care îl oferă. La momentul actual, la nivel național autoritățile competente gestionează monede virtuale indisponibilizate în valoare 6.000.000 USD, provenite în principal din dosare penale având ca obiect infracțiuni informatice.

Din informațiile colectate de la autorități, au reieșit și alte tendințe importante, printre care scenariile de fraudare ce implică impersonarea angajaților unor instituții publice sau financiare de încredere. În aceste cazuri, atacatorii contactează utilizatorii de servicii financiare sub falsa identitate a unor reprezentanți oficiali, modificându-și identitatea pentru a reflecta poziții de autoritate. Sub pretextul prevenirii unor fraude iminente, aceștia conving victimele să deschidă linii de credit și să depună sumele obținute într-un portofel digital controlat de atacatori, folosind mijloace de conversie în active virtuale.

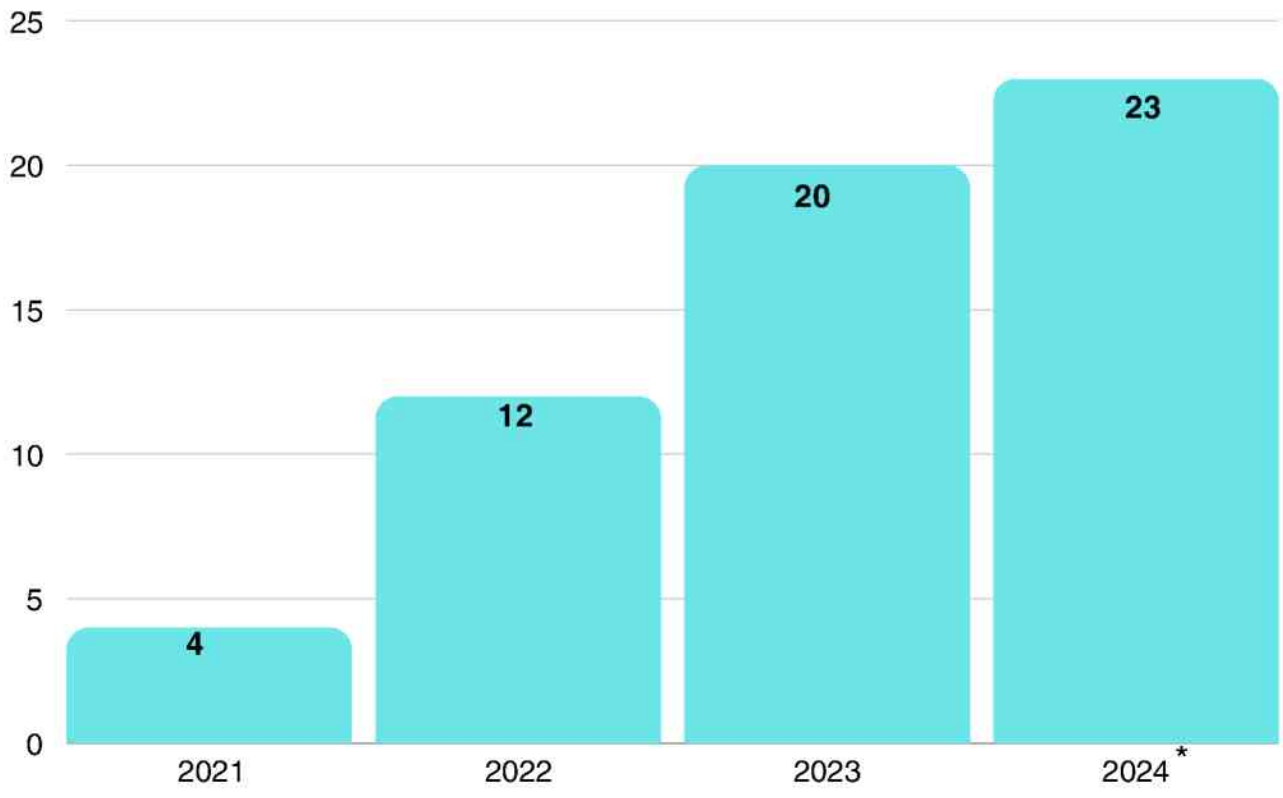
Criminalitatea transfrontalieră reprezintă o vulnerabilitate semnificativă în sectorul VASP, având în vedere caracterul global și descentralizat al criptomonedelor. Aceste caracteristici facilitează utilizarea lor pentru spălarea banilor și alte activități infracționale cu caracter transnațional. Infractorii apelează frecvent la tehnici de „layering" și „mixing" pentru a disimula originea fondurilor ilicite, ceea ce complică eforturile autorităților de a urmări fluxurile financiare și de a recupera aceste fonduri. În cadrul tranzacțiilor transfrontaliere, VASP-urile sunt adesea folosite pentru operațiuni internaționale complexe, implicând multiple jurisdicții, ceea ce creează provocări semnificative pentru autoritățile competente în investigarea și combaterea acestor infracțiuni.

Din informațiile puse la dispoziție de către organele de aplicare a legii, s-au evidențiat solicitări de asistență reciprocă în investigarea infracțiunilor de spălare a banilor, bazate pe infracțiuni predicat asociate sectorului VASP. Aceste solicitări subliniază importanța cooperării cu Europol, care facilitează schimbul de informații și coordonarea la nivel internațional, contribuind astfel la combaterea eficientă a criminalității transfrontaliere. Colaborarea strânsă cu Europol și alte organisme internaționale este esențială pentru a depăși provocările juridice și operaționale implicate în investigarea tranzacțiilor complexe care traversează multiple jurisdicții.

În ceea ce privește cooperarea internațională, ONPCSB-FIU România a gestionat un număr semnificativ de informări spontane din partea unităților de informații financiare din alte state membre, transmise ulterior autorităților competente, contribuind astfel la gestionarea riscurilor din sectorul VASP. În același timp, ONPCSB a primit cereri de informații care au facilitat colaborarea internațională, consolidând eforturile de monitorizare și combatere a infracțiunilor transfrontaliere.

Fraudele de tip „investment scam” în sectorul VASP reprezintă o tendință emergentă importantă. În cadrul acestor scheme, infractorii atrag investitorii cu promisiunea unor randamente rapide și ridicate din investiții în criptomonede și NFT-uri false, prezentate ca oportunități legitime. Mulți dintre acești investitori sunt în cele din urmă înșelați, iar fondurile lor sunt redirecționate rapid în portofele digitale controlate de infractori. Aceste scheme sunt adesea amplificate de utilizarea tehnologiilor avansate de phishing și acces la distanță, permițând infractorilor să manipuleze conturile victimelor și să transfere fondurile în multiple jurisdicții, complicând eforturile de recuperare. Utilizarea platformelor VASP cu reglementări incomplete și cerințe minime KYC, oferă un grad ridicat de anonimitate pentru astfel de infractori, subliniind vulnerabilitățile pe care acest sector le prezintă în fața acestui tip de înșelăciune.

În contextul riscurilor asociate sectorului VASP, rapoartele de tranzacții suspecte (RTS) transmise de entitățile raportoare reprezintă un instrument esențial în identificarea și prevenirea activităților infracționale. În perioada 2021-2024, ONPCSB a primit un număr semnificativ de rapoarte de tranzacții suspecte asociate indirect cu sectorul VASP și 59 de RTS-uri de la VASP-uri. Urmare a rapoartelor de tranzacții suspecte primite în perioada 2021-2024, au fost diseminate 10 informări către Parchetul de pe lângă Înalta Curte de Casație și Justiție, care au avut ca obiect și tranzacții cu monede virtuale, fiind întocmite 6 dosare penale.
Totalul de 59 de RTS-uri primite de la entitățile din categoria VASP sunt defalcate astfel:




*până în octombrie 2024

Cu toate acestea, raportările specifice sectorului VASP rămân insuficiente pentru a oferi o imagine completă a riscurilor, ceea ce sugerează necesitatea unei supravegheri mai riguroase și a dezvoltării capacităților de analiză.

Fenomenul infracțional în sectorul VASP evoluează rapid, alimentat de inovațiile tehnologice și de creșterea utilizării criptomonedelor și a altor active digitale. Infractorii își ajustează permanent tacticile pentru a profita de vulnerabilitățile existente. Deși autoritățile și sectorul privat depun eforturi pentru a implementa măsuri mai stricte de supraveghere și reglementare, este necesară identificarea unor soluții tehnologice mai avansate pentru a monitoriza și urmări eficient tranzacțiile și a preveni activitățile ilicite.

O altă tendință îngrijorătoare este creșterea infracțiunilor de înșelăciune legate de investiții în criptomonede, aceste scheme devinind din ce în ce mai sofisticate și transnaționale, îngreunând capacitatea autorităților de a le combate. Utilizarea aplicațiilor de control la distanță complică detectarea și prevenirea acestor infracțiuni, iar victimele sunt adesea manipulate să participe involuntar la activități de spălare a banilor, amplificând astfel complexitatea investigațiilor și extinzând impactul asupra populațiilor vulnerabile.

Tendințele semnificative identificate reflectă utilizarea unor scheme complexe de „layering" și a serviciilor de „mixing" pentru a disimula proveniența fondurilor. Aceste metode subliniază nevoia de colaborare internațională mai strânsă și de dezvoltare a soluțiilor tehnologice capabile să facă față metodelor tot mai avansate utilizate de infractori.

Evaluarea riscurilor asociate sectorului VASP în România relevă un potențial ridicat de inovare financiară, dar subliniază, în același timp, vulnerabilități semnificative exploatate de infractori. Deși numărul cazurilor de spălare a banilor asociate sectorului este redus, complexitatea și sofisticarea acestor infracțiuni, inclusiv utilizarea tehnicilor de disimulare precum „layering" și „mixing," creează riscuri majore. Criminalitatea transfrontalieră și caracterul global al criptomonedelor complică eforturile autorităților în urmărirea fluxurilor financiare și recuperarea fondurilor ilicite.

Pentru a aborda aceste riscuri emergente, consolidarea reglementărilor, utilizarea unor soluții tehnologice avansate și intensificarea cooperării internaționale, în special cu instituții precum Europol, sunt esențiale. De asemenea, datele și informațiile limitate existente la nivel național subliniază necesitatea unor mecanisme de raportare mai eficiente și a unei supravegheri mai riguroase pentru a oferi o înțelegere completă a fenomenului infracțional și a proteja integritatea sistemului financiar.

În concluzie, sectorul VASP impune o atenție sporită, o monitorizare continuă și o adaptare permanentă la noile tendințe și riscuri infracționale pentru a preveni exploatarea fenomenului infracțional și pentru a asigura protecția sistemului financiar național și internațional.

IV

# Identificarea amenințărilor și vulnerabilităților

## 4.1. Tipologii de spălare a banilor în domeniul VASP

Combaterea spălării banilor în sectorul furnizorilor de servicii de criptoactive este o prioritate, atât pentru autorități, cât și pentru instituțiile financiare, având în vedere anonimitatea și descentralizarea criptoactivelor, care facilitează activități ilegale. Odată cu creșterea popularității și utilizării criptoactivelor, eforturile de reglementare s-au intensificat, impunând măsuri mai stricte de cunoaștere a clientelei și monitorizare a tranzacțiilor. Totuși, sectorul rămâne vulnerabil din cauza inovației rapide și a diversității platformelor de tranzacționare și a produselor.

Pe baza ghidului ***„Indicatori de suspiciune și tipologii de spălare a banilor în domeniul criptoactivelor”***, publicat de Oficiul Național de Prevenire și Combatere a Spălării Banilor în 2023, au fost analizate șase dintre cele mai comune tipologii de spălare a banilor identificate în domeniul criptoactivelor. Acest ghid actualizat oferă o imagine clară a modului în care rețelele criminale folosesc tehnologiile criptoactive pentru a-și desfășura activitățile ilicite.

## 01 Utilizarea platformelor neconforme

Spălarea de bani directă prin tranzacții cu criptoactive reprezintă procesul prin care fondurile ilicite sunt introduse în mediul cripto, transferate prin multiple tranzacții pentru a ascunde originea lor și apoi convertite în criptoactive curate.

## 02 Utilizarea cărăușilor de bani în spălarea de bani

Utilizarea cărăușilor de bani în spălarea banilor în domeniul criptoactivelor se referă la implicarea persoanelor intermediare în procesul de transfer și conversie a fondurilor ilicite, cu scopul de a ascunde traseul și beneficiarii finali ai acestor fonduri.

## 03 Utilizarea mixerelor și a platformelor DeFi pentru ascunderea urmelor

Este o tehnică folosită în spălarea de bani în domeniul criptoactivelor, în care tranzacțiile sunt amestecate și transferate prin intermediul platformelor descentralizate pentru a crește dificultatea identificării și urmăririi originii și destinației fondurilor.

## 04 Utilizarea ATM-urilor de cripto în scopul spălării banilor

Reprezintă o metodă prin care fondurile ilicite sunt convertite în criptoactive prin intermediul ATM-uriloe cripto, oferindu-le infractorilor posibilitatea de a obține fonduri "curate" într-un mod aparent legal și fără a dezvălui identitatea lor.

## 05 Utilizarea NFT-urilor în scopul spălării banilor

Utilizarea NFT-urilor în scopul spălării banilor implică transferul fondurilor ilicite prin intermediul acestor active digitale unice, care permit infractorilor să ascundă originea ilicită și să spele fondurile, profitând de caracteristicile speciale și dificultatea de urmărire asociate cu acestea.

## 06 Utilizarea ICO-urilor în scopul spălării banilor

Utilizarea ICO-urilor în scopul spălării banilor constă în lansarea de campanii de finanțare colectivă prin intermediul criptoactivelor, prin care infractorii își ascund originile fondurilor ilicite și obțin aparența legalității prin intermediul investițiilor și tranzacțiilor cripto.

## 1. Utilizarea platformelor neconforme

Una dintre metodele comune de spălare a banilor prin tranzacții cu criptoactive implică utilizarea platformelor de schimb neconforme. Infractorii exploatează vulnerabilitățile acestor platforme, care adesea nu implementează măsuri de cunoaștere a clientelei și nu se conformează reglementărilor din jurisdicțiile specifice.

Platformele de schimb neconforme sau care impun cerințe minime de cunoaștere a clientelei oferă un mediu propice pentru spălarea banilor, deoarece nu solicită informații detaliate despre identitatea clienților sau despre originea fondurilor. Acestea tind să evite aplicarea rigorilor reglementărilor anti-spălare de bani și a standardelor KYC, facilitând astfel utilizarea de conturi anonime sau cu informații de identificare minime, permițând infractorilor să efectueze tranzacții fără a fi supuși unei verificări adecvate a identității lor și fără a fi înregistrate detaliile relevante în scopul de a identifica activitățile ilicite. De asemenea, aceste platforme nu aplică restricții privind volumul și valorile tranzacțiilor, oferind astfel posibilitatea infractorilor de a efectua tranzacții mari și frecvente fără a atrage atenția autorităților.

### Descrierea tipologiei

- **un individ obține criptoactive prin intermediul unui atac ransomware**, care constă în preluarea controlului asupra sistemelor informatice ale victimelor și în solicitarea unei răscumpărări în criptoactive. După obținerea criptoactivelor, infractorul urmărește să le legalizeze prin scheme complexe de spălare a banilor, cum ar fi schimburile succesive pe platforme neconforme, pentru a ascunde urma tranzacțiilor și pentru a îngreuna urmărirea activităților ilicite;

- primul pas în procesul de spălare a banilor constă în **identificarea unei platforme de schimb neconforme și deschiderea unui cont anonim pe aceasta**. Prin deschiderea unui cont anonim, persoana evită furnizarea de informații detaliate despre identitatea sa, ceea ce îi permite să efectueze tranzacții fără a fi supus unei verificări adecvate a identității și fără a lăsa urme digitale care ar putea duce la identificarea sa. Alegerea unei astfel de platforme neconforme este esențială, deoarece aceasta oferă un grad mai mare de anonimat și reduce riscul de a fi detectat de către autorități sau instituțiile de aplicare a legii;

- după ce criptoactivele obținute ilegal sunt transferate pe această platformă, **acestea vor fi convertite în alte active digitale sau în monede fiduciare;**

- **criptoactivele „murdare”, transformate în alte active digitale, vor fi ulterior schimbate în monedă fiduciară prin intermediul unor tranzacții succesive**, realizate atât pe platforme neconforme, cât și pe platforme conforme;

- **fondurile rezultate din aceste schimburi de criptoactive vor fi apoi transferate într-un cont bancar sau vor fi retrase în numerar de la un ATM de cripto.** Prin această etapă, infractorul încearcă să integreze fondurile obținute ilegal în sistemul financiar tradițional sau să le convertească în bani lichizi, facilitând astfel utilizarea lor în activități legale sau pentru a evita detectarea tranzacțiilor ilicite. Această acțiune adițională contribuie la crearea unei aparențe de legalitate asupra fondurilor și complică urmărirea fluxurilor de bani, adăugând un nivel suplimentar de complexitate în procesul de investigare a activităților infracționale.

## Indicatori specifici tipologiei

1. Platforma de schimb utilizată nu respectă reglementările anti-spălare a banilor, fiind adesea nou înființată;

2. Conturi anonime sunt deschise fără verificări adecvate sau măsuri de cunoaștere a clientelei;

3. Nu sunt impuse limite asupra valorilor sau volumelor tranzacțiilor, permițând tranzacții mari fără a atrage atenția;

4. Clienții participă frecvent la tranzacții pe platforme neconforme, care nu aplică standarde KYC;

5. Platforma de schimb afișează pe site-ul său web mesaje sugestive care promovează anonimatul utilizatorilor și menționează acceptarea numerarului în tranzacțiile cu criptoactive;

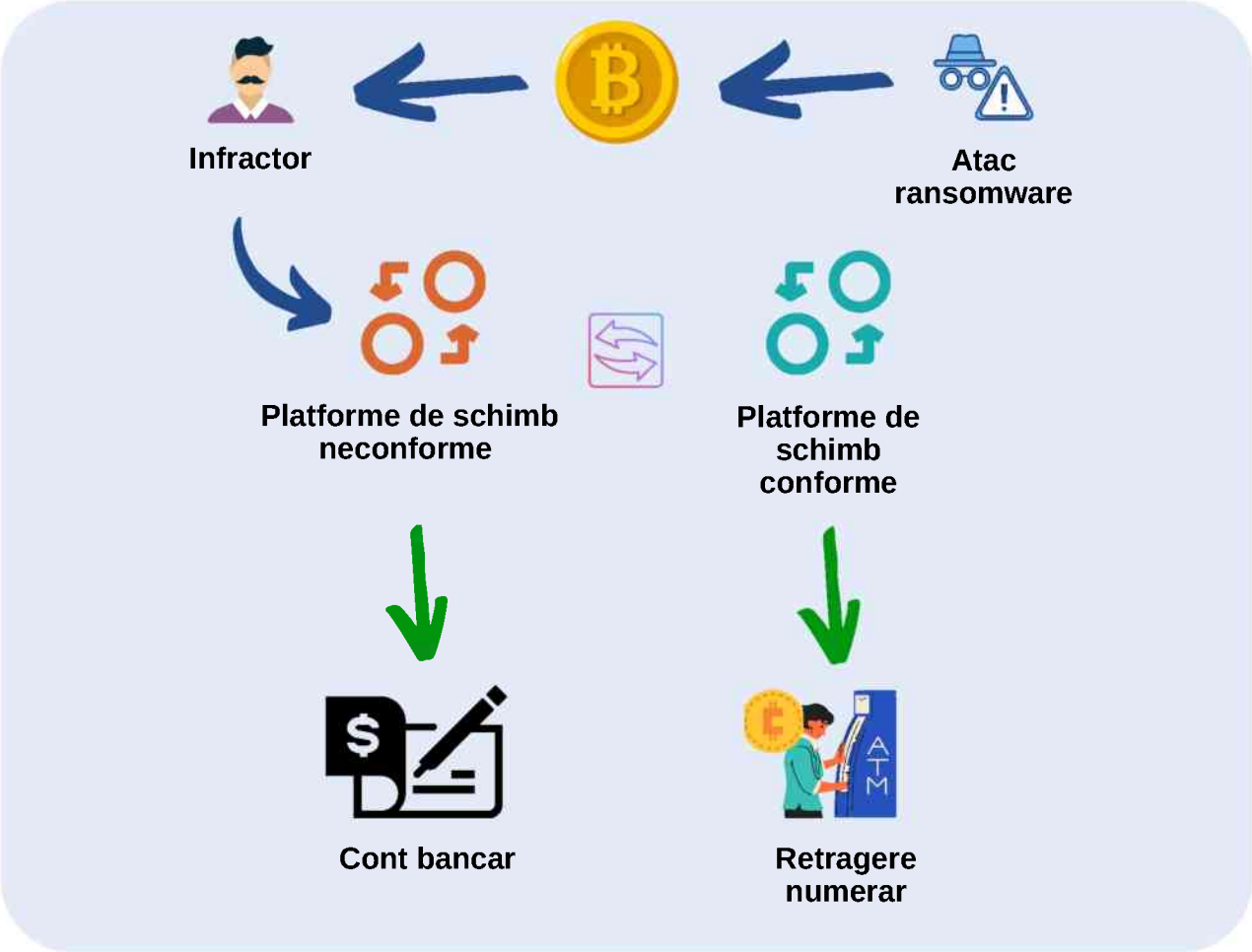
6. Platforma de schimb neconformă oferă servicii de chat între utilizatori, creând un mediu propice pentru comunicarea și coordonarea tranzacțiilor ilegale, precum și discuții legate de activități suspecte.

7. Implicarea platformei de schimb în tranzacții cu criptoactive de proveniență ilicită: există informații care indică implicarea platformei de schimb în tranzacții cu criptoactive provenite din surse ilicite. Acest lucru poate fi relevat de investigații anterioare sau de surse de informații disponibile public.

## Exemple concrete

1. Un individ implicat în activități ilegale, cum ar fi traficul de droguri sau infracțiuni cibernetice, folosește o platformă de schimb neconformă pentru a spăla banii. Deschide un cont fără a oferi informații detaliate și efectuează tranzacții fără verificări stricte ale identității, transferând și convertind criptoactivele pentru a ascunde originea fondurilor [13].

2. Un individ implicat în fraude online sau phishing folosește o platformă neconformă pentru a transfera fondurile în criptoactive. Efectuează schimburi între adrese anonime, evitând verificările stricte de identitate și crescând anonimatul. Astfel, își poate converti rapid fondurile obținute ilegal, făcând dificilă urmărirea și recuperarea acestora de către autorități [14].




[13] Financial Action Task Force (FATF) - Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html
[14] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021, https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

## 2. Utilizarea cărăușilor de bani în spălarea de bani

Spălarea de bani în domeniul criptoactivelor implică adesea utilizarea unor tactici sofisticate pentru a ascunde originile ilicite ale fondurilor și a evita detectarea de către autorități. Una dintre aceste tipologii este reprezentată de utilizarea cărăușilor de bani, cunoscuți și sub denumirea de „money mules".

Acești indivizi devin intermediari în transferul de fonduri ilicite, facilitând astfel spălarea și dispersia acestora prin intermediul criptoactivelor. Cărăușii de bani acceptă să primească fonduri provenite din activități ilegale în conturile lor personale sau în portofelele lor electronice, urmând apoi instrucțiunile infractorilor cu privire la transferurile și conversiile necesare pentru a ascunde urmele tranzacțiilor și a dispersa fondurile într-un mod aparent legal.

Prin implicarea cărăușilor de bani în acest proces complex, infractorii își pot spăla banii și pot beneficia de caracteristicile anonime și descentralizate ale criptoactivelor, oferindu-le o protecție suplimentară împotriva identificării și urmăririi de către autorități.

### Descrierea tipologiei

- recrutarea cărăușilor de bani: infractorii identifică potențiali cărăuși de bani prin intermediul diferitelor canale, cum ar fi site-uri de recrutare online, platforme de socializare sau chiar prin intermediul cunoștințelor personale. Aceștia sunt atrași prin promisiuni de câștiguri rapide și ușoare sau prin oferte de "muncă" în cadrul unor companii fictive;

- instruirea și implicarea cărăușilor de bani se referă la faptul că aceștia sunt instruiți și li se furnizează informații personale și bancare pentru a facilita transferurile de fonduri prin conturile lor, inclusiv crearea de conturi de criptoactive și desfășurarea tranzacțiilor în numele infractorilor;

- transferurile de fonduri: cărăușii de bani transferă fondurile ilicite către adresele de criptoactive specificate de infractori, folosind platforme de schimb sau portofele digitale;

- divizarea și disiparea fondurilor: odată ce fondurile sunt transferate către adresele de criptoactive, infractorii încearcă să disipeze și să divizeze aceste fonduri pentru a crește dificultatea urmăririi și identificării lor. Acest lucru poate implica realizarea unor tranzacții multiple și complexe între diferite adrese de criptoactive, amestecarea fondurilor prin intermediul mixerelor și utilizarea altor tactici de dispersare a fondurilor;

- Conversia în monede fiduciare: în final, fondurile convertite în criptoactive pot fi transferate înapoi în moneda fiduciară pentru a încerca să se spargă legătura cu activitățile ilegale inițiale. Pentru a realiza aceste transferuri, infractorii pot utiliza platforme de schimb cripto-monede fiduciare sau pot recurge la tranzacții P2P, implicând persoane sau entități dispuse să efectueze schimbul monetar. Acest proces complex contribuie la dificultatea de a urmări originea și destinația finală a fondurilor;

- Complicitatea cărăușilor de bani: este important de menționat că, în multe cazuri, cărăușii de bani pot fi conștienți sau chiar complici în activitățile ilegale în care sunt implicați, fiind motivați de profit sau manipulați prin șantaj sau amenințări.

## Indicatori specifici tipologiei

1. Relații cu persoane cunoscute ca fiind implicate în activități criminale: cauza principală a implicării caraușilor de bani în spălarea banilor este relația lor cu infractorii care au obținut fondurile ilegal. Acești carauși de bani au adesea conexiuni și cunoștințe în lumea infracțională, ceea ce facilitează procesul de spălare a banilor prin intermediul lor;

2. Servicii de intermediere financiară neautorizate: cărăușii de bani operează adesea ca intermediari financiari neautorizați, oferind servicii de transfer de fonduri și conversie valutară în numele infractorilor. Aceștia pot acționa ca persoane fizice sau pot avea societăți fantomă prin intermediul cărora își desfășoară activitățile ilegale;

3. Tranzacții financiare neobișnuite și atipice: cărăușii de bani desfășoară tranzacții financiare care nu se încadrează în tiparele normale de afaceri. Aceste tranzacții pot include schimburi frecvente de valută, transferuri rapide și repetate de fonduri între conturi și utilizarea unor modalități complexe de a ascunde urmele transferurilor financiare;

4. Utilizarea conturilor bancare multiple: cărăușii de bani utilizează de obicei conturi bancare multiple pentru a dispersa și ascunde fondurile. Aceștia pot avea conturi în diferite jurisdicții și pot efectua transferuri între aceste conturi pentru a îngreuna urmărirea fluxului de bani și pentru a ascunde urmele activităților ilicite;

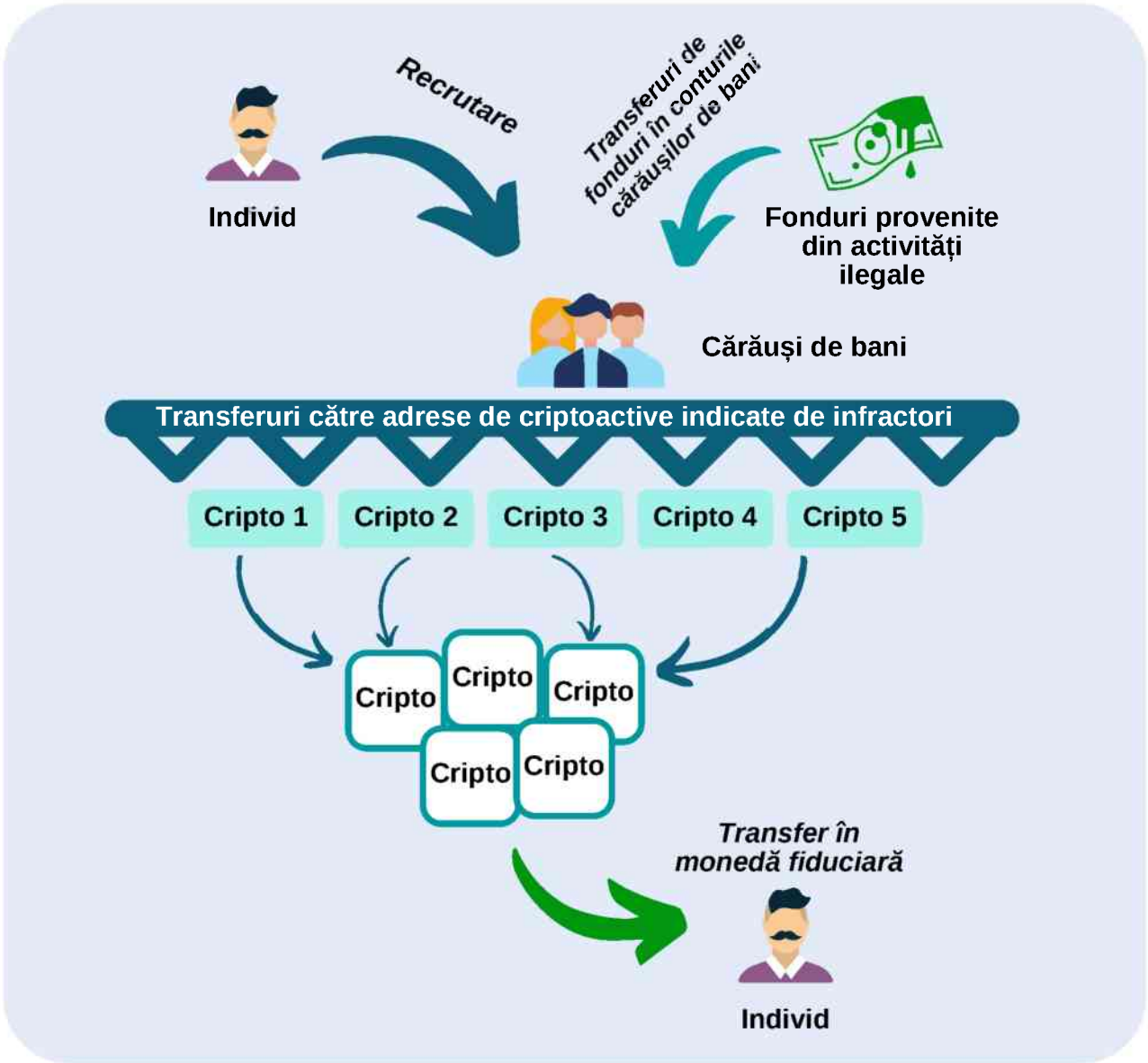
5. Tranzacții cu numerar: cărăușii de bani sunt implicați adesea în tranzacții cu numerar, deoarece oferă un nivel mai mare de anonimat și facilitează spălarea banilor prin schimburi rapide de fonduri în numerar între diferite persoane și locații;

6. Utilizarea unor scheme de structurare a tranzacțiilor: pentru a evita declanșarea RTS-urilor, cărăușii de bani pot utiliza scheme de structurare a tranzacțiilor prin care împart sume mari de bani în tranzacții mai mici pentru a evita atragerea atenției autorităților financiare.

## Exemple concrete

1. Un individ este recrutat pentru a transfera fonduri ilicite prin intermediul criptoactivelor către o persoană din altă țară. El primește instrucțiuni precise cu privire la conturile de criptoactive în care trebuie să efectueze transferurile și primește o parte din fonduri ca recompensă pentru serviciile sale [15];

2. Un grup infracțional utilizează o rețea extinsă de cărăuși de bani pentru a transfera fonduri provenite din activități de phishing și fraudă online în criptoactive. Aceștia folosesc adrese de criptoactive diverse și servicii de mixare pentru a ascunde originea fondurilor și a face dificilă urmărirea lor [16];




[15] Elliptic Typologies Report 2022 Edition, Preventing Financial Crime in Cryptoassets
[16 ] https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html;

## 3. Utilizarea mixerelor și a platformelor DeFi pentru ascunderea urmelor

Unul dintre instrumentele folosite de infractori pentru a ascunde urmele și a spăla fondurile ilicite este utilizarea mixerelelor și a platformelor descentralizate. Mixerele, cunoscute și sub denumirea de crypto tumblers, sunt platforme specializate care permit amestecarea criptoactivelor prin combinarea și amestecarea multiplelor tranzacții, ceea ce face dificilă urmărirea originii fondurilor. Aceste mixere oferă o formă de anonimat, deoarece nu este posibilă identificarea exactă a surselor și destinațiilor tranzacțiilor.

### Descrierea tipologiei

Utilizarea mixerelelor și a platformelor descentralizate reprezintă o tipologie comună în procesul de spălare a banilor prin intermediul criptoactivelor. Această tipologie implică următorii pași:

- infractorul își transferă criptoactivele într-un mixer. Acesta preia criptoactivele de la diverși utilizatori și le redistribuie într-un mod care maschează legătura dintre adresele de origine și cele de destinație. Acest proces implică de obicei mai multe tranzacții interne și schimburi între adrese diferite, ceea ce complică și mai mult urmărirea fondurilor;

- tranzacții anonime și lipsa verificării identității: mixerele și platformele descentralizate oferă utilizatorilor posibilitatea de a efectua tranzacții fără a fi obligați să dezvăluie informații personale detaliate sau să treacă prin verificări riguroase ale identității lor. Această caracteristică oferă utilizatorilor un nivel crescut de anonimat și confidențialitate în tranzacțiile financiare;

- lipsa controlului centralizat și stocarea fondurilor: platformele descentralizate, fără intermediari centralizați și fără stocarea fondurilor utilizatorilor, asigură confidențialitate și securitate sporită. Această caracteristică oferă utilizatorilor protecție, dar și infractorilor oportunitatea de a efectua tranzacții discreționare, fără lăsarea de urme evidente;

- mixerele și exchange-urile descentralizate oferă servicii de chat între utilizatori, favorizând comunicarea și coordonarea tranzacțiilor ilegale. Acest aspect facilitează schimbul de informații despre activități suspecte și sprijină infractorii în realizarea tranzacțiilor ilegale, fără a fi detectați;

- unele platforme pot fi implicate în tranzacții cu criptoactive ilicite. Mesajele sugestive de pe site, cum ar fi acceptarea numerarului sau instrucțiuni detaliate pentru transferuri bancare, pot semnala posibila implicare în activități ilegale.

## Indicatori specifici tipologiei:

- **Folosirea mixerelelor:** unul dintre indicatorii specifici este transferul frecvent al criptactivelor într-un mixer, precum Tornado Cash. Infractorii pot efectua o serie de tranzacții interne și schimburi între multiple adrese diferite, astfel încât să amestece criptoactivele și să ascundă urma tranzacțiilor. Acest proces complex și repetitiv de transferuri și schimburi are ca scop îngreunarea investigațiilor și identificarea originii sau destinației fondurilor;

- **Schimbul între criptoactive diferite:** un alt indicator este schimbul criptoactivelor amestecate în alte active digitale sau în monedă fiduciară prin intermediul platformelor descentralizate. Infractorii pot folosi aceste platforme pentru a converti criptoactivele în alte forme de active, făcând urmărirea tranzacțiilor mai dificilă;

- **Lipsa verificării riguroase a identității:** mixerele și platformele descentralizate nu impun măsuri stricte de verificare a identității utilizatorilor. Aceasta le permite infractorilor să deschidă conturi anonime fără a furniza informații personale detaliate sau a fi supuși unor verificări adecvate ale identității lor;

- **Mesaje sugestive privind anonimatul:** acestea pot fi prezentate pe unele platforme de mixare a criptoactivelor sau pe diverse platforme descentralizate, sugerând că utilizatorii pot efectua tranzacții fără a fi detectați sau urmăriți. Aceste mesaje pot încuraja utilizatorii să aibă încredere în platformă și să considere că activitățile lor financiare vor fi ascunse și protejate de ochiul autorităților. Prin promovarea unui sentiment de anonimat și confidențialitate, aceste mesaje pot atrage atenția infractorilor care doresc să își ascundă urmele și să profite de oportunitățile de spălare de bani fără consecințe;

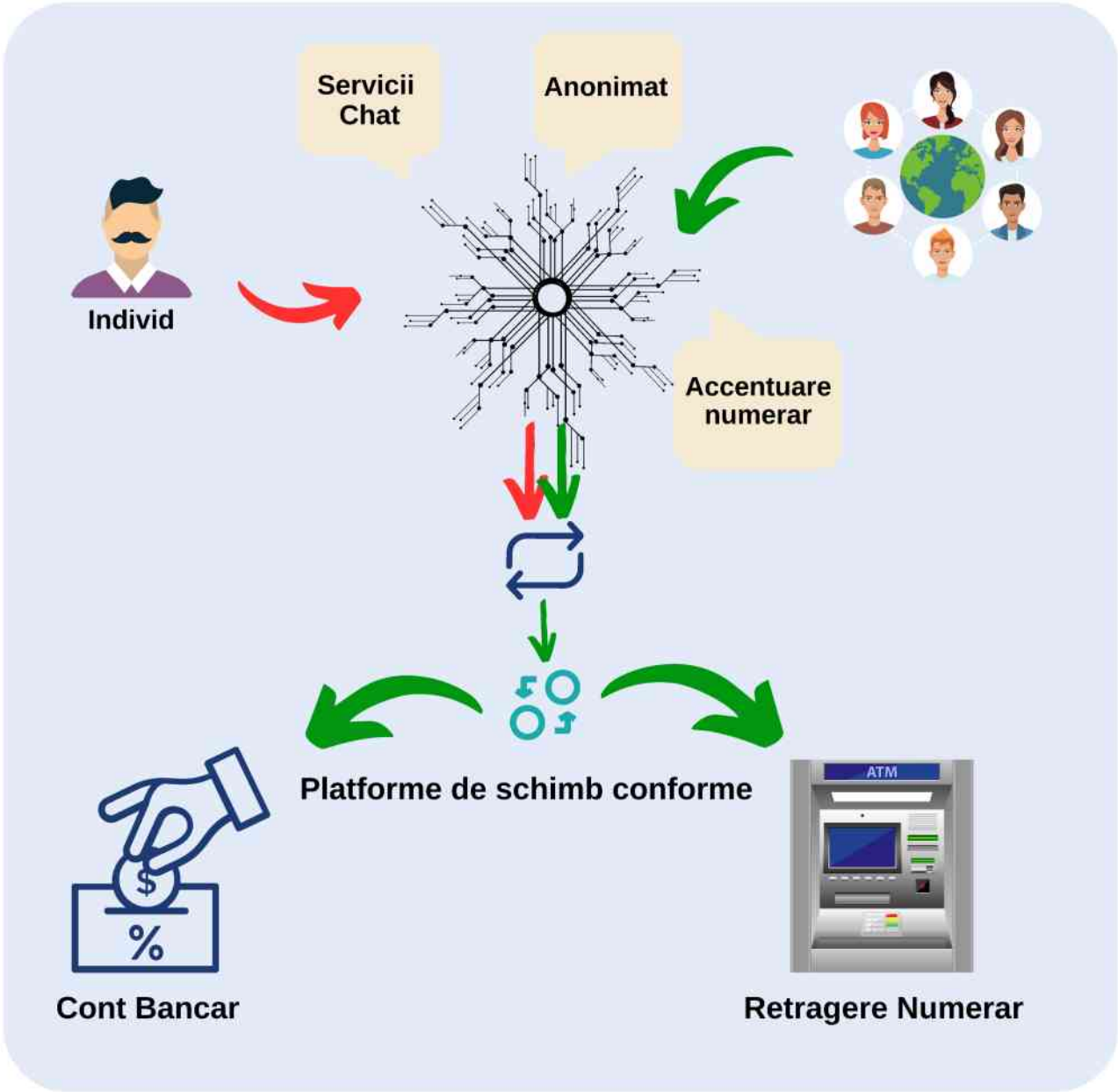
- **Implicarea platformelor în tranzacții ilicite:** există situații în care platformele de mixare de criptoactive sau platformele descentralizate sunt implicate în tranzacții cu criptoactive de proveniență ilicită. Acest lucru poate fi evidențiat prin investigații și informații relevante despre activitățile suspecte desfășurate pe aceste platforme.

## Exemple concrete:

1. Silk Road a fost un marketplace online cunoscut pentru comercializarea ilegală de droguri și alte bunuri ilicite. În acest caz, utilizatorii implicați în activități ilegale au folosit mixere descentralizate pentru a amesteca criptoactivele obținute ilegal, ascunzând astfel originea fondurilor și făcându-le să pară curate [17].

2. AlphaBay a fost un marketplace online închis în 2017 de către FBI, cunoscut pentru vânzarea ilegală de droguri, arme și alte bunuri ilicite. În acest caz, un grup infracțional a utilizat platforma descentralizată pentru a schimba criptoactivele obținute prin activități ilegale în alte active digitale sau în monedă fiduciară [18].

3. Un individ sau un grup infracțional implicat în infracțiuni financiare, cum ar fi fraudă bancară sau evaziune fiscală, utilizează un mixer pentru a amesteca criptoactivele obținute prin aceste activități ilicite. Mixerul preia criptoactivele și le amestecă cu alte fonduri provenite din surse legale, ceea ce face dificilă urmărirea și identificarea tranzacțiilor specifice [19].




[17] United States Department of Justice (DOJ), https://www.justice.gov/usao-sdny/press-release/file/1549821/download;
[18] FBI, https://www.fbi.gov/news/stories/alphabay-takedown;
[19] Europol - "Internet Organised Crime Threat Assessment (IOCTA) 2020" (https://www.europol.europa.eu/iocta-2020).

## 4. Utilizarea ATM-urilor de cripto în scopul spălării banilor

În contextul creșterii popularității ATM-urilor de cripto, acestea au devenit o soluție tot mai utilizată pentru a achiziționa și a vinde criptomonede într-un mod convenabil și accesibil. Cu toate acestea, o problemă semnificativă care trebuie abordată este legată de potențialul riscului de spălare a banilor asociat cu utilizarea acestor ATM-uri.

Potrivit unui studiu [20] efectuat în anul 2021, România se situează pe locul 9 în lume în ceea ce privește numărul raportat de ATM-uri de cripto, având în total 86 de astfel de ATM-uri în funcțiune. Această cifră indică o prezență semnificativă a acestor facilități în țara noastră, reflectând interesul crescut al populației pentru tranzacțiile cu criptoactive și nevoia de accesibilitate la acestea. Însă, odată cu creșterea utilizării ATM-urilor de cripto, se pun în evidență și o serie de riscuri asociate, în special în ceea ce privește spălarea banilor și utilizarea necorespunzătoare a criptoactivelor.

### Descrierea tipologiei

Utilizarea ATM-urilor de cripto în scopul spălării banilor reprezintă o tactică eficientă prin care infractorii încearcă să transforme fondurile provenite din activități ilegale în criptomonede.

ATM-urile cripto sunt dispozitive electronice care permit utilizatorilor să cumpere și să vândă criptomonede, precum Bitcoin, Ethereum sau Litecoin, într-un mod rapid și simplu.

Prin intermediul acestui tip de ATM-uri, infractorii pot realiza tranzacții anonime și confidențiale, fără a fi nevoie să-și dezvăluie identitatea sau să treacă prin procese de verificare riguroase. Această caracteristică a ATM-urilor de cripto oferă infractorilor un mediu propice pentru a spăla banii obținuți în mod ilegal. Aceștia pot achiziționa criptoactive prin intermediul acestor dispozitive, folosind fonduri provenite din activități ilicite și apoi pot vinde sau transfera criptoactivele către alte adrese, astfel ascunzând originile și destinațiile fondurilor.

În plus, ATM-urile de cripto permit efectuarea tranzacțiilor în numerar, ceea ce face procesul de spălare a banilor și mai greu de detectat. Infractorii pot depune numerar într-un ATM de cripto și pot primi criptoactive în schimb, fără ca sursa fondurilor să fie identificată sau urmărită. Această capacitate de a converti rapid numerarul în criptomonede facilitează procesul de spălare a banilor și complică investigațiile ulterioare ale autorităților. Fiind o tehnologie relativ nouă și în continuă evoluție, regulamentele și procedurile de supraveghere pot întâmpina dificultăți în a ține pasul cu inovațiile și tacticiile

[20] https:cryptohead.io/research/cryto-ready-index

utilizate de infractori.

Un alt aspect important al utilizării ATM-urilor de cripto în scopul spălării banilor este faptul că aceste dispozitive pot fi localizate în locații publice sau private, cum ar fi centre comerciale, baruri, restaurante sau chiar birouri. Acest fapt oferă infractorilor o gamă largă de locații în care pot efectua tranzacții fără a ridica suspiciuni. De asemenea, instalarea și configurarea unui ATM de cripto nu necesită licențe sau aprobări speciale în multe jurisdicții, ceea ce face dificilă monitorizarea și reglementarea eficientă a acestor facilități.

## Indicatori Specifici

- **Utilizarea repetată a aceluiași ATM de cripto pentru tranzacții semnificative în numerar** poate ridica semne de întrebare în privința provenienței fondurilor și a scopului utilizării acestora. Acest lucru poate indica o activitate suspectă, cum ar fi spălarea banilor sau finanțarea activităților ilegale;

- **ATM-ul de cripto este amplasat în zone cu un grad ridicat de infracționalitate** sau într-o locație asociată cu o afacere de fațadă, care poate fi deținută de către infractori;

- **Efectuarea unor tranzacții cu sume mari de bani într-un interval de timp scurt** reprezintă o tactică utilizată pentru a fragmenta și dispersa fondurile. Scopul acestei practici este de a ascunde urmele tranzacțiilor și de a îngreuna urmărirea și investigarea ulterioară a acestora de către autorități.

- **Efectuarea tranzacțiilor prin intermediul ATM-urilor de cripto în scopul transferului rapid** al fondurilor între adrese de criptomonede anonime. Utilizarea criptomonedelor cu caracter anonim facilitează ascunderea originii și destinației fondurilor, ceea ce poate indica o activitate ilegală;

- **Mai multe portofele digitale trimit fonduri prin intermediul ATM-urilor** către un singur destinatar într-o perioadă scurtă de timp;

- **Utilizarea unui număr mare de carduri sau portofele digitale** pentru a realiza tranzacții cu ATM-urile de cripto;

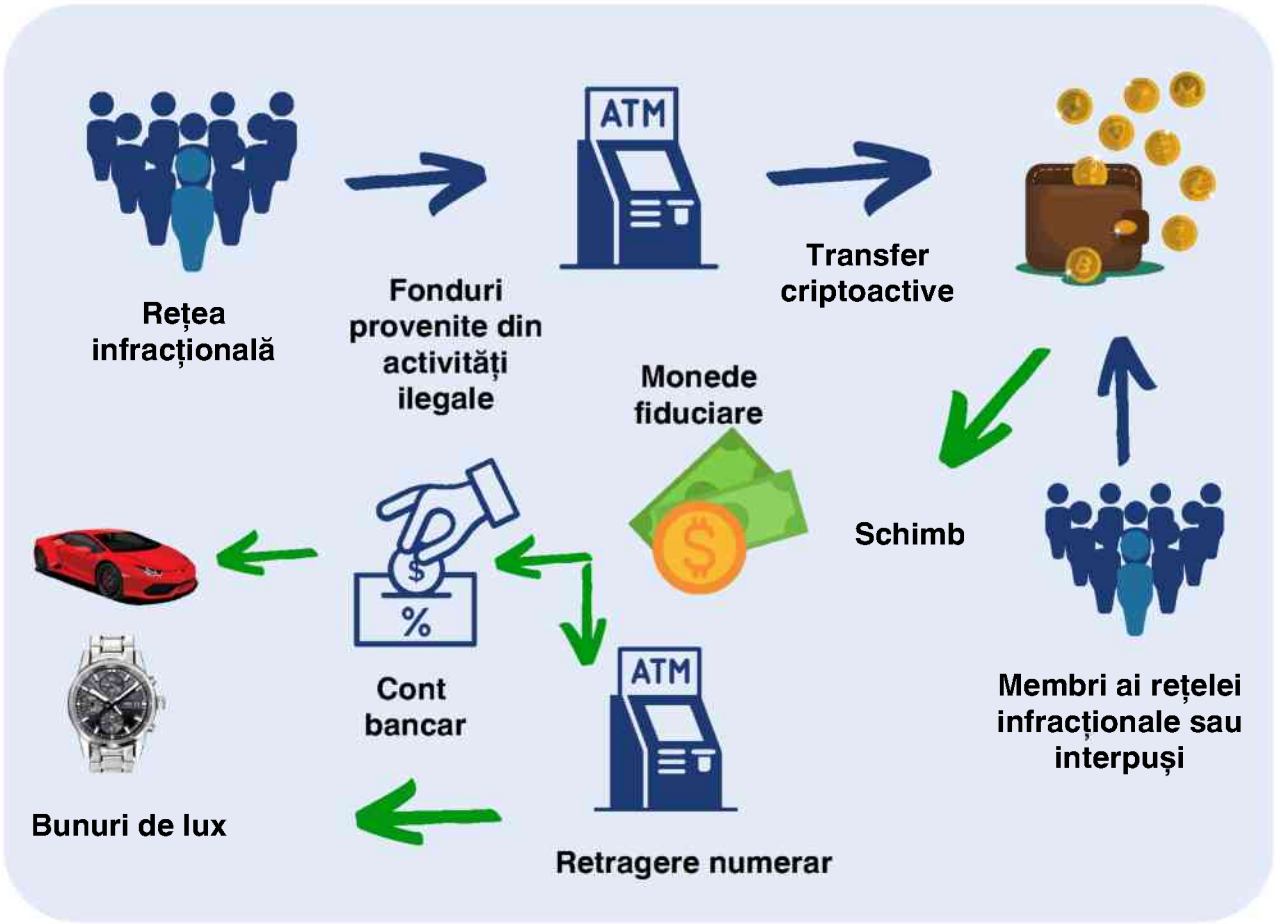
- **Efectuarea tranzacțiilor cu sume mai mici și foarte apropiate de pragurile de raportare** stabilite de autoritățile financiare poate ridica suspiciuni în ceea ce privește intenția de a evita obligațiile de raportare și de a ascunde activitățile financiare;

- **Folosirea ATM-urilor de cripto în scopul transferului de criptomonede** către platforme neautorizate sau neconforme din jurisdicții cu reguli slabe în ceea ce privește identificarea clientelei**.**

## Exemple Concrete

1. Un grup infracțional utilizează ATM-uri de cripto amplasate în țări cu reglementări slabe pentru a converti sume mari de bani obținute din traficul de droguri în criptomonede. Acest lucru indică o strategie adoptată de infractori pentru a ascunde și spăla fondurile provenite din activități ilegale, prin exploatarea lacunelor din reglementările și practicile de supraveghere a acestor țări [21].

2. Un individ efectuează tranzacții repetate de vânzare-cumpărare folosind ATM-uri de cripto. Acesta adoptă o strategie prin care fragmentează și dispersează fondurile în diferite tipuri de criptomonede, încercând astfel să îngreuneze urmărirea și investigarea tranzacțiilor sale [22].




[21] Elliptic Typologies Report 2022 Edition, Preventing Financial Crime in Cryptoassets
[22] Financial Action Task Force (FATF) - Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html

## 5. Utilizarea NFT-urilor în scopul spălării banilor

NFT-urile au câștigat popularitate în ultima perioadă, reprezentând proprietatea asupra unui bun digital unic, cum ar fi o operă de artă digitală sau un joc video. Potrivit definiției dată de Clifford Change, NFT-urile sunt token-uri digitale create pe baza tehnologiei blockchain, care conferă proprietarului dreptul de a deține și tranzacționa un obiect digital unic și nedivizibil.

Cu toate acestea, o consecință nedorită a popularității NFT-urilor este utilizarea lor în scopul spălării banilor. Această creștere a utilizării NFT-urilor ridică îngrijorări semnificative în privința integrității și legalității tranzacțiilor efectuate cu acestea. Deoarece NFT-urile permit tokenizarea unor active digitale unice și chiar a unor active fizice, există riscul ca aceste tranzacții să fie folosite pentru a ascunde sau a spăla fonduri provenite din activități ilegale. Deoarece NFT-urile sunt tranzacționate online și înregistrate pe blockchain, aparenta transparență este prezentă. Totuși, datorită caracterului unic și nedivizibil al NFT-urilor, identificarea părților implicate și urmărirea originii fondurilor devin dificile.

### Descrierea tipologiei

Spălarea banilor folosind NFT-urile poate implica mai multe tipuri de scheme și strategii. Iată câteva exemple ale tipologiei de spălare de bani care pot fi asociate cu NFT-urile:

- **Crearea și tranzacționarea NFT-urilor fictive:** în această schemă, infractorii creează NFT-uri false sau fictive și le tranzacționează între conturile lor sau cu complicitatea unor părți terțe. Scopul este de a crea aparența unor tranzacții legitime și de a spăla fondurile provenite din activități ilegale prin intermediul acestor NFT-uri;

- **Utilizarea NFT-urilor reale, dar achiziționate cu fonduri obținute ilegal:** în această strategie, infractorii utilizează fondurile obținute din activități ilegale pentru a achiziționa NFT-uri reale. Aceste NFT-uri pot fi tranzacționate ulterior pe piețele NFT legale, legitimând aparent originea fondurilor. În acest mod, infractorii încearcă să ascundă tranzacțiile ilegale și să obțină profituri "curate" prin intermediul NFT-urilor;

- **Utilizarea NFT-urilor pentru transferuri de valoare:** o altă strategie de spălare a banilor prin NFT-uri implică utilizarea acestora pentru transferuri de valoare între diferite entități sau adrese de criptomonede. Infractorii pot achiziționa NFT-uri și le pot transfera între conturile lor sau către un complice pentru a ascunde fluxurile de bani și a îngreuna urmărirea tranzacțiilor;

- **Spălarea banilor prin intermediul artei digitale:** o tactică din ce în ce mai frecventă este aceea de a asocia NFT cu arta digitală. Infractorii pot crea sau achiziționa opere de artă digitală şi le pot transforma în NFT-uri, dându-le o aparență de unicitate şi valoare. Aceste NFT pot fi apoi tranzacționate pe platforme NFT, iar banii din aceste tranzacții pot fi considerați "curați". Astfel, infractorii pot folosi arta digitală și NFT-urile ca instrumente de spălare a banilor.

Acestea sunt doar câteva exemple ale tipologiei de spălare de bani care pot fi asociate cu NFT-urile. Este important de menționat că aceste activități pot varia în complexitate și pot implica tehnici și strategii suplimentare pentru a ascunde tranzacțiile ilegale și a îngreuna urmărirea lor de către autorități.

**Indicatori specifici**

- **Tranzacțiile cu NFT-uri la prețuri extrem de ridicate** pot sugera spălarea banilor, mascând adevăratul scop al acestor operațiuni;

- **Transferurile frecvente de NFT-uri între adrese anonime** pot indica încercări deliberate de a ascunde tranzacțiile și de a evita detectarea activităților ilegale.

- **Utilizarea platformelor de schimb neconforme pentru tranzacționarea NFT-urilor** poate indica o activitate ilegală și un mediu propice pentru spălarea banilor, deoarece aceste platforme pot oferi un grad mai mare de anonimat și o aplicare mai slabă sau inexistentă a măsurilor de conformitate;

- **Crearea de NFT-uri folosind adrese anonime** reprezintă o practică în care token-urile sunt generate și tranzacționate fără a fi asociate cu identități verificabile. Aceasta poate fi realizată prin utilizarea portofelelor digitale anonime sau a altor servicii care permit ascunderea identității utilizatorului;

- **Tranzacțiile cu NFT-uri în jurisdicții cu reglementări slabe** indică desfășurarea activităților în zone cu standarde reduse de conformitate în domeniul criptoactivelor;

- **Utilizarea NFT-urilor ca instrument pentru transferul de valoare** între criptoactive reprezintă o strategie prin care se utilizează NFT-urile pentru a facilita schimbul de active digitale între diferite tipuri de criptomonede sau criptoactive.

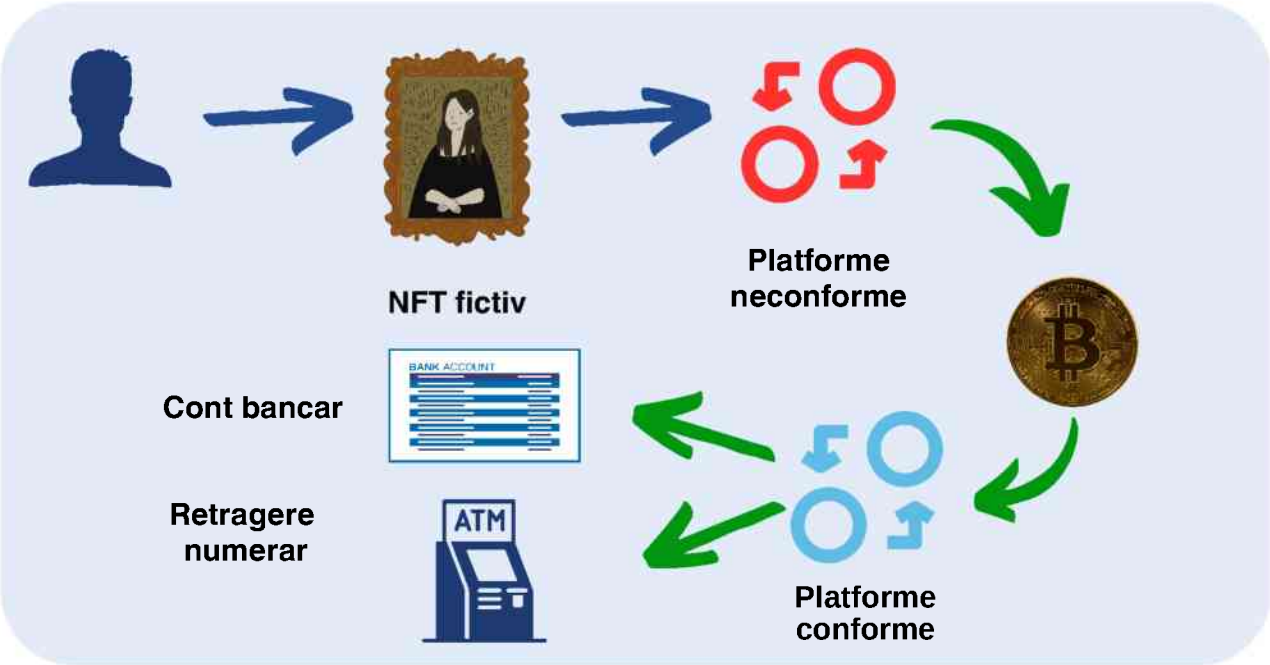
Această utilizare a NFT-urilor poate fi exploatată în scopul spălării banilor, deoarece transferul de valoare prin intermediul NFT-urilor poate complica urmărirea fondurilor și identificarea activităților ilegale.

## Exemple concrete

1. Un individ care deține un NFT dorește să spele o sumă de bani obținută în mod ilegal prin intermediul acestuia. Pentru a face ca NFT-ul să pară mai valoros decât este în realitate, individul creează mai multe adrese anonime în portofelul său digital. El efectuează apoi tranzacții fictive între aceste adrese, încheind cumpărări și vânzări false ale NFT-ului la prețuri exorbitante [23].

Prin aceste tranzacții trucate, individul reușește să creeze aparența unei cereri mari și a unui interes ridicat pentru NFT-ul său. Astfel, poate atrage atenția cumpărătorilor legitimi și să vândă NFT-ul la un preț mai mare. Suma obținută din această tranzacție este acum considerată "curată" și poate fi utilizată în mod legal, ascunzând astfel originea ilicită a fondurilor;

2. Un grup infracțional utilizează Bitcoin și NFT-uri pentru a spăla banii obținuți în mod ilegal. Datorită anonimatului oferit de blockchain, tranzacțiile cu Bitcoin sunt confidențiale și nu dezvăluie informații despre cumpărători și vânzători. Aceasta permite infractorilor să achiziționeze artă digitală sau alte active folosind fonduri obținute în mod ilegal fără a atrage atenția autorităților. Tranzacțiile cu Bitcoin sunt imutabile, ceea ce înseamnă că nu pot fi rambursate sau anulate, iar originea fondurilor rămâne necunoscută. Astfel, prin utilizarea NFT-urilor, infractorii pot ascunde proveniența ilicită a banilor și să-i legitimizeze prin intermediul tranzacțiilor aparent legale cu active digitale [24].




[23]Chainalysis 2022 Crypto Crime Report, https://go.chainalysis.com/2022-Crypto-Crime-Report.html;
[24] NFT money laundering and AML compliance, https://withpersona.com/blog/nfts-and-compliance-what-to-know-about-this-crypto-era-commodity.

## 6. Utilizarea ICO-urilor în scopul spălării banilor

ICO-urile (Initial Coin Offerings - Ofertă Inițială de Monede) reprezintă o metodă populară de finanțare în domeniul criptomonedelor, prin care se emite o nouă monedă digitală sau un token în schimbul investițiilor în proiecte. Cu toate acestea, utilizarea ICO-urilor poate fi susceptibilă la abuzuri și utilizare necorespunzătoare în scopul spălării banilor.

Utilizarea ICO-urilor în scopul spălării banilor reprezintă o preocupare majoră pentru autoritățile de reglementare financiară. Această practică abuzivă implică transformarea fondurilor provenite din activități ilegale în monede digitale prin intermediul ICO-urilor, cu scopul de a le integra în economia legală și de a le ascunde originea ilicită. Astfel, ICO-urile devin un instrument atractiv pentru spălarea banilor, datorită caracteristicilor lor specifice. Este important să subliniem că spălarea banilor prin intermediul ICO-urilor nu este o practică generalizată, însă este esențial să identificăm și să înțelegem riscurile asociate acestei tipologii pentru a dezvolta măsuri și soluții eficiente de combatere a acestui fenomen.

### Descrierea tipologiei

**1. Anonimatul:** ICO-urile oferă un grad ridicat de anonimat, deoarece participanții nu sunt obligați să dezvăluie identitatea lor completă în timpul procesului de investiție. Acest lucru face ca identificarea și urmărirea tranzacțiilor să devină mai dificile, permițând spălarea banilor prin intermediul ICO-urilor;

**2. Utilizarea altor criptomonede:** unele ICO-uri permit investitorilor să achiziționeze token-uri folosind alte criptomonede în loc de monedele tradiționale. Acest aspect oferă oportunitatea spălării banilor prin intermediul ICO-urilor, deoarece fondurile provenite din activități ilegale pot fi mai întâi convertite într-o altă criptomonedă, apoi utilizate pentru a cumpăra token-uri în cadrul ICO-urilor;

**3. Complexitatea structurilor ICO:** unele ICO-uri pot avea structuri complexe și mecanisme avansate, care pot fi folosite în mod intenționat pentru a ascunde originea fondurilor și a crea un proces de spălare a banilor mai dificil de urmărit. Aceste structuri pot implica utilizarea mai multor etape de finanțare, intermediari sau adrese de criptomonede multiple pentru a complica investigațiile ulterioare;

**4. Jurisdicții cu reglementări slabe:** ICO-urile pot beneficia de jurisdicții cu reglementări slabe sau inexistente în ceea ce privește combaterea spălării banilor. Aceste jurisdicții oferă un mediu propice pentru desfășurarea ICO-urilor în scopul spălării banilor, deoarece există mai puține restricții și controale legale care să prevină și să detecteze aceste activități ilicite;

**5. Utilizarea fondurilor în afara proiectelor ICO:** unele ICO-uri pot fi utilizate în mod fraudulos, în sensul că fondurile strânse nu sunt folosite în mod corespunzător pentru dezvoltarea proiectului propus. În schimb, aceste fonduri pot fi direcționate în conturile personale ale emitenților sau în alte investiții speculative, contribuind astfel la spălarea banilor.

Este important de menționat faptul că descrierea tipologiei nu acoperă toate aspectele legate de utilizarea ICO-urilor în scopul spălării banilor, deoarece aceste practici pot varia în funcție de circumstanțe și strategii specifice utilizate de infractori.

## Indicatori specifici

- **Volume mari de fonduri:** utilizarea ICO-urilor în scopul spălării banilor poate implica investiții semnificative, deoarece sumele mari de bani pot fi fragmentate și ascunse în spatele token-urilor emise în cadrul evenimentului. Prin împărțirea sumelor mari în tranșe mici și distribuirea acestora în diferite proiecte ICO, spălătorii de bani pot obține token-uri digitale în schimbul banilor lor, ceea ce le permite să profite de potențialul de creștere al acestor active digitale și să obțină fonduri aparent legitime;

- **Utilizarea unor platforme de schimb neautorizate sau neconforme:** spălătorii de bani pot alege să desfășoare ICO-uri pe platforme neautorizate sau neconforme sau în jurisdicții cu reguli slabe în ceea ce privește identificarea clientelei, pentru a evita supravegherea și verificările riguroase ale autorităților;

- **Utilizarea mixării fondurilor:** spălătorii de bani pot utiliza tehnici avansate de mixare a fondurilor pentru a îngreuna urmărirea tranzacțiilor realizate în cadrul ICO-urilor și pentru a ascunde legăturile dintre adresele de criptomonede implicate. Această tactică implică amestecarea și transferul de fonduri prin mai multe adrese de criptomonede, în încercarea de a crea o rețea complexă de tranzacții care este dificil de urmărit;

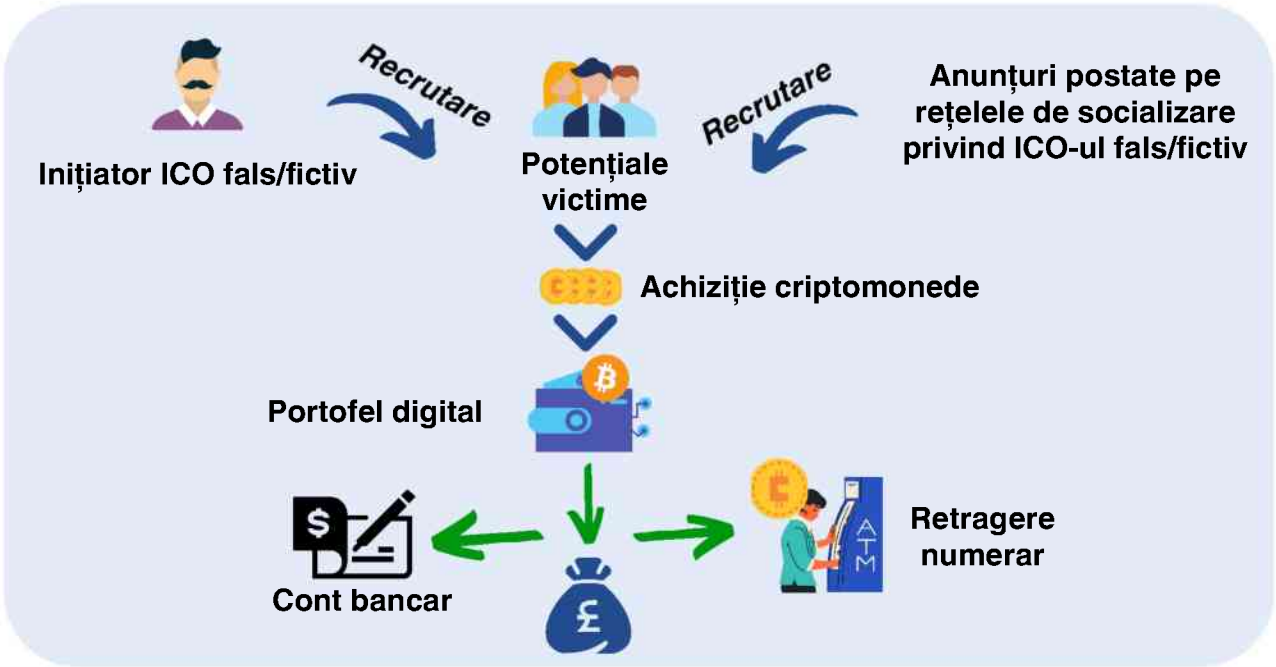
- **Implicarea multiplelor jurisdicții:** utilizarea ICO-urilor în scopul spălării banilor poate implica operațiuni desfășurate în diferite jurisdicții, ceea ce complică cooperarea între autorități și investigarea activităților ilegale. Spălătorii de bani pot profita de natura transfrontalieră a criptomonedelor și a ICO-urilor pentru a transfera fonduri între diferite țări și jurisdicții cu reguli diferite privind criptomonedele și spălarea banilor;

- **Complexitatea tranzacțiilor:** utilizarea ICO-urilor în scopul spălării banilor implică adesea transferuri de fonduri între adrese de criptomonede anonime, utilizând tehnici avansate de criptografie și protocoale blockchain complexe. Această complexitate a tranzacțiilor face dificilă urmărirea fluxurilor de bani și identificarea originii acestora.

## Exemple concrete

1. Utilizarea unor platforme neautorizate sau neconforme: în perioada 2017-2020, Comisia pentru Bursă și Valori Mobiliare a SUA (SEC) a emis avertismente și a intentat acțiuni legale împotriva mai multor ICO-uri care au fost identificate ca fiind neautorizate și care nu respectau reglementările privind valorile mobiliare. Aceste acțiuni legale au vizat încercările de spălare a banilor prin intermediul ICO-urilor și au avut ca rezultat sancțiuni financiare și interdicții. SEC a intentat acuzații împotriva lui Dominic Lacroix și companiei sale, PlexCorps, pentru că au promovat și vândut valori mobiliare numite PlexCoin pe internet către investitori din SUA și din alte țări. Aceștia au făcut afirmații false, susținând că investițiile în PlexCoin ar aduce un profit de 1.354% în mai puțin de 29 de zile [25].

2. Utilizarea mixării fondurilor în cadrul ICO-urilor poate fi exemplificată prin proiectul platformei de criptomonede Monero. În cadrul procesului ICO, Monero a implementat tehnici avansate de mixare a fondurilor pentru a îmbunătăți nivelul de confidențialitate al tranzacțiilor. Acest lucru a fost realizat prin utilizarea unui protocol special denumit "Ring Confidential Transactions". Acest protocol grupează tranzacțiile într-un "inel" de semnături digitale, ceea ce face dificilă identificarea originii tranzacțiilor. Această practică a atras atât investitorii preocupați de confidențialitate, cât și indivizi cu intenții ilegale, care au văzut în Monero o modalitate de spălare a banilor. Amestecul de fonduri a sporit opacitatea și a îngreunat investigarea tranzacțiilor suspecte de către autorități [26].




[25] Comisia pentru Bursă și Valori Mobiliare a SUA, SEC Emergency Action Halts ICO Scam, https://www.sec.gov/news/press-release/2017-219;;
[26] Virtual Asset Red Flag Indicators of Money Laundering and Terrorist Financing, https://ciphertrace.com/virtual-asset-red-flag-indicators-of-money-laundering

## 4.1. Finanțarea terorismului: magnitudine și natură

Finanțarea terorismului reprezintă o amenințare globală la adresa securității, care necesită o abordare coordonată și concertată din partea autorităților naționale și internaționale. În acest context, furnizorii de servicii de active virtuale devin din ce în ce mai vizibili pentru entitățile teroriste datorită caracteristicilor specifice criptomonedelor, care facilitează transferuri financiare rapide și evitarea controlului autorităților. Deși utilizarea criptomonedelor de către organizațiile teroriste reprezintă o mică parte din tranzacțiile ilicite din ecosistemul criptografic, rămâne o preocupare constantă. Gravitatea oricăror fonduri care contribuie la terorism, indiferent de sumă, necesită o atenție maximă din partea sectorului public și privat.

Potrivit Strategiei Naționale de Apărare pentru perioada, 2020-2024, în România, fenomenul terorist își menține caracterul conjunctural, fiind dependent de evoluțiile din spațiul extern. Exprimându-se indirect, prin asocierea cu NATO, UE, SUA și statele europene implicate activ în combaterea terorismului, România rămâne o țintă de oportunitate pentru organizațiile teroriste. Acțiunile informaționale ostile radical islamiste continuă să fie principalul factor de alimentare a proceselor de (auto)radicalizare, care constituie unul dintre riscurile securitare semnificative în România, deși fără a atinge o anvergură de fenomen.

Strategia Națională de Apărare 2020-2024 subliniază tendințe majore cu potențial de afectare și influențare a mediului de securitate, inclusiv criptomonedele, tehnologia blockchain, inteligența artificială, machine learning, Internet of Things, big data și tehnologia cuantică, care pot fi utilizate în planul criminalității organizate, infracționalității cibernetice, activităților de profil hacktivist, terorist sau extremist, precum și în operațiunile ofensive coordonate de entități care susțin interesele unor actori statali. Riscurile adaptării acțiunilor ofensive cu caracter hibrid la evoluțiile tehnologice se profilează printr-o diversificare continuă a modalităților de acțiune și a resurselor coordonate, având ca scop afectarea intereselor naționale, inclusiv cele de securitate.

## Ce este infracțiunea de finanțare a terorismului?

*„Colectarea sau punerea la dispoziție, direct ori indirect, de fonduri, licite sau ilicite, cu intenția de a fi folosite sau cunoscând că acestea urmează a fi folosite, în tot ori în parte, pentru săvârşirea actelor de terorism sau pentru susținerea unei entități teroriste şi se pedepseşte cu închisoare de la 5 la 12 ani şi interzicerea unor drepturi [27]*

Legislația națională a creat cadrul necesar pentru derularea de consultări interinstituționale, facilitând schimbul adecvat de informații și analiza integrată a riscurilor în domeniul de competență. Entitățile raportoare, implicit furnizorii de servicii de schimb între monede virtuale și monede fiduciare, precum și furnizorii de portofele digitale, au obligația de a transmite Oficiului Național de Prevenire și Combatere a Spălării Banilor un raport privind tranzacțiile suspecte, dacă au cunoștință, suspectează sau au motive întemeiate să suspecteze activități de finanțare a terorismului. Capacitatea acestora de a identifica operațiunile de finanțare a terorismului este esențială pentru documentarea activităților ilicite.

ONPCSB analizează și prelucrează informațiile primite, iar în cazul în care există indicii de finanțare a terorismului, informează de îndată autoritățile competente în materie.

Orientările FATF [28] recomandă adoptarea unui cadru robust de reglementare pentru VASP-uri, care să includă obligația de a raporta tranzacțiile suspecte și de a respecta cerințele de cunoaștere a clientului. Acest lucru este important pentru a preveni utilizarea criptomonedelor în activități de finanțare a terorismului.

De precizat faptul că în perioada supusă evaluării, nu au fost primite de ONPCSB rapoarte de tranzacții suspecte legate de activități de finanțare a terorismului.

Implementarea noului cadru juridic european va stabili cerințe clare pentru autorizarea și supravegherea VASP-urilor, aliniind legislația națională la standardele internaționale și contribuind la reducerea riscurilor legate de finanțarea terorismului.

[27] Legea nr. 535/2004 privind prevenirea și combaterea terorismului
[28] FATF (June 2021) Guidance On Proliferation Financing Risk Assessment And Mitigation

Criptomonedele, fundamentul principal al serviciilor oferite de VASP-uri, au caracteristici care le fac atractive pentru activități ilicite, inclusiv pentru finanțarea terorismului. Anonimitatea relativă a tranzacțiilor, complică identificarea utilizatorilor, oferind actorilor rău intenționați posibilitatea de a masca fondurile utilizate pentru acțiuni teroriste. Transferurile transfrontaliere rapide reduc substanțial capacitatea autorităților de a controla fluxurile financiare internaționale. Această lipsă de reglementare globală uniformă permite teroriștilor să exploateze lacunele legislative dintre state, utilizând VASP-uri din jurisdicții mai puțin reglementate.

Din anul 2020, în România folosește un sistem de alertă teroristă bazat pe patru niveluri: Scăzut, Precaut, Ridicat și Critic [29]. În prezent, nivelul de alertă este "Precaut", ceea ce sugerează un risc scăzut de atac terorist, dar cu o monitorizare constantă a potențialelor amenințări. Conform Strategiei Naționale de Apărare 2020-2024 și Sistemului Național de Alertă Teroristă (SNPCT), România nu se confruntă cu o amenințare teroristă semnificativă, nefiind identificate organizații teroriste active pe teritoriul său. Cu toate acestea, riscul latent al utilizării criptomonedelor pentru finanțarea terorismului poate crește pe măsură ce aceste active digitale devin tot mai răspândite.

Raportul Chainalysis din anul 2024 evidențiază faptul că organizațiile teroriste, precum Hezbollah, au demonstrat capacitatea de a utiliza criptomonede pentru a-și extinde rețelele financiare tradiționale. În iunie 2023, un exemplu concret a fost sechestrarea a aproximativ 1,7 milioane de dolari în criptomonede, legate de Hezbollah, prin intermediul unui operator hawala. Această situație ilustrează complexitatea infrastructurii de finanțare a terorismului, care se bazează adesea pe intermediari care facilitează transferuri de fonduri, făcând dificilă estimarea activităților legate de terorism.

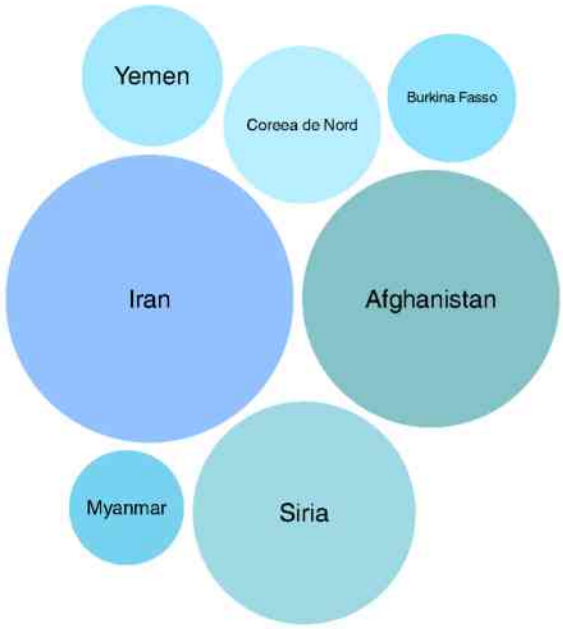
Sectorul VASP din România este în fază de dezvoltare, iar în prezent nu este supus unui regim de autorizare specific. Cu toate acestea, acest lucru se va schimba odată cu implementarea Regulamentului MiCA (Markets in Crypto-Assets), care va introduce un cadru clar de autorizare și supraveghere pentru furnizorii de servicii de active virtuale. Deși, nu au fost raportate cazuri de finanțare a terorismului prin intermediul VASP-urilor din România, riscurile asociate vor crește pe măsură ce criptomonedele devin mai populare.

Migrația și expunerea transfrontalieră reprezintă alte vulnerabilități. România, situată pe o rută secundară de tranzit pentru migranți din Orientul Mijlociu, Africa de Nord și Asia de Sud, poate crea o vulnerabilitate indirectă. În plus, tranzacțiile efectuate de VASP-urile din România către jurisdicții terțe cu risc ridicat necesită o supraveghere sporită, având în vedere expansiunea rapidă a sectorului la nivel international, deși din datele și informațiile

[29] https://www.sri.ro/sistemul-national-de-alerta-terorista

colectate nu au fost identificate legături cu astfel de jurisdicții.

Volumul tranzacțiilor legate de sancțiuni reprezintă o parte tot mai mare din totalul tranzacțiilor ilicite, în parte din cauza creșterii numărului de entități sancționate, dar și din cauza dificultății de a aplica sancțiuni împotriva entităților din anumite regiuni sau a operațiunilor descentralizate. Raportul Chainalysis din 2024 a menționat că fluxurile de criptomonede către entități și jurisdicții sancționate au reprezentat 61,5% din volumul total al tranzacțiilor ilicite în 2023 [30].




**Principalele jurisdicții considerate cu risc ridicat de către VASP-uri în ceea ce privește finanțarea terorismului**

Din informațiile colectate prin intermediul chestionarelor, a rezultat că 80% dintre entități efectuează verificări pe listele de sancțiuni internaționale pentru a evalua riscurile asociate jurisdicțiilor clienților lor în contextul finanțării terorismului (FT), ceea ce demonstrează o atenție sporită în gestionarea riscurilor legate de clienți și jurisdicții sancționate.

Totodată, un singur VASP a raportat că a identificat cazuri în care, înainte de inițierea unei relații de afaceri sau în timpul monitorizării unui client existent, au descoperit clienți care figurau pe listele de sancțiuni internaționale.

În acest caz, verificările efectuate prin platforme specializate, cum ar fi Ondato și Google, au condus la refuzul deschiderii relațiilor de afaceri, demonstrând eficiența măsurilor de prevenire a expunerii la riscurile de FT. Aceste măsuri contribuie la alinierea la cerințele internaționale și la reducerea riscului de implicare în activități ilicite.

În concluzie, riscurile de finanțare a terorismului în sectorul VASP din România sunt scăzute în acest moment, dar acest lucru se datorează stadiului incipient de dezvoltare a sectorului și nivelului scăzut de amenințare teroristă pe plan național. Cu toate acestea, caracteristicile inerente ale criptomonedelor – anonimitatea, viteza transferurilor și lipsa unei reglementări uniforme – continuă să reprezinte factori de risc semnificativi. Autoritățile române trebuie să implementeze reglementări suplimentare, să întărească supravegherea

[30] Chainalysis Crypto Crime Report 2024

și să mențină o colaborare internațională strânsă, adoptând o atitudine proactivă și măsuri preventive eficiente pentru a preveni utilizarea sectorului în scopuri teroriste, adaptându-se astfel la noile provocări ale tehnologiilor financiare inovative și contribuind la combaterea globală a finanțării terorismului.

## 4.3. Analiza vulnerabilităților în asociere cu alte sectoare economice

Sectorul VASP în România prezintă o serie de vulnerabilități semnificative, amplificate de interacțiunile sale cu diverse sectoare economice. Relațiile acestuia cu alte domenii creează riscuri semnificative din perspectiva prevenirii spălării banilor și finanțării terorismului, în special în contextul în care multe dintre aceste sectoare sunt deja identificate ca fiind de risc ridicat în cadrul Evaluării Naționale a Riscurilor din 2022. Aceste vulnerabilități provin din lipsa unor reglementări adecvate pentru criptoactive și din dificultatea supravegherii tranzacțiilor anonime și rapide facilitate de aceste active.

Vulnerabilitățile sectorului VASP sunt determinate de mai mulți factori care includ structura pieței, specificul proprietății, produse și activități, geografie, clienți și tranzacții și canale. Analiza vulnerabilității sectorului criptoactivelor este complexă și poate fi realizată luând în considerare interacțiunile și dependențele acestuia cu alte sectoare economice.

În cazul sectorului bancar, acesta este este unul dintre cele mai reglementate domenii, cu măsuri stricte de cunoaștere a clientelei (KYC) și raportare a tranzacțiilor suspecte (RTS). Cu toate acestea, interacțiunea cu criptoactivele ar putea aduce provocări semnificative, având în vedere anonimitatea tranzacțiilor și dificultatea în identificarea beneficiilor reali ai tranzacțiilor cu criptoactive. Transformarea criptomonedelor în monedă fiat prin intermediul conturilor bancare reprezintă un risc considerabil, având în vedere potențialul ca fonduri ilicite să fie integrate în sistemul financiar tradițional. Deși băncile sunt reglementate strict, creșterea utilizării criptoactivelor impune o îmbunătățire a mecanismelor de supraveghere și cooperare cu VASP-urile pentru a preveni eventualele abuzuri.

Comerțul electronic este un alt sector unde interacțiunea cu criptoactivele adaugă un nou nivel de risc. Tranzacțiile online sunt rapide, anonime și dificil de monitorizat, ceea ce le face un vehicul ideal pentru spălarea banilor. În plus, platformele de comerț electronic pot fi folosite pentru a masca fonduri de proveniență ilicită, în special atunci când criptomonedele sunt acceptate fără verificări adecvate. Această anonimitate face supravegherea și aplicarea măsurilor de prevenire a spălării banilor extrem de dificile.

Rezultatele Evaluării Naționale a Riscurilor (2022) subliniază, de asemenea, vulnerabilitatea sectorului VASP în asocierea cu alte sectoare economice cu risc ridicat, cum ar fi imobiliarele, jocurile de noroc și consultanța în afaceri. Aceste sectoare prezintă

deja riscuri semnificative în ceea ce privește spălarea banilor, iar integrarea criptoactivelor în aceste domenii nu face decât să crească nivelul de expunere la activități ilicite.

Sectorul VASP în asociere cu sectorul imobiliar este un subiect complex, având în vedere interconexiunile din economie și natura volatilă a ambelor piețe. Aspectele fundamentale care pot fi considerate în cadrul acestei analize constau în volatilitatea criptoactivelor prin fluctuațiile rapide ale prețurilor care pot afecta stabilitatea financiară a persoanelor care investesc în imobiliare folosind criptomonede și care poate duce la pierderi semnificative, influențând astfel deciziile de investiție în sectorul imobiliar. Criptoactivele oferă o lichiditate mai mare în comparație cu sectorul imobiliar traditional, astfel că o scădere abruptă a valorii criptoactivelor poate duce la imposibilitatea investitorilor de a valorifica investițiile imobiliare, iar absența unor reglementări clare și a unui cadru legal solid poate introduce riscuri semnificative pentru investitorii imobiliari care folosesc criptoactive, investițiile în criptoactive având tendințe susceptibile la atacuri cibernetice. Dacă un investitor ar pierde accesul la wallet-ul său de criptomonede din cauza unui hack, aceasta ar putea afecta capacitatea sa de a achiziționa sau de a vinde proprietăți imobiliare. De asemenea, platformele imobiliare care acceptă plăți în criptomonede pot fi ținte pentru atacuri, punând în pericol fondurile utilizatorilor. Sintetizând, sectorul criptoactivelor poate prezenta oportunități pentru diversificarea și inovarea în investițiile imobiliare, dar vine și cu o serie de riscuri semnificative. Investitorii ar trebui să fie conștienți de volatilitatea pieței criptoactivelor, reglementările informației și riscurile cibernetice, precum și de impactul pe care aceste active îl pot avea asupra investițiilor imobiliare.

Analiza vulnerabilității sectorului criptoactivelor în asociere cu sectorul jocurilor de noroc este un subiect vast, având în vedere creșterea popularității criptomonedelor și a platformelor de jocuri de noroc online. Din cauza volatilității mari a criptoactivelor, jucătorii s-ar putea confrunta cu pierderi semnificative rapid, iar operatorii de jocuri de noroc ar putea avea dificultăți în gestionarea riscurilor financiare. De asemenea, criptoactivele permit anonimitate, ceea ce poate facilita spălarea de bani și alte activități ilicite, iar sectorul jocurilor de noroc, în special cel online, poate fi utilizat pentru a spăla fonduri obținute din surse ilegale. Concluzia este că sectorul criptoactivelor, în asociere cu sectorul jocurilor de noroc, prezintă vulnerabilități semnificative care necesită o atenție sporită atât din partea reglementatorilor, cât și a utilizatorilor. Corelarea riscurilor financiare, legale și de securitate este foarte importantă pentru a asigura un mediu mai sigur și mai stabil pentru toți participanții. Este esențial să existe un cadru legislativ clar și să se investească în educația utilizatorilor pentru care tranzacționează în acest domeniu.

Legătura dintre sectorul VASP și cel al serviciilor oferite de profesioniștii în consultanță managerială și de afaceri este remarcabilă, având în vedere că cele două domenii se influențează reciproc pe diverse niveluri. Totuși, aceste activități pot amplifica riscurile dacă recomandările nu sunt aliniate corect cu cerințele legale. Pe măsură ce criptoactivele sunt integrate în strategii financiare tradiționale, pot apărea riscuri de neconformitate, în special în lipsa unor ghiduri clare privind utilizarea criptoactivelor în consultanță. Consultanții pot aduce perspective valoroase privind colaborarea eficientă între aceste două sfere și pot sugera metode de integrare a criptoactivelor în strategiile financiare deja existente. Vulnerabilitatea sectorului, în interacțiunea cu serviciile de consultanță managerială și de afaceri, este o problemă multipartită care implică reglementări, securitate, volatilitate, transparență și etică. Abordările proactive din partea consultanților pot ajuta atât investitorii, cât și companiile să navigheze aceste provocări, reducând riscurile și maximizând oportunitățile în acest sector în continuă evoluție.

În concluzie, sectorul criptoactivelor prezintă un grad ridicat de vulnerabilitate din cauza interconectivității cu alte domenii economice, a reglementărilor în continuă evoluție, a volatilității și a riscurilor tehnologice. Este esențial ca investitorii, autoritățile de reglementare și celelalte părți implicate să fie conștienți de aceste riscuri, să colaboreze pentru a asigura o integrare adecvată a criptoactivelor în economia globală și să adopte măsuri eficiente pentru a le gestiona.


# Gestionarea Riscurilor

## 5.1. Măsuri de prevenire și atenuare a riscurilor

Măsurile de prevenire și atenuare a riscurilor în sectorul VASP trebuie să fie integrate și bine structurate, pentru a răspunde eficient provocărilor și vulnerabilităților identificate. Aceste măsuri trebuie să fie adaptate specificităților acestui sector, ținând cont de caracteristicile tranzacțiilor anonime, de rapiditatea și de natura globală a pieței activelor virtuale, precum și de gradul ridicat de expunere la riscuri de spălare a banilor și finanțare a terorismului.

Primul pas esențial pentru prevenirea riscurilor în acest sector este elaborarea și implementarea unor politici la nivel național care sunt clare și eficiente. Aceste politici trebuie să fie coordonate între autoritățile implicate în sectorul VASP și să sprijine dezvoltarea unui cadru legislativ și de reglementare solid. Implementarea noului cadru juridic european va aduce mai multă claritate și va asigura conformitatea cu standardele internaționale, în special în ceea ce privește prevenirea spălării banilor și finanțării terorismului.

Odată cu introducerea reglementărilor privind autorizarea VASP-urilor la nivel național, se va crea un mecanism formal de supraveghere și control. Acest proces va include cerințe stricte de autorizare și înregistrare pentru furnizorii de servicii de active virtuale, stabilind reguli clare pentru conformitatea cu cerințele SB/FT. Aceasta va permite monitorizarea continuă a activităților și va îmbunătăți capacitatea autorităților de a identifica și a combate riscurile asociate, prevenind utilizarea activelor virtuale în scopuri ilicite. Regulamentul MiCA asigură că toate entitățile care oferă servicii de criptoactive în Uniunea Europeană vor fi supuse unui proces de autorizare uniform, crescând astfel transparența și responsabilitatea sectorului.

În plus, colaborarea internațională este un element cheie, facilitând schimbul de informații și de bune practici între statele membre ale Uniunii Europene, în special în domeniul schimbului de date privind tranzacțiile cu active virtuale și activitățile suspecte.

Pentru a asigura o prevenire eficientă a riscurilor, VASP-urile trebuie să aplice măsuri stricte de cunoaștere a clientelei (KYC) și de due diligence extins, în special în cazul tranzacțiilor care implică jurisdicții cu risc ridicat sau care sunt de mare valoare. Verificarea identității clienților și monitorizarea activităților acestora sunt esențiale pentru a preveni utilizarea activelor virtuale în scopuri ilicite. Monitorizarea continuă a tranzacțiilor, utilizând tehnologii avansate precum blockchain, va permite detectarea automată a activităților suspecte și va facilita prevenirea și combaterea activităților ilegale. Implementarea cerințelor "travel rule", care impun transmiterea de informații despre clienți în tranzacțiile transfrontaliere, este un element central pentru prevenirea riscurilor. În plus, operatorii platformelor de tranzacționare pentru criptoactive trebuie să elaboreze și să pună în aplicare mecanisme eficiente de gestionare a riscurilor și să instituie controale interne riguroase pentru a preveni activitățile frauduloase.

Supravegherea operativă și aplicarea legii sunt esențiale pentru prevenirea riscurilor. Autoritățile de aplicare a legii trebuie să colaboreze strâns cu autoritățile de supraveghere și alte autorități implicate, pentru a răspunde rapid la activitățile suspecte din sector. VASP-urile ar trebui să implementeze sisteme tehnologice avansate pentru monitorizarea continuă a tranzacțiilor și pentru detectarea automată a activităților suspecte sau cu risc ridicat. În acest context, ar trebui să se intensifice controalele on-site, la sediile VASP-urilor, pentru a verifica conformitatea acestora cu cerințele legale. Aceste măsuri vor asigura o supraveghere constantă și eficientă a sectorului.

În concluzie, aplicarea unei abordări bazate pe risc și consolidarea măsurilor de prevenire și atenuare a riscurilor sunt elemente centrale în gestionarea sectorului VASP, așa cum sunt reglementate în noul cadru juridic european, completând astfel măsurile de supraveghere stabilite la nivel național. Modificarea cadrului juridic național și adoptarea

unor măsuri pentru implementarea noului cadru juridic european reprezintă un element cheie în prevenirea și atenuarea riscurilor în sectorul activelor virtuale. Aceste măsuri vor permite alinierea reglementărilor naționale la cerințele europene și internaționale, asigurând o supraveghere mai riguroasă a VASP-urilor și sporind transparența și responsabilitatea în prevenirea spălării banilor și finanțării terorismului.

Aceste măsuri, implementate în mod adecvat și coerent, vor contribui la creșterea încrederii în piața activelor virtuale și la prevenirea utilizării acesteia în scopuri ilicite, consolidând astfel integritatea și transparența pieței.

## 5.2. Strategii de răspuns și management al riscurilor

Strategiile de răspuns și gestionare a riscurilor din sectorul VASP trebuie să fie dinamice, integrate și să țină cont de specificul tranzacțiilor din acest sector. Aceste strategii au drept scop prevenirea riscurilor de spălare a banilor (SB) și finanțare a terorismului (FT) printr-o abordare bazată pe risc și măsuri de răspuns rapide și eficiente, care să asigure conformitatea continuă cu reglementările naționale și internaționale.

Abordarea bazată pe risc (Risk-Based Approach - RBA) reprezintă fundamentul strategiei de răspuns. Supravegherea și controlul entităților din sectorul VASP trebuie realizate pe baza profilului de risc al fiecărei entități și tranzacții. Astfel, entitățile care prezintă un grad ridicat de risc, cum ar fi cele care facilitează anonimitatea utilizatorilor sau desfășoară tranzacții transfrontaliere complexe, ar trebui prioritizate în procesele de supraveghere și control. VASP-urile trebuie să implementeze măsuri extinse de due diligence, în special pentru clienți și tranzacții cu risc ridicat, ceea ce include verificarea detaliată a identității clienților, monitorizarea continuă a tranzacțiilor și colectarea de informații suplimentare despre sursa fondurilor și scopul tranzacțiilor. Această abordare permite alocarea eficientă a resurselor pentru a răspunde rapid la riscurile majore.

În cazul detectării unor tranzacții suspecte sau a unor potențiale breșe de securitate, VASP-urile trebuie să aibă în vigoare planuri de răspuns rapide. Aceste planuri includ măsuri precum blocarea imediată a tranzacțiilor suspecte, investigarea internă a incidentelor și raportarea imediată către autoritățile competente. În plus, strategiile de răspuns trebuie să includă mecanisme de evaluare și remediere a deficiențelor, pentru a preveni repetarea incidentelor și pentru a îmbunătăți conformitatea pe termen lung. Implementarea unor astfel de măsuri rapide este esențială pentru a menține integritatea pieței și pentru a preveni utilizarea activelor virtuale în scopuri ilicite.

Cooperarea cu autoritățile competente în materie este un alt element cheie în gestionarea eficientă a riscurilor din sectorul VASP. Furnizorii de servicii de active virtuale trebuie să colaboreze strâns cu autoritățile pentru a facilita schimbul rapid de informații privind tranzacțiile suspecte și pentru a răspunde prompt la solicitările de date. Această cooperare este esențială pentru aplicarea regulii "travel rule", care impune transmiterea de informații despre clienți în tranzacțiile transfrontaliere, crescând astfel transparența și trasabilitatea tranzacțiilor.

Dezvoltarea și implementarea unor planuri de răspuns operațional eficiente sunt fundamentale pentru a gestiona amenințările cibernetice, fraudele și alte riscuri care ar putea compromite securitatea platformelor de tranzacționare a activelor virtuale. VASP-urile trebuie să aibă capacitatea de a răspunde prompt la atacuri cibernetice sau la incidente de securitate, asigurând astfel continuitatea operațiunilor și protecția datelor clienților. Actualizarea constantă a infrastructurii tehnologice și efectuarea de teste periodice de securitate vor ajuta la identificarea și remedierea vulnerabilităților.

Supravegherea continuă și actualizarea evaluărilor de risc sunt esențiale pentru a asigura o monitorizare eficientă a activităților VASP. Autoritățile de supraveghere trebuie să efectueze controale periodice on-site și off-site pentru a monitoriza conformitatea cu cerințele legale și pentru a evalua eficiența măsurilor de prevenire a SB/FT. Aceste controale trebuie să fie flexibile și să fie adaptate în funcție de noile riscuri emergente, cum ar fi noile tipologii de tranzacții ilegale care implică criptomonede cu grad înalt de anonimitate sau tranzacții transfrontaliere complexe.

În concluzie, strategiile de răspuns și management al riscurilor în sectorul VASP trebuie să fie dinamice și bine coordonate. Prin implementarea unor măsuri bazate pe risc, planuri de răspuns rapide, colaborare eficientă cu autoritățile și utilizarea tehnologiilor avansate de monitorizare, se va asigura protecția pieței activelor virtuale și conformitatea cu standardele internaționale și europene, contribuind astfel la prevenirea utilizării acestui sector în scopuri ilicite.

## 5.3. Evaluarea și stabilirea profilului de risc pentru sectorul VASP

Stabilirea unui profil de risc adecvat pentru furnizorii de servicii pentru active virtuale (VASP) din România necesită o evaluare detaliată a riscurilor asociate acestui sector. Riscurile majore au fost identificate în legătură cu clienții, produsele și serviciile oferite, tranzacțiile efectuate, precum și conformitatea cu reglementările. Aceste riscuri sunt analizate în funcție de probabilitatea lor de a se materializa și de impactul pe care îl pot avea asupra sectorului, pentru a determina nivelul general de risc și a stabili măsuri.

În sectorul VASP din România, un factor important care contribuie la nivelul de risc este lipsa unui cadru de reglementare strict și clar pentru autorizarea VASP-urilor. Această absență a reglementărilor specifice privind autorizarea, permite operarea VASP-urilor fără supravegherea necesară a întregului sector și pune în pericol integritatea pieței prin expunerea la riscuri ridicate de spălare a banilor și finanțare a terorismului.

Riscurile asociate clienților în sectorul VASP sunt semnificative, în special în contextul clienților anonimi sau proveniți din jurisdicții cu risc ridicat. De asemenea, există riscuri asociate clienților considerați persoane expuse public (PEP) și celor care activează în sectoare economice vulnerabile. Chiar dacă majoritatea clienților provin din România și din Uniunea Europeană, există o expunere moderată la riscurile transfrontaliere și la structurile juridice complexe. Vulnerabilitățile principale provin din lipsa uniformității în aplicarea măsurilor de cunoaștere a clientelei (KYC) și dificultatea de a monitoriza activitățile clienților cu risc ridicat. Aplicarea măsurilor stricte de due diligence este esențială pentru a preveni activitățile ilicite în acest sector.

Probabilitatea acestui risc este considerată medie spre ridicată, având în vedere expunerea sectorului la clienți din jurisdicții vulnerabile. Impactul potențial este ridicat, deoarece activitățile de spălare a banilor și finanțare a terorismului pot afecta grav integritatea sectorului.

Produsele și serviciile oferite de VASP-uri, în special criptomonedele care facilitează anonimitatea și schimburile între monede virtuale și monede fiduciare, prezintă un risc ridicat. Aceste activități sunt adesea greu de monitorizat, iar anonimitatea oferită de criptomonede sporește riscul utilizării lor în activități ilegale. Serviciile OTC (over-the-counter), care permit tranzacții private, contribuie și ele la riscul ridicat din acest sector. Dificultatea monitorizării tranzacțiilor și a aplicării măsurilor de due diligence pentru aceste servicii complică conformitatea cu reglementările anti-spălare de bani și anti-finanțare a terorismului (SB/FT).

Probabilitatea acestui risc este ridicată, deoarece produsele și serviciile oferite de VASP-uri, prin natura lor, favorizează anonimitatea. Impactul este de asemenea ridicat, deoarece aceste produse pot facilita spălarea banilor și finanțarea terorismului, în absența unor măsuri stricte de monitorizare și reglementare. Lipsa unui cadru clar de reglementare pentru autorizarea VASP-urilor agravează aceste riscuri, oferind o fereastră de oportunitate pentru activități ilicite în acest sector.

Tranzacțiile anonime și transfrontaliere din sectorul VASP sunt o sursă de risc considerabil. Deși datele recente arată o scădere a volumului tranzacțiilor în perioada

2021-2024, unele VASP-uri continuă să înregistreze volume semnificative de tranzacții. Fluctuațiile pieței criptoactivelor influențează aceste tranzacții, iar anonimitatea specifică multor tranzacții transfrontaliere adaugă un nivel suplimentar de risc.

Probabilitatea este medie, în contextul scăderii activității recente, dar se menține un risc ridicat datorită volumului mare de tranzacții care rămâne în sector. Impactul este ridicat, deoarece tranzacțiile anonime și transfrontaliere continuă să fie o modalitate de a transfera fonduri ilicite. Monitorizarea atentă a acestor tranzacții și adaptarea constantă a măsurilor de conformitate sunt necesare pentru a limita aceste riscuri.

Riscul de conformitate în sectorul VASP din România rămâne o preocupare majoră, având în vedere provocările legate de aplicarea uniformă a reglementărilor SB/FT. Deși majoritatea VASP-urilor au implementat măsuri de conformitate, inclusiv proceduri KYC și soluții automate de monitorizare, există încă provocări semnificative în ceea ce privește raportarea activităților suspecte și aplicarea măsurilor de prevenire. Cunoașterea insuficientă a tipologiilor de SB/FT și lipsa unui cadru de reglementare clar pentru autorizarea VASP-urilor contribuie la aceste riscuri.

Probabilitatea acestui risc este medie, datorită eforturilor depuse de VASP-uri pentru implementarea măsurilor de conformitate. Cu toate acestea, impactul este ridicat, deoarece neconformitatea poate atrage sancțiuni legale și riscuri reputaționale semnificative.

Amenințările globale la nivel sectorial în sectorul VASP se referă la riscurile majore care afectează întregul sector la nivel internațional, având un impact semnificativ asupra integrității și securității acestuia. Aceste amenințări nu sunt limitate la o singură jurisdicție și pot afecta multiple platforme și entități care operează în întreaga lume. Cu toate că cadrul juridic european (MiCA și TFR) va fi aplicabil în curând, riscurile globale persistă din cauza specificității pieței criptoactivelor, a naturii digitale a acestor active și a vulnerabilităților inerente la atacuri cibernetice și alte activități ilicite.

## Matrice a riscurilor asociate sectorului VASP din România

| Categorie | Amenințări | Vulnerabilități | Probabilitate | Impact | Nivel de risc |
|---|---|---|---|---|---|
| Riscuri privind clienții | Clienți anonimi, din jurisdicții cu risc ridicat | Măsuri insuficiente de KYC, expunere transfrontalieră | Medie spre ridicată | Ridicat | Ridicat |
| Riscuri privind produsele și serviciile | Criptomonede anonime, servicii OTC și ATM-uri | Dificultăți de monitorizare, anonimitate, lipsa autorizării | Ridicată | Ridicat | Ridicat |
| Riscuri privind tranzacțiile | Tranzacții transfrontaliere anonime de mare valoare sau cu numerar prin ATM-uri | Fluctuații pe piața criptoactivelor, anonimitate sporită | Ridicată | Ridicat | Ridicat |
| Riscuri de conformitate | Reglementări insuficiente, Neconformitate cu reglementările SB/FT | Provocări legate de raportarea activităților suspecte, lipsa autorizării | Medie | Ridicat | Mediu - Ridicat |
| Amenințări globale | Atacuri cibernetice, tranzacții transfrontaliere complexe, răspândirea DeFi | Dificultatea trasabilității tranzacțiilor anonime, expunerea la jurisdicții non-cooperante | Ridicată | Ridicat | Ridicat |

**Risc asociat sectorului VASP din România: Risc Ridicat**

Probabilitatea se referă la șansa sau frecvența cu care un risc identificat se poate materializa în sectorul VASP. Aceasta este evaluată în funcție de frecvența istorică a riscului, vulnerabilitățile sectorului și contextul în care operează furnizorii de servicii pentru active virtuale. Probabilitatea este clasificată pe patru niveluri. În cazul unei probabilități foarte mari, riscul este considerat inevitabil, apărând frecvent din cauza unor deficiențe sistemice sau din cauza naturii activităților din sectorul VASP, cum ar fi tranzacțiile anonime sau transfrontaliere cu criptomonede. O probabilitate mare indică faptul că riscul este foarte probabil să apară în condiții favorabile, cum ar fi interacțiunile cu clienți din jurisdicții cu risc ridicat. Dacă probabilitatea este moderată, există o șansă medie ca riscul să apară, de obicei în circumstanțe specifice, cum ar fi fluctuațiile pieței criptoactivelor. La nivelul unei probabilități scăzute, riscul este puțin probabil să apară și se manifestă doar în situații izolate, cum ar fi deficiențe operaționale minore.

Impactul se referă la gravitatea sau consecințele pe care un risc le poate avea asupra sectorului VASP dacă se materializează. Acesta poate include atât efecte financiare, cât și consecințe legale. În cazul unui impact ridicat, riscul poate avea consecințe grave asupra funcționării sectorului, stabilității financiare și conformității cu reglementările, cum ar fi nerespectarea cerințelor SB/FT, ceea ce poate duce la sancțiuni majore și pierderi semnificative. Un impact moderat indică faptul că riscul ar afecta activitatea sectorului, dar într-o măsură gestionabilă pe termen mediu, cum ar fi deficiențele temporare în aplicarea măsurilor KYC. Dacă impactul este scăzut, consecințele sunt minore și pot fi gestionate fără efecte pe termen lung asupra VASP-urilor, cum ar fi erorile operaționale minore fără consecințe asupra securității fondurilor sau conformității.

Matricea de risc combină probabilitatea și impactul pentru a determina nivelul general de risc pentru fiecare categorie. De exemplu, un risc cu probabilitate mare și impact ridicat este clasificat ca fiind ridicat, ceea ce înseamnă că necesită măsuri imediate de atenuare. În schimb, un risc cu probabilitate scăzută și impact moderat va fi considerat mediu sau scăzut, și poate fi gestionat cu intervenții periodice și resurse mai puțin semnificative.

La nivel general, riscurile ridicate necesită intervenții urgente și aplicarea unor măsuri riguroase de prevenire și atenuare, precum și o monitorizare constantă pentru a preveni consecințele grave asupra sectorului. Riscurile mediu-ridicate necesită acțiuni prompte și măsuri de prevenire stricte, dar sunt gestionabile pe termen lung. Riscurile medii sunt mai puțin presante și pot fi gestionate prin măsuri de prevenire deja existente, iar riscurile scăzute pot fi abordate prin intervenții minore, fără a avea un impact semnificativ asupra activității generale.

În concluzie, evaluarea sectorială a riscurilor SB/FT în domeniul VASP din România indică un risc ridicat, datorită anonimității tranzacțiilor, complexității produselor și serviciilor oferite, precum și provocărilor de conformitate și reglementare, subliniind necesitatea implementării unor măsuri stricte de monitorizare și control pentru a preveni utilizarea sectorului în activități ilicite.


# Concluzii și recomandări

## 6.1. Rezumatul principalelor constatări

Evaluarea riscurilor asociate sectorului VASP din România scoate în evidență mai multe vulnerabilități esențiale și riscuri majore. Adoptarea noului cadru juridic , care va armoniza legislația națională cu reglementările europene MiCA și TFR, marchează o etapă importantă în reglementarea sectorului criptoactivelor. Acest cadru juridic armonizat va contribui la asigurarea conformității sectorului cu standardele internaționale de prevenire a spălării banilor și finanțării terorismului (SB/FT), protejând astfel investitorii și stabilitatea financiară, oferind în același timp un cadru adecvat pentru inovare și dezvoltare.

Informațiile obținute prin supravegherea realizată de Oficiul Național de Prevenire și Combatere a Spălării Banilor oferă o bază solidă pentru evaluarea riscurilor asociate sectorului VASP. Cu toate acestea, aceste date sunt limitate de dimensiunea redusă a sectorului și de numărul scăzut de controale efectuate, subliniind astfel necesitatea ca evaluarea riscurilor să fie un proces continuu și dinamic. Acest lucru este esențial pentru

a ține pasul cu evoluția sectorului și a amenințărilor emergente, asigurând un sistem eficient de prevenire și combatere a spălării banilor și finanțării terorismului.

Pe plan global, riscurile asociate sectorului VASP sunt amplificate de anonimitatea tranzacțiilor, vulnerabilitățile geografice și utilizarea noilor tehnologii financiare descentralizate. Concentrarea activităților ilicite în jurul anumitor platforme specifice adaugă un nivel suplimentar de risc. În acest context, implementarea completă a recomandărilor FATF și adoptarea unor măsuri stricte de reglementare și conformitate rămân esențiale pentru atenuarea acestor riscuri.

Riscurile legate de clienți sunt, de asemenea, semnificative, în special în ceea ce privește clienții proveniți din jurisdicții cu risc ridicat, persoanele expuse public (PEP) și cei care activează în sectoare economice vulnerabile. Chiar dacă majoritatea clienților provin din România și Uniunea Europeană, există o expunere moderată la riscuri transfrontaliere și la structuri juridice complexe. Aplicarea măsurilor stricte de cunoaștere a clientelei (KYC) și due diligence rămâne esențială pentru a reduce aceste vulnerabilități și a preveni activitățile ilicite.

În ceea ce privește produsele și serviciile oferite de VASP-uri, riscul este considerat ridicat. Anonimitatea și complexitatea tranzacțiilor, inclusiv schimburile între monede virtuale și monede fiduciare, custodia criptoactivelor și operarea ATM-urilor de criptoactive, ridică provocări majore în ceea ce privește conformitatea cu reglementările SB/FT. Serviciile OTC (over-the-counter) contribuie, de asemenea, la acest risc ridicat, datorită naturii private a tranzacțiilor, care necesită o monitorizare mai strictă și măsuri riguroase de cunoaștere a clientelei.

Riscul de conformitate este, de asemenea, un element semnificativ în sectorul VASP din România astfel, deși majoritatea VASP-urilor au implementat măsuri de conformitate, inclusiv proceduri KYC și soluții automate de monitorizare, există în continuare provocări legate de uniformitatea aplicării acestor măsuri și de identificarea și raportarea activităților suspecte. Monitorizarea atentă și aplicarea constantă a măsurilor de prevenire sunt esențiale pentru a asigura integritatea acestui sector în continuă creștere.

În ceea ce privește riscul asociat tranzacțiilor, datele colectate pentru perioada 2021-2024 arată o scădere a activității atât la nivelul ATM-urilor de criptoactive, cât și al volumului general de tranzacții. Această scădere poate fi atribuită fluctuațiilor pieței criptoactivelor, care, după vârful din 2021, a intrat într-o fază de corecție. Deși activitatea în sector a scăzut, complexitatea și valoarea mare a fondurilor implicate în tranzacțiile rămase subliniază necesitatea unei monitorizări continue și a unor măsuri stricte de conformitate.

Deși numărul cazurilor de spălare a banilor asociate sectorului este redus, complexitatea și sofisticarea acestor infracțiuni creează riscuri majore. Criminalitatea transfrontalieră și caracterul global al criptomonedelor complică eforturile autorităților în urmărirea fluxurilor financiare și recuperarea fondurilor ilicite. Pentru a aborda aceste riscuri emergente, consolidarea reglementărilor, utilizarea unor soluții tehnologice avansate și intensificarea cooperării internaționale, sunt esențiale.

Sectorul VASP din România a fost evaluat cu un grad de risc ridicat pe baza riscurilor identificate la nivel național, dar și ținând cont de tendințele globale și riscurile transfrontaliere semnificative. Anonimitatea tranzacțiilor, complexitatea produselor și expunerea la jurisdicții cu risc ridicat amplifică vulnerabilitățile sectorului. În plus, lipsa unui cadru de reglementare complet la nivel național, în special în ceea ce privește autorizarea VASP-urilor, contribuie la creșterea riscurilor. Aceste elemente, combinate cu riscurile internaționale și utilizarea criptoactivelor în activități ilicite, subliniază necesitatea unor măsuri stricte de supraveghere și reglementare.

## 6.2. Recomandări pentru autorități și entități

Pe baza riscurilor identificate în sectorul VASP din România, este esențial ca autoritățile și entitățile implicate să adopte măsuri eficiente și integrate pentru a gestiona vulnerabilitățile și a preveni utilizarea acestui sector în activități ilicite. Implementarea unui cadru de reglementare complet, armonizat cu cerințele europene și internaționale, este crucială pentru consolidarea supravegherii și conformității în acest domeniu.

Un prim pas necesar este adoptarea urgentă a unui cadru clar și coerent pentru autorizarea furnizorilor de servicii pentru active virtuale (VASP). Lipsa unei reglementări stricte pentru autorizarea VASP-urilor reprezintă un risc semnificativ. Implementarea reglementărilor europene, cum ar fi MiCA și TFR, va asigura un control mai bun asupra activităților din acest sector, reducând riscurile de spălare a banilor și finanțare a terorismului (SB/FT).

În același timp, se recomandă ca furnizorii de servicii de schimb între monede virtuale și monede fiduciare, precum și furnizorii de portofele digitale să fie încadrați sub un cod CAEN specific, ceea ce ar facilita o monitorizare mai eficientă a activităților din acest sector și ar contribui la gestionarea riscurilor de spălare a banilor și finanțare a terorismului. Consolidarea măsurilor de cunoaștere a clientelei (KYC) și de due diligence este, de asemenea, esențială. VASP-urile trebuie să aplice măsuri stricte în evaluarea și monitorizarea clienților lor, în special celor din jurisdicții cu risc ridicat și persoanelor expuse public (PEP). Această cooperare ar trebui să includă schimbul de informații între autoritățile de supraveghere și VASP-uri, pentru a facilita identificarea și reducerea riscurilor.

Autoritățile relevante în materie trebuie să colaboreze strâns cu VASP-urile pentru a se asigura că măsurile KYC sunt implementate uniform și eficient. Această cooperare ar trebui să includă schimbul de informații între autoritățile de supraveghere și VASP-uri, pentru a facilita identificarea și reducerea riscurilor.

Având în vedere că România se numără printre primele 10 țări la nivel global în ceea ce privește numărul de ATM-uri pentru criptoactive (86 de aparate), precum și riscurile de SB/FT asociate tranzacțiilor în numerar efectuate prin intermediul acestora, alături de lipsa aplicării consistente a măsurilor de cunoaștere a clientelei, este necesară introducerea unor cerințe mai stricte pentru verificarea identității utilizatorilor și monitorizarea tranzacțiilor realizate prin crypto-ATM-uri.

În plus, riscurile ridicate asociate tranzacțiilor anonime și transfrontaliere necesită dezvoltarea unor mecanisme avansate de monitorizare. Utilizarea tehnologiilor moderne, cum ar fi soluțiile automate de monitorizare a tranzacțiilor suspecte, implementarea cerințelor „travel rule" și schimbul de date între autoritățile competente din diferite jurisdicții vor fi esențiale pentru a detecta rapid activitățile suspecte. De asemenea, este important să se consolideze cooperarea între VASP-uri și autorități pentru a asigura respectarea standardelor internaționale și a reglementărilor naționale.

Cooperarea la nivel național între organele de aplicare a legii, autoritățile de supraveghere și alte autorități implicate este esențială pentru o supraveghere eficientă a sectorului VASP și pentru a asigura o reacție rapidă și coordonată în fața riscurilor. Această cooperare poate implica schimbul de informații, investigarea comună a tranzacțiilor suspecte și aplicarea consecventă a sancțiunilor pentru neconformitate.

Având în vedere caracterul transfrontalier al tranzacțiilor cu criptoactive, cooperarea internațională rămâne esențială. Organele de aplicare a legii, autoritățile de supraveghere și alte autorități relevante, trebuie să continue colaborarea cu partenerii din alte state pentru a detecta activitățile suspecte care implică mai multe jurisdicții. Îmbunătățirea mecanismelor de schimb de informații la nivel internațional, în special între autoritățile de supraveghere și organele de aplicare a legii, va contribui la prevenirea activităților de spălare a banilor și finanțare a terorismului.

Deși ONPCSB desfășoară sesiuni de instruire pentru entitățile VASP, este importantă consolidarea continuă a capacității de conformitate. Aceste sesiuni trebuie să fie extinse și actualizate constant pentru a reflecta noile tipologii de spălare a banilor și finanțare a terorismului, asigurându-se astfel că VASP-urile sunt pregătite să reacționeze rapid la riscurile emergente și să aplice măsurile de conformitate conform reglementărilor SB/FT.

În concluzie, pentru a atenua riscurile ridicate identificate în sectorul VASP din România, este esențială adoptarea unui cadru juridic robust și implementarea unor măsuri stricte de prevenire și monitorizare. De asemenea, cooperarea eficientă la nivel național între autoritățile competente în materie este vitală pentru o supraveghere eficientă a sectorului. Prin aplicarea unor măsuri adecvate și dezvoltarea unor mecanisme eficiente de monitorizare și raportare, sectorul VASP poate fi protejat împotriva utilizării în activități ilicite, contribuind la menținerea stabilității financiare și la protejarea investitorilor.