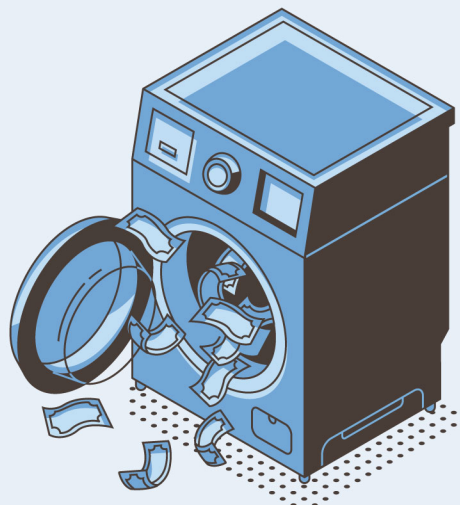
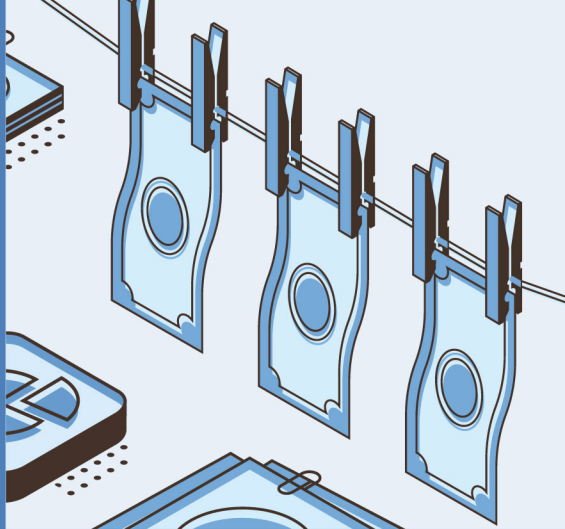


# Tipologii de spălare a banilor în Republica Moldova



## Broșură pentru jurnaliști

Combaterea corupției prin aplicarea legii și prevenire (CLEP)

Funded  
by the European Union  
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented  
by the Council of Europe

# TIPOLOGII DE SPĂLARE A BANILOR ÎN REPUBLICA MOLDOVA

Broșură pentru jurnaliști

**Combaterea Corupției prin Aplicarea Legii și Prevenire (CLEP)**

---

Funded  
by the European Union  
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

---

Implemented  
by the Council of Europe

**Ediție în limba română**

Publicată de către Consiliul Europei,  
F-67075 Strasbourg Cedex  
[www.coe.int](http://www.coe.int)

© Consiliul Europei, aprilie 2020

Machetare copertă și text:

Foxtrot SRL, Chișinău

Imprimat de Foxtrot SRL, Chișinău

Număr de exemplare: 250 unități

Toate drepturile rezervate. Nicio parte a acestei publicații nu poate fi tradusă, reprodușă sau transmisă, în orice formă sau prin orice mijloace, electronice (CD-Rom, Internet etc) sau mecanice, inclusiv fotocopiere, înregistrare sau orice sistem de stocare sau extragere a informațiilor, fără permisiunea prealabilă în scris a Directoratului pentru Comunicare (F-67075 Strasbourg Cedex sau [publishing@coe.int](mailto:publishing@coe.int))

Această lucrare a fost elaborată cu asistența financiară a Uniunii Europene și a Consiliului Europei.

Opiniile exprimate în această lucrare aparțin autorilor și în nici un fel nu reflectă opinia oficială a Uniunii Europene și/sau a Consiliului Europei.

Pentru informații mai detaliate privind conținutul acestei lucrări, vă rugăm să contactați:

Subdiviziunea pentru Crime  
Economice și Cooperare,  
Departamentul Acțiuni împotriva Crimelor,  
Directoratul General pentru Drepturile  
Omului și Supremația Legii,  
Consiliul Europei

E-mail: [contact.econcrime@coe.int](mailto:contact.econcrime@coe.int)

Internet: [www.coe.int/corruption](http://www.coe.int/corruption)

# CUPRINS

---

<b>INTRODUCERE</b>	<b>5</b>
<b>SCHEMELE PROFESIONISTE TRANSFRONTALIERE DE SPĂLARE DE BANI (DE TIP „SPĂLĂTORIE”) ȘI MODUL DE OPERARE</b>	<b>7</b>
<b>SPĂLAREA VENITURILOR PROVENITE DIN DROGURI. MODUL DE OPERARE AL GRUPURILOR CRIMINALE CARE VÂND DROGURI PRIN DARK WEB SAU PRIN SERVICIILE DE MESAGERIE ONLINE</b>	<b>12</b>
<b>SPĂLAREA VENITURILOR PROVENITE DIN INFRAȚIUNI DE CORUPȚIE</b>	<b>15</b>
<b>CATEGORII DE DATE ȘI RESURSE INFORMAȚIONALE CARE POT SUSȚINE INVESTIGAȚIILE JURNALISTICE</b>	<b>18</b>
<b>LISTA RESURSELOR ONLINE (BAZE DE DATE DISPONIBILE PUBLIC) PENTRU A SUSȚINE INVESTIGAȚIILE PRIVIND SPĂLAREA BANILOR</b>	<b>20</b>
<b>BIBLIOGRAFIE UTILĂ PENTRU SUSȚINEREA INVESTIGAȚIILOR SB</b>	<b>22</b>



# INTRODUCERE

---

**A**ceastă broșură oferă o descriere a modului de operare a actorilor infracționali și a spălătorilor de bani care sunt relevanți pentru contextul de risc din Republica Moldova.

— Evaluarea Națională a Riscului (ENR) din Republica Moldova, realizată în 2017, prezintă principalele amenințări, vulnerabilități și riscuri de spălare a banilor și finanțare a terorismului (SB/FT) la care este expusă țara.

— Principalul risc provine din infracțiunile predicat de trafic de droguri, corupție, trafic de persoane, evaziune fiscală și contrabandă. Vulnerabilitățile în ceea ce privește spălarea banilor o constituie utilizarea majoră a numerarului, structurile fundamentale de beneficiari efectivi opace și utilizarea societăților fictive pentru schemele de spălare a banilor. Corupția este recunoscută în ENR ca una dintre cele mai stringente probleme din Republica Moldova.

— Traficul de droguri și traficul de persoane sunt principalele amenințări de spălare a banilor provenite din infracțiunile comise în afara țării. Detaliind problema, ENR indică faptul că Republica Moldova nu este o țară care produce droguri, dar servește ca punct de tranzit către Europa de Est și, într-o măsură mai redusă, este o țară de destinație. În ceea ce privește traficul de persoane, una dintre caracteristici este prezența sistematică a Grupării de Crimă Organizată (GCO) în săvârșirea infracțiunilor.

— În ceea ce privește încasările care generează infracțiuni săvârșite pe plan intern, corupția, evaziunea fiscală și contrabanda sunt principalele amenințări privind spălarea banilor.

— Această broșură se concentrează și descrie tipologiile și modul de operare al infractorilor angajați în următoarele activități ilegale:

- ▶ Schemele profesionale transfrontaliere de spălare a banilor (de tip „spălătorie”);
- ▶ Traficul de droguri (inclusiv vânzarea de droguri fără contact prin intermediul Dark Web);
- ▶ Spălarea de bani pentru veniturile provenite din acte de corupție.



# SCHEMELE PROFESIONISTE TRANSFRONTALIERE DE SPĂLARE DE BANI (DE TIP „SPĂLĂTORIE”) ȘI MODUL DE OPERARE

---

**D**eși faimoasa schemă de tip „Spălătorie”, care depindea foarte mult de utilizarea sistemului financiar al Republicii Moldova, a fost utilizată doar o singură dată, riscurile asociate schemelor de spălare a banilor (SB) bazate pe comerț și utilizarea conturilor societăților fantomă offshore rămân relativ mari.

■ Schema de tip „Spălătorie” era o schemă tradițională profesionistă la scară largă de SB, concepută pentru a muta fonduri ale terților (inclusiv actori infracționali). Profesioniștii specializați în spălarea banilor (PSSB) sunt facilitatori care oferă servicii de spălare a banilor infractorilor în schimbul unui onorariu/comision. Aceștia nu sunt implicați în activitățile infracționale propriu-zise care generează venituri și își pot oferi serviciile unei game largi de infractori (inclusiv celor implicați în traficul de droguri și persoane, fraude, infracțiuni informatice, corupție și delapidare).

■ Raportul privind spălarea de bani profesionistă emis de Grupul de Acțiune Financiară Internațională (GAFI) în iulie 2018 oferă o descriere generală a modelului de afaceri PML și a unei game largi de mecanisme și instrumente pe care acestea le utilizează.

■ În general, schemele financiare executate de PSSB constă în trei etape<sup>1</sup>:

---

1. Raportul GAFI, iulie 2018, *Spălare de bani profesionistă*, accesat în martie 2020.



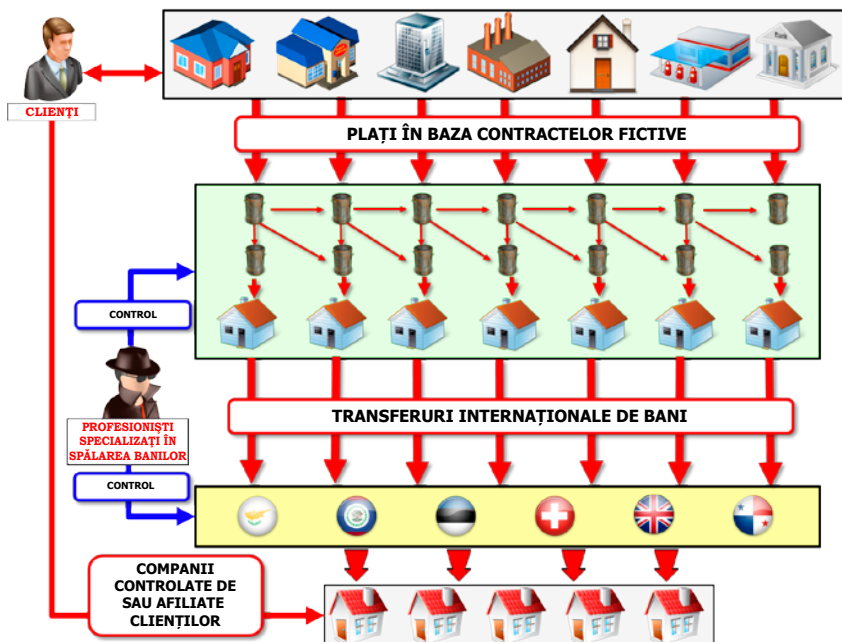


Figura 1. Etapele schemei SB

## ETAPA I: VENITURILE PROVENITE DIN ACTE INFRAȚIONALE SUNT TRANSFERATE CĂTRE, SAU COLECTATE DE CĂTRE, PSSB

În această primă etapă, fondurile sunt transferate, fizic sau electronic, către PSSB sau către entități care operează în numele acestora. Modul de introducere a fondurilor în schema de spălare a banilor variază în funcție de tipurile de infrațiune(i) predicat<sup>2</sup> și de forma în care au fost generate veniturile provenite din acte infraționale (de ex., numerar, fonduri bancare, monedă virtuală etc.).

Infracțorii care obțin venituri într-o formă de monedă virtuală (de ex., proprietarii de magazine online ilegale, inclusiv piețele din Dark Web) trebuie să aibă portofele electronice sau adrese de cripto-monedă, la care pot fi accesate de PSSB.

2. O infrațiune predicat de SB este activitatea infracțională subiacentă care a generat bunurile/proprietățile spălate.

## Exemple:

- ▶ Numerarul este înmănat unui colector de numerar care efectuează depozite de numerar în conturi bancare.
- ▶ Veniturile provenite din acte infracționale (de exemplu, veniturile rezultate din fraude, delapidări și infracțiuni fiscale) sunt alocate în conturi bancare, ulterior aceste fonduri sunt transferate electronic către un prim nivel de societăți care sunt controlate de SBP.

## ETAPA II: ETAPA DE STRATIFICARE EXECUTATĂ DE PERSOANE ȘI/SAU REȚELE

■ În etapa de stratificare, majoritatea PSSB utilizează lichidarea de conturi și mecanisme complexe pentru a face mai dificilă urmărirea fondurilor. O combinație de tehnici diferite de spălare a banilor poate fi utilizată ca parte a unei scheme.

■ Fondurile care au fost transferate în conturile bancare gestionate de spălătorul profesionist sunt, de cele mai multe ori, mutate prin scheme complexe de stratificare sau structuri prin împuterniciți. Structurile prin împuterniciți constau dintr-un lanț complex de conturi ale societăților fantomă, stabilite atât pe plan intern, cât și în străinătate. Fondurile de la clienți diferiți sunt amestecate în cadrul acelorași conturi, ceea ce face mai dificilă urmărirea fondurilor provenite de la un anumit client.



**Figura 2.** O parte din schema transfrontalieră „tradițională” PSSB care poate fi vizibilă pentru Moldova. Veniturile din infracțiuni sunt transferate în contul unei societăți offshore deschise la o bancă din Moldova, în baza unei hotărâri judecătorești fictive și transferate aproape imediat în conturi bancare străine, în temeiul unui contract de împrumut.

## ETAPA III: FONDURILE SPĂLATE SUNT PREDATE ÎNAPOI CLIEŢILOR PENTRU INVESTIŢII SAU ACHIZIŢII DE ACTIVE

■ În ultima etapă, fondurile sunt transferate în conturile controlate de clienţii PSSB, asociaţii apropiaţi ai acestora sau terţi care acţionează în numele lor sau în numele unor persoane juridice afiliate. PSSB poate investi veniturile ilicite în numele acestor clienţi în imobiliare, bunuri de lux şi întreprinderi din străinătate (sau, în unele cazuri, în ţări din care provin fondurile).<sup>3</sup>

■ Un mod de operare similar este utilizat şi în **scopul evaziunii fiscale şi vamale**. Societăţile importatoare (de exemplu, cele situate în Republica Moldova) transferă fonduri pentru „bunurile importate” către un strat de societăţi fantomă intermediare, pentru a-şi creşte, în mod artificial, cheltuielile şi a reduce impozitul pe venit care trebuie plătit. O parte din fonduri este apoi transferată către exportatorii reali aflaţi în străinătate, iar restul fondurilor – mutat mai departe în conturile unor societăţi offshore controlate de beneficiarii acestei scheme.

## UTILIZAREA CONTURILOR „CATĂRILOR FINANCIARI” ÎN CADRUL SCHEMELOR SB

**Un catâr financiar** este o persoană care primeşte bani de la un terţ (sau al cărui cont este utilizat de către un terţ) şi îi transferă într-un alt cont sau îi retrace în numerar pentru a-i preda. În schimbul acestor „servicii”, catârrii financiari obţin un comision.

■ Infraactorii şi, în mod special, profesioniştii specializaţi în spălarea banilor, utilizează pe scară largă conturile catârrii financiari pentru a muta şi a spăla veniturile din obţinute infracţiuni. Catârrii financiari pot efectua tranzacţii fie ei înşişi sau pot emite doar instrumente financiare (conturi bancare, carduri, portofele electronice) pe numele lor şi le pot furniza terţilor pentru plată.

■ Conturile catârrii financiari sunt utilizate pe scară largă în Dark Web – scheme aferente sau în infracţiuni informatice (de exemplu, phishing, atacuri cu coduri ostile (malware), fraude la licitaţii online şi altele).

3. Raportul GAFI, iulie 2018, *Spălarea de bani profesioniastă*, accesat în martie 2020.

■ Catării financiare sunt recrutați în diverse moduri, inclusiv:

- ▶ sub formă de oferte de muncă inițial legitime aferente „serviciilor de transfer de bani”, trimise prin intermediul forumurilor online de locuri de muncă, rețelelor sociale, e-mailurilor etc.;
- ▶ sub formă de mesaje directe trimise prin servicii de mesagerii precum Viber, WhatsApp, Telegram;
- ▶ prin contact direct (pe stradă).

■ Studenții și alte persoane cu vârsta până în 35 de ani sunt persoanele cele mai vizate cărora li se oferă „să facă bani ușori”. Reclamele pentru catării financiare afirmă, de obicei, că reprezintă o societate străină care recrutează „agenți la nivel național” pentru a acționa în numele acesteia și pentru a facilita transferurile financiare. Uneori, aceste reclame subliniază faptul că tranzacțiile nu prezintă niciun fel de riscuri, sunt „100% legitime” și „garantate”.



**Deși catării financiare nu sunt implicați în infracțiunile care generează profiturile infracționale, aceștia sunt complici, deoarece facilitează spălarea veniturilor provenite din acte infracționale.**

■ Autoritățile din Republica Moldova au detectat scheme de criminalitate informatică bazate pe tipologia catărilor financiare. De exemplu, conturile catărilor financiare au fost menționate în „cazul Urgenta”<sup>4</sup>. Un grup de persoane fizice au primit fonduri în conturile lor bancare din Moldova din conturi bancare românești. Fondurile au fost retrase imediat în numerar prin intermediul terminalelor POS (Terminale electronice de plată) de la diverse sucursale bancare din Chișinău. Analizele ulterioare au relevat faptul că conturile bancare românești au fost creditate din conturi bancare din Regatul Unit deținute de cetățeni moldoveni și români. Autoritățile au identificat faptul că această schemă financiară a fost utilizată pentru a muta fonduri furate prin utilizarea virusurilor Dridex și Dyrecare.

■ Conturile catărilor financiare sunt utilizate pe scară largă în schemele financiare care facilitează comerțul ilicit în Dark Web.

4. Consiliul European, Moneyval, *Raportul aferent rundeii a cincea de evaluare reciprocă a Republicii Moldova*, 2019, pagina 57, accesată în martie 2020.

# SPĂLAREA VENITURILOR PROVENITE DIN DROGURI. MODUL DE OPERARE AL GRUPURILOR CRIMINALE CARE VÂND DROGURI PRIN DARK WEB SAU PRIN SERVICIILE DE MESAGERIE ONLINE

---

■ Odată cu trecerea comerțului de droguri în mediul online, infractorii își schimbă modul de operare și utilizează așa-numita vânzare de droguri fără contact, care este susținută prin utilizarea de noi instrumente de plată, cum ar fi portofelele electronice și activele virtuale. Aceasta ar trebui să fie o tendință nouă, dar în creștere, pentru Republica Moldova, care înlocuiește vânzarea tradițională a drogurilor cu utilizare de numerar.

■ Modul general de operare al grupurilor infracționale care vând droguri prin internet este următorul.

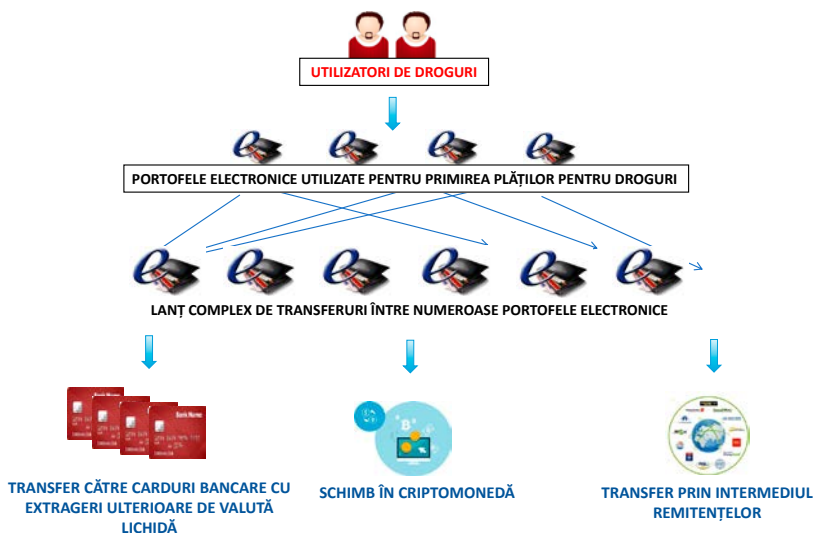
- ▶ La plasarea „comenzii”, clienții magazinelor de droguri din mediul online pot alege între două mijloace de plată – fie transferul de fonduri către portofelul electronic indicat (care aparține magazinului online de droguri), fie la adresa Bitcoin.
- ▶ Schema financiară pentru magazinele de droguri este, de obicei, organizată și gestionată de către un finanțator și rețeaua sa. Rețeaua de spălare a banilor este responsabilă numai de mutarea fondurilor și nu are legături cu traficul de droguri. Numeroase portofele electronice și carduri de debit sunt înregistrate pe numele persoanelor din prima linie. Aceasta implică, de obicei, studenți care emit portofele electronice și carduri de credit și le vând membrilor rețelei de spălare a banilor, neștiind scopul

infracțional al utilizării ulterioare a acestora. Unele portofele electronice sunt utilizate în stadiul de plasare al procesului de spălare.

- ▶ Software-ul special utilizat de către infractori permite schimbarea automată a portofelelor electronice care sunt utilizate pentru plățile drogurilor și transferul fondurilor la un alt nivel de mixare a portofelelor electronice atunci când este atinsă limita. Bani digitali sunt mutați automat printr-un lanț complex de portofele electronice diferite.
- ▶ Bani din portofelele electronice sunt apoi transferați pe carduri bancare și retrași în numerar prin intermediul ATM-urilor (automate bancare). Retragerile prin ATM-uri sunt efectuate de „coordonatorii de numerar” care au mai multe cărți de debit la îndemână (toate cardurile sunt, de obicei, emise pe numele oamenilor de paie. Apoi, numerarul este predat părților interesate. Pentru a crește complexitatea, veniturile pot fi re-depuse pe un nou set de carduri de debit și transferate organizatorilor grupurilor infracționale de trafic de droguri (aflați, de obicei, în străinătate).

**Omul de paie** este o persoană care își oferă cardurile de credit infractorilor și nu știe nimic despre utilizarea ulterioară a acestora în scopuri infracționale.

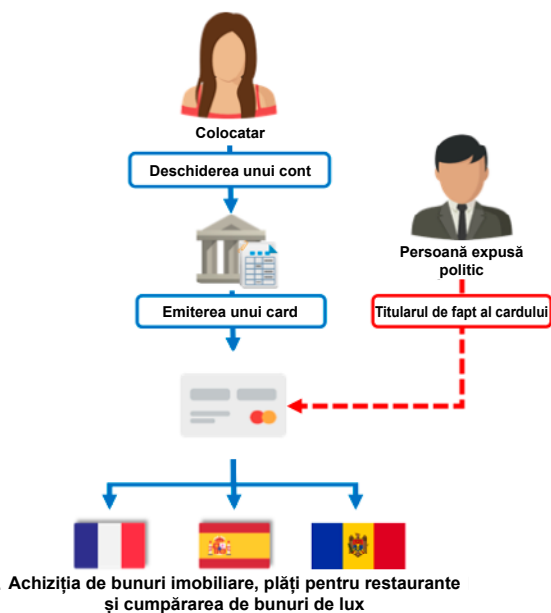
- ▶ Fondurile din portofelele electronice pot fi, de asemenea, preschimbate în Bitcoin-uri prin intermediul caselor de schimb virtuale. Bitcoin-urile sunt uneori utilizate pentru a plăti salarii membrilor organizațiilor de trafic de droguri, inclusiv membrilor de nivel inferior, cum ar fi traficanții mărunți și contrabandiștii, care facilitează vânzarea de droguri. Același finanțator poate lucra cu mai mulți proprietari ai magazinelor din Dark Web, distribuind fondurile spălate către GCO-le respective.



**Figura 3.** Mișcarea fondurilor din magazinele ilicite din Dark Web

# SPĂLAREA VENITURILOR PROVENITE DIN INFRAȚIUNI DE CORUPȚIE

— După cum este recunoscut prin Evaluarea Națională a Riscurilor în Republica Moldova (2017) și alte surse internaționale, corupția este în continuare răspândită în Republica Moldova. Funcționarii corupți care primesc mită, în majoritatea cazurilor, se bazează pe asistența asociaților apropiaților, inclusiv rude, prieteni apropiați, parteneri de încredere și persoane juridice și aranjamente conexe. Aceste categorii de persoane și tranzacțiile semnificative în număr, transferurile internaționale de bani și achizițiile de bunuri imobiliare și de mare valoare ale acestora necesită o atenție sporită.



**Figura 4.** Utilizarea unui cont bancar aparținând unei părți afiliate de către PEP (Persoană Expusă Politic) pentru a ascunde tranzacțiile



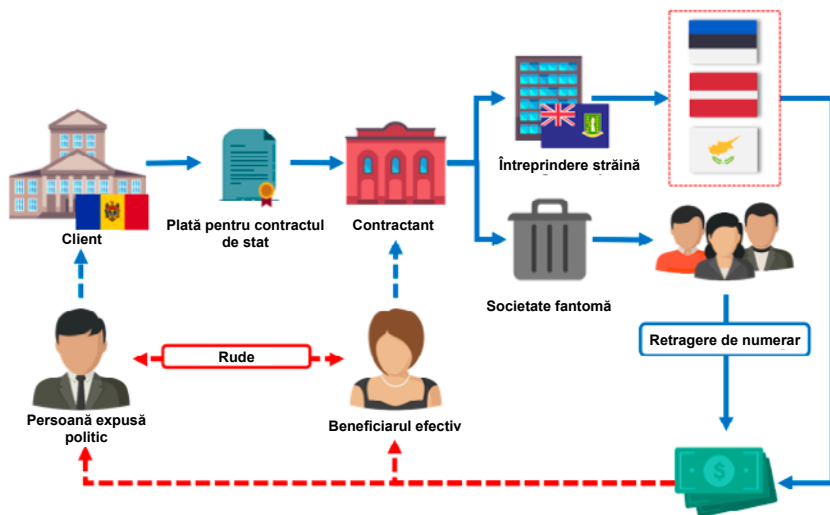
■ Elementele de bază în detectarea fluxurilor financiare care decurg din corupție includ:

- ▶ detectarea averii – activelor și proprietăților inexplicabile persoanelor expuse politic (PEP) și ale rudelor și asociaților acestora, care nu sunt în concordanță cu veniturile declarate;
- ▶ depistarea asociaților apropiați ai PEP – contactele frecvente, rudele, prietenii, partenerii de afaceri, șoferii acestora și alte persoane care pot fi utilizate ca terți în tranzacțiile financiare efectuate în numele PEP;
- ▶ depistarea persoanelor juridice (inclusiv a companiilor străine) aflate sub controlul PEP și al apropiaților acestora;
- ▶ detectarea centrelor geografice de atracție (dacă un PEP intern călătorește frecvent în Spania sau Italia, este foarte probabil ca acesta/aceasta să dețină proprietăți sau bunuri în această țară).



Corupția este, în marea majoritate a cazurilor, asociată fondurilor publice, delapidării și abuzului în serviciu, astfel încât se pot trage multe concluzii pe baza analizei datelor privind achizițiile publice (inclusiv informațiile privind părțile la contracte, directorii în cauză, membrii consiliului de licitație și alte persoane implicate, condițiile contractelor și caracteristicile suspecte ale acestora, care reflectă fluctuațiile prețului contractului, termene limită neobișnuit de rapide ale procedurilor de licitație, indicarea unor caracteristici foarte specifice ale bunurilor și serviciilor etc.)

■ Schema de mai jos reflectă o tipologie tradițională de „recul”, în care fondurile publice furnizate contractantului sunt încasate prin intermediul societăților fantomă și a conturilor bancare ale persoanelor fizice sau mutate în străinătate prin conturi ale societăților offshore, și apoi predate PEP, asociaților apropiați ai acestora și proprietarilor contractantului angajat în delapidare.



**Figura 5.** Tipologia delapidării fondurilor publice și a corupției

# CATEGORII DE DATE ȘI RESURSE INFORMAȚIONALE CĂRE POT SUSȚINE ÎNVESTIGAȚIILE JURNALISTICE

---

■ Următoarele categorii de informații sunt esențiale pentru depistarea și investigarea activității infracționale și de SB:

- ▶ **Informații comerciale** (inclusiv informații cu privire la activitățile comerciale ale persoanelor juridice, numărul personalului, contabilitatea financiară, care pot fi disponibile public în funcție de țara de constituire și tipul de societate – importante atât pentru evaluarea activităților societăților care operează în mod real, cât și pentru detectarea societăților fantomă, care sunt utilizate pentru a muta fonduri în scheme SB);
- ▶ **Contracte și licitații** (de regulă publice și care permit obținerea de informații privind părțile contractante, directorii în cauză, membrii consiliului de licitație și alte persoane implicate, condițiile contractelor – inclusiv caracteristicile suspecte ale acestora, care reflectă fluctuațiile ale prețului contractului, termene limită neobișnuit de rapide ale procedurilor de licitație, indicarea unor caracteristici foarte specifice ale bunurilor și serviciilor etc.);
- ▶ **Informații privind proprietatea** (inclusiv registrele naționale ale companiilor cu sursă deschisă, datele de proprietate din diverse scurgeri de date și baze de date comerciale – unele dintre acestea permit descărcarea tuturor societăților străine deținute sau gestionate de cetățeni ai unei anumite țări, cu detaliile personale ale acestora). Aceste informații sunt cruciale pentru detectarea beneficiarilor efectivi, rețelelor afiliate, verificarea conflictelor de interese, detectarea riscurilor de corupție;
- ▶ **Informații vamale** (inclusiv informații de bază cu sursă deschisă privind implicarea persoanelor juridice în activități comerciale);

- ▶ **Informații privind veniturile publice** (cu precădere importante pentru detectarea corupției și a schemelor de delapidare a fondurilor publice prin detectarea discrepanțelor între veniturile declarate ale PEP și rudele acestora și bunurile și proprietățile deținute în fapt – și investigarea ulterioară a unei averi inexplicabile);
- ▶ **Informații tehnice și de geolocalizare** (inclusiv adrese IP, de exemplu, în tranzacțiile blockchain);
- ▶ **Informații de comunicare** (inclusiv numere de telefon mobil, nume de cont);
- ▶ **Relația socială** (inclusiv informații din rețelele sociale cu privire la „prieteni” și contacte);
- ▶ **Informații penale** (inclusiv baze de date ale poliției naționale disponibile public, liste Interpol, diverse „site-uri web cu treburi murdare” etc.);
- ▶ **Datele instanțelor comerciale** (inclusiv în scopul detectării hotărârilor judecătorești falsificate, care au fost utilizate ca pretext pentru transferul transfrontalier de bani în schemele de tip „Spălătorie”)
- ▶ **Diverse liste și registre cu sursă deschisă**, inclusiv liste publice ale PEP interne și străine, scurgeri de date.

# LISTA RESURSELOR ONLINE (BAZE DE DATE DISPONIBILE PUBLIC) PENTRU A SUSȚINE INVESTIGAȚIILE PRIVIND SPĂLAREA BANILOR

---

## 1. Baza de date Off-shore Leaks:

■ <https://offshoreleaks.icij.org>

■ Baza de date este întreținută de Consorțiul Internațional al Jurnaliștilor de Investigație. Aceasta conține informații cu privire la peste 785 de mii de companii, fundații și trusturi offshore din investigațiile Panama Papers, Offshore Leaks, Bahamas Leaks și Paradise Papers.

## 2. Catalogul tabloului de investigații a Bazelor de date de cercetare:

■ <https://investigativedashboard.org/databases>

■ Baza de date conține link-uri web către numeroase registre ale societăților reglementate, registre funciare și imobiliare, baze de date ale hotărârilor judecătorești, informații ale biroului de brevete și alte informații disponibile public la nivel mondial (grupate pe țări și regiuni).

## 3. Baza de date PRCOC Aleph:

■ <https://aleph.occrp.org>

■ Baza de date este o arhivă globală de materiale de cercetare pentru raportare investigativă, care conține diferite scurgeri, liste de sancțiuni și PEP, baze de date de active și companii, contracte, informații privind achizițiile etc.

#### **4. Harta traficului maritim în timp real:**

■ [www.marinetraffic.com](http://www.marinetraffic.com)

■ Harta informațiilor de urmărire globală a navelor care arată poziția actuală și informațiile de bază despre navele maritime.

#### **5. Dispozitiv de geolocație prin IP:**

■ <https://www.iplocation.net>

■ Baza de date oferă suport pentru identificarea locației aproximative a unui utilizator IP (adresă IP).

#### **6. Căutare gratuită a Persoanelor Expuse Politic:**

■ <https://namescan.io/FreePEPCheck.aspx>

■ Baza de date oferă o examinare pentru PEP și rudele și asociații apropiate ai acestora.

#### **7. Căutare de Persoane urmărite de Interpol:**

■ <https://www.interpol.int/en/How-we-work/Notices/View-Red-Notices>

■ Conține Avertismente roșii publice pentru persoanele date în urmărire (Avertismentele roșii sunt emise pentru fugarii dați în urmărire fie în scopul urmăririi penale, fie pentru executarea unei sentințe. Un Avertisment roșu este o solicitare către organele de aplicare a legii din întreaga lume pentru localizarea și arestarea provizorie a unei persoane aflate în așteptarea extrădării, predării sau a unei acțiuni juridice similare).

# BIBLIOGRAFIE UTILĂ PENTRU SUSȚINEREA INVESTIGAȚIILOR SB

---

1. *Buletinul Grupului Egmont, iulie 2019, Facilitatori profesioniști a spălării banilor;*
2. *Buletinul Grupului Egmont, iulie 2019, Fraude de compromitere a afacerilor prin e-mail;*
3. *Buletinul Grupului Egmont, iulie 2019, Proiect de finanțare împotriva terorismului – actori singurari și celule mici (rezumat public);*
4. *Grupul Egmont, Rezumat public, iulie 2019, Instrumente și practici UIF pentru investigarea spălării veniturilor obținute din acte de corupție);*
5. *GAFI – Grupul Egmont, 2018, Tănuirea beneficiarului efectiv;*
6. *Raportul GAFI, iulie 2018, Fluxuri financiare din traficul de persoane;*
7. *Raportul GAFI, iulie 2018, Spălare de bani profesionistă;*
8. *Raportul GAFI, ianuarie 2018, Finanțarea recrutării în scopuri teroriste;*
9. *Raportul GAFI, octombrie 2015, Spălarea banilor prin transportul fizic al numerarului;*
10. *GAFI, octombrie 2015, Riscuri emergente de finanțare a terorismului;*
11. *Raportul GAFI, iulie 2015, Riscurile și vulnerabilitățile spălării banilor și finanțării terorismului asociate cu aurul;*
12. *Raportul GAFI, iunie 2014, Fluxurile financiare aferente producției și traficului de opiacee afgane;*
13. *Raportul GAFI, iunie 2014, Riscul de abuzuri teroriste în organizațiile non-profit;*
14. *Raportul GAFI, octombrie 2013, Rolul Hawala și al altor furnizori similari de servicii în spălarea banilor și finanțarea terorismului;*
15. *Raportul GAFI, iunie 2013, Vulnerabilitățile spălarea banilor și finanțării terorismului profesioniștilor din domeniul juridic.*







**A**ceastă broșură oferă o descriere a tipologiilor de spălare a banilor (SB) relevante contextului de risc din Republica Moldova. Aceasta descrie, de asemenea, metodele utilizate de infractori referitoare la infracțiunile specifice de SB și analizează exemple concrete și scheme care au ca scop facilitarea înțelegerii de către cititori a celor mai des întâlniți pași făcuți în cadrul procesului de spălare a banilor. Broșura mai are ca scop de a oferi jurnaliștilor informații și resurse care pot să ajute investigațiile privind SB, precum și o listă de baze de date online, disponibile public, care ar fi utile în acest sens.

[www.coe.int/clep](http://www.coe.int/clep)

RON

Consiliul Europei este cea mai mare organizație în materie de drepturi ale omului de pe continent. Aceasta include 47 de state membre, dintre care 28 sunt state membre ale Uniunii Europene. Toate statele membre ale Consiliului Europei au aderat la Convenția Europeană a Drepturilor Omului, un tratat conceput pentru a proteja drepturile omului, democrația și statul de drept. Curtea Europeană a Drepturilor Omului veghează la respectarea prevederilor Convenției de către statele semnatare.

[www.coe.int](http://www.coe.int)

Statele membre ale Uniunii Europene au hotărât să-și unească cunoștințele, resursele și destinele sale. Împreună, ele au creat o zonă de stabilitate, democrație și dezvoltare durabilă, în același timp menținând diversitatea culturală, toleranța și libertățile individuale. Uniunea Europeană este decisă să împărtășească realizările și valorile sale cu țările și popoarele din afara hotarelor sale.

<http://europa.eu>



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE