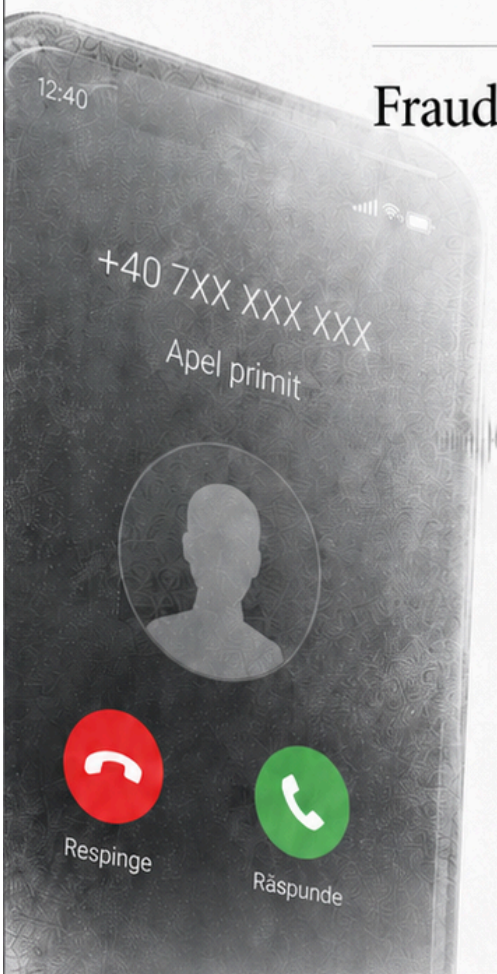
WE WATCH THE GOVERNMENT FOR YOU
WATCH DOG MD

Scamafonie mobilă

Frauda telefonică ca industrie regională

MAI 2026



FILE NO. [redacted]

SUBJECT [redacted]

ID [redacted]

[redacted]

Andrei Curăraru

[redacted]

expert politici publice

[redacted]

FRAUDĂ

Scamafonie mobilă

Op-ed de Andrei Curăraru, Watchdog.md

Milton Group a operat simultan din Israel, Kyiv și Londra. Fondatorul său, David Kezerashvili, este un fost ministru al apărării georgian. Pe 9 decembrie 2024, FSB (Serviciul Federal de Securitate al Federației Ruse) a percheziționat un birou al companiei din Moscova și a arestat 11 angajați și manageri, inclusiv un conducător al rețelei, cetățean israeliano-ucrainean. Dar David Kezerashvili, pentru care Rusia emite un mandat anterior, nu a fost reținut, se afla în Londra. Co-conducătorul D. Todua, cetățean israeliano-georgian, nu a fost prins nici el. The Moscow Times și The Record au documentat detaliile, cu rezerva că afirmațiile FSB nu au putut fi verificate independent.

Industria înșelătoriei telefonice s-a construit pe rețelele rusești ale anilor 1990 și 2000. CarderPlanet, unul dintre primele forumuri majore de fraudă bancară electronică, a apărut la Odesa în 2001, administrat de vorbitori de rusă, cu rețele de distribuție și spălare de bani concentrate în Moscova și Sankt-Petersburg. Victimele primare vorbeau tot rusă. Capitalul acumulat a construit infrastructura care funcționează și azi.

Rusia: producătorul și victima

Rusia este astăzi și cel mai mare furnizor și cel mai mare consumator al industriei pe care a construit-o. FSB a raportat în 2024 pierderi de 170 de miliarde de ruble cauzate de frauda telefonică. Ministerul de Interne al Federației Ruse a citat 200 de miliarde. Sberbank, cea mai mare bancă de stat rusă, a estimat 295 de miliarde. Cifrele provin din surse cu interese diferite și nu pot fi verificate independent; diferența reflectă metodologii diferite. Poliția rusă a înregistrat oficial peste 640.000 de dosare penale pentru fraudă telefonică în același an.

Ce nu apare în statisticile oficiale sunt atacurile asupra celor care au raportat escrocii sau nu le-au transferat bani. Mediazona, publicație independentă rusă, a documentat cel puțin 187 de incendii deliberate, organizate de rețele de fraudatori împotriva persoanelor care n-au transferat bani sau au denunțat escrocii. Date publicate în ianuarie 2025. Echipe trimise la locuințe pentru a provoca incendii. Nu există un echivalent al acestei practici documentat sistematic în altă țară europeană. Ea indică o fuziune între frauda financiară și crima organizată violentă, fuziune posibilă numai printr-un grad ridicat de toleranță instituțională.

Toleranța are rădăcini documentate anterior războiului ruso-ucrainean. La finele anilor 2010, autoritățile ruse confiscaseră mii de telefoane mobile din colonii penale, penitenciarele funcționau ca platforme de operare a schemelor de fraudă. Zece ani mai târziu, situația s-a schimbat. O parte din operațiuni au migrat peste hotarele Rusiei. În 2021, FSIN (Serviciul Federal de Executare a Pedepselor din Rusia) nega public existența „centrelor de apeluri din penitenciare”, iar adjunctul șefului poliției din Moscova recunoștea că aproximativ 40% din furturile la distanță implicau centre situate în afara Rusiei. Infrastructura se mutase deja, nu dispăruse. Rețelele existau și funcționau neperturbat inclusiv datorită coruperii organelor locale de ordine. Potrivit unei cercetări Sberbank privind centrele de apeluri frauduloase, aceștia primeau plăți regulate pentru a închide ochii la existența rețelei.

Continuitatea după 2022 are exemple concrete. Milton Group funcționa cu birourile din Moscova active și recruta studenți ruși pentru centre de apeluri. Când FSB a acționat în decembrie 2024, cei doi conducători ai rețelei nu au putut fi arestați pentru că se aflau în afara Rusiei. Raportul GI-TOC (Global Initiative Against Transnational Organized Crime, inițiativă internațională de monitorizare a crimei organizate transnaționale) din aprilie 2026 documentează că zonele de impunitate juridică constituie factorul principal de supraviețuire al industriei.

> În context, putem presupune că Transnistria intră în această categorie nu doar ca potențială locație a centrelor de apeluri, ci ca spațiu prin care circulă bani fără supraveghere bancară funcțională și unde urmărirea penală se oprește la limita administrativă.

Expansiunea post-2022

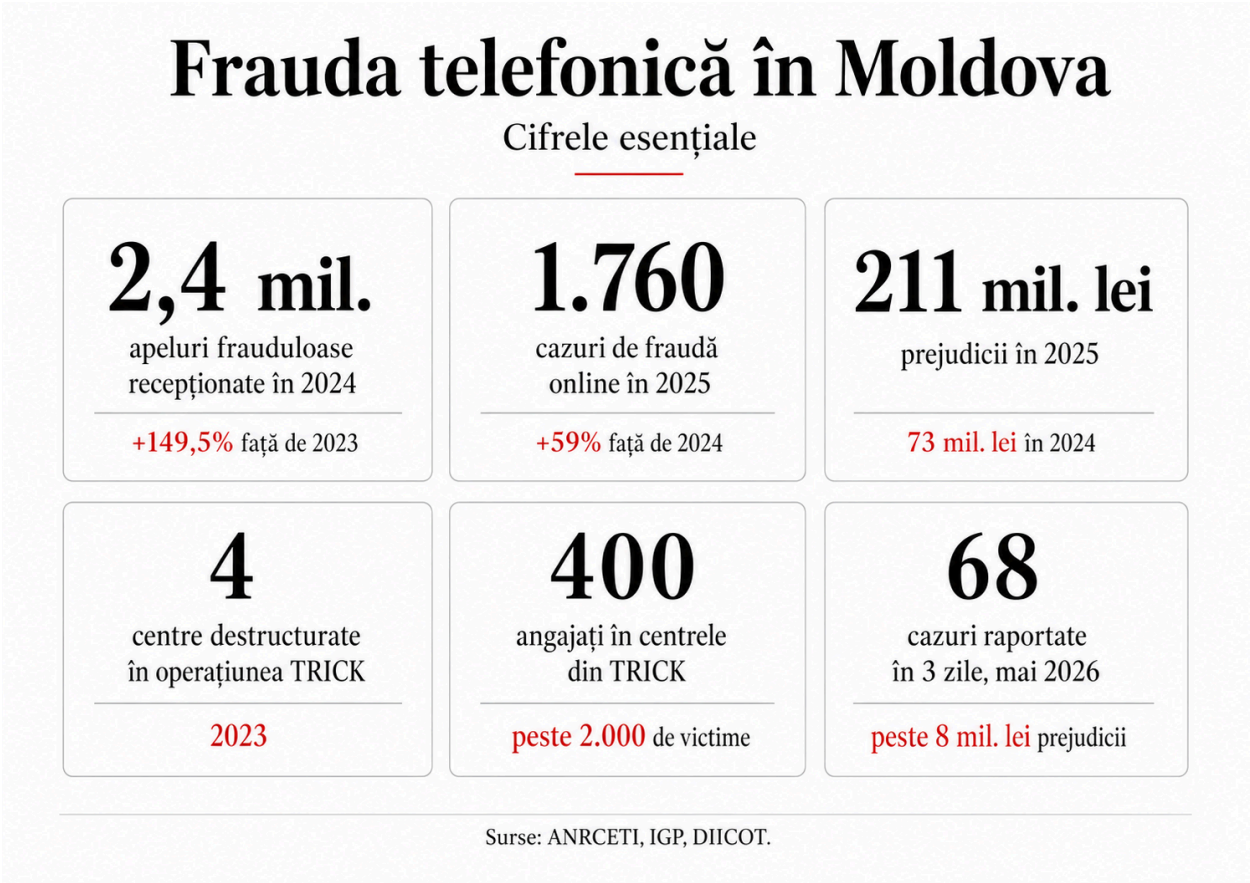
GI-TOC estimează că industria s-a extins semnificativ după 2022. OCCRP (Organized Crime and Corruption Reporting Project, rețea internațională de jurnalism investigativ) a documentat în martie 2025 operațiunea „Scam Empire”: cel puțin 32.000 de victime în toată lumea, aproximativ 275 de milioane de dolari, centre active în Georgia, Israel, Bulgaria, Ucraina, Spania și Cipru.

Ucraina a ajuns să găzduiască între 1.500 și 2.000 de centre de apeluri active în 2024, unele centre recrutează persoane dislocate de conflict. Războiul a creat vulnerabilitate economică și dezorganizare instituțională..

Răspunsul instituțional ucrainean diferă de cel rusesc. Pe 9 decembrie 2024, aceeași zi cu raidul FSB, autorități din Cehia, Letonia, Lituania și Ucraina, cu sprijinul Eurojust, au efectuat 72 de percheziții în Dnipro, Ivano-Frankivsk și Kyiv. Doisprezece persoane au fost arestate, 45 identificate ca suspecți, prejudicii estimate peste 10 milioane de euro. Când au existat dovezi și cooperare internațională, au urmat arestări. Europol a finalizat separat, în aprilie 2024, operațiunea PANDORA: 12 centre de apeluri frauduloase au fost desființate în Albania, Bosnia-Herțegovina, Kosovo și Liban.

Moldova: gazdă și victimă

Moldova nu este doar o observatoare a acestui fenomen. În 2024, utilizatorii de telefonie mobilă din Republica Moldova au recepționat aproximativ 2,4 milioane de apeluri frauduloase, în creștere cu 149,5% față de 2023, date raportate de operatori către ANRCETI (Agenția Națională de Reglementare în Comunicații Electronice și Tehnologia Informației). În 2025, IGP (Inspectoratul General al Poliției) a înregistrat oficial 1.760 de cazuri de fraudă online, cu 59% mai mult decât în 2024, cu prejudicii de 211 milioane de lei față de 73 de milioane în anul anterior, aproape triple într-un singur an.



Ce s-a făcut în ultimii ani pentru a contracara acest fenomen? În 2023, DIICOT (Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism din România), în parteneriat cu autoritățile moldovenești, a finalizat operațiunea TRICK. Patru centre de apeluri pe teritoriul Republicii Moldova, 400 de angajați, peste 2.000 de victime, prejudicii de 3 milioane de euro. Centrele funcționau din 2021 iar victime erau cetățeni români..

În mai 2026, fraudele telefonice au ieșit din zona infracțiunii oportuniste și arată ca activitate organizată la nivel industrial: recrutare de curieri, colectare de numerar, conversie în criptovalută, transfer mai departe.

În doar trei zile, au fost raportate 68 de cazuri și prejudicii de peste 8 milioane de lei. Pe 19 mai, 24 de cazuri într-o singură zi au produs pierderi de 1,5 milioane de lei. În weekendul 23-24 mai, alte 29 de cazuri au dus la peste 6 milioane de lei pierdute și circa 350 de tentative prevenite.

Victimele nu sunt alese întâmplător. Cazurile mari indică oameni din Capitală cu economii disponibile și vulnerabilitate la autoritate: peste 2 milioane de lei în Ciocana, peste 500.000 de lei în Buiucani, peste 200.000 de lei în Rîșcani. Alți 400.000 de lei la Ceadîr-Lunga. În dosarele documentate anterior, Poliția a identificat grupări cu membri între 17 și 53 de ani, inclusiv cetățeni străini, curieri prinși în flagrant, colectori de bani și persoane care transformau sumele în criptovalută.

Metoda folosește autoritate falsă și presiune temporală. Apelantul se prezintă drept bancă, poliție, BNM, SIS, Moldcell, Premier Energy sau funcționar public. Scenariul introduce un pericol imediat: fraudă bancară, dosar penal, blocarea contului, datorie inventată, suspiciune de finanțare a terorismului. Victima este izolată psihologic, împinsă să nu verifice, apoi direcționată spre transfer sau predare de numerar. Din punct de vedere criminologic, avem o schemă de fraudă cu inginerie socială, logistică locală și mecanism de spălare rapidă a banilor.

Pe de altă parte, există și dimensiunea de dezinformare pe subiectul escrocheriilor telefonice. DFRLab (laboratorul de cercetare digitală al Atlantic Council, specializat în dezinformare) a documentat în decembrie 2024 că o rețea de portaluri pro-Kremlin, parte din ecosistemul Pravda, acoperă disproporționat cazurile de fraudatori cu cetățenie ucraineană care operează în Moldova. Cazurile sunt reale. Selecția este tendențioasă. Publicul vede escrocul cu pașaport ucrainean, nu rețelele mai vechi și mai mari care au construit industria.

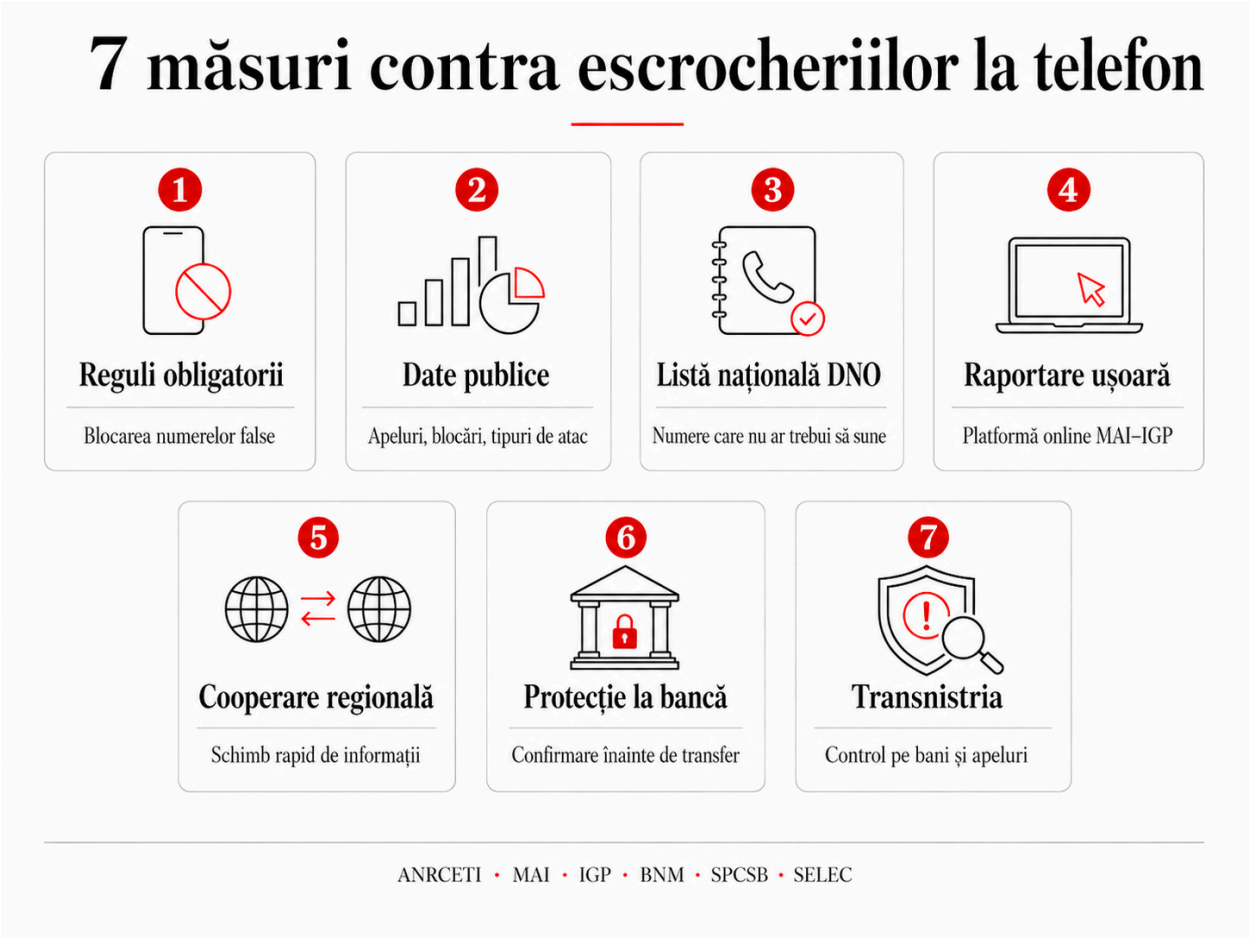
Ce s-a făcut și ce lipsește

Ofcom, autoritatea britanică de reglementare în comunicații, a raportat în iulie 2024 că BT (British Telecom) **blochează** un milion de apeluri suspecte zilnic. Procentul apelurilor frauduloase a scăzut de la 56% la 48% în doi ani. Mecanismul se numește STIR/SHAKEN și autentifică numeric originea fiecărui apel înainte de a-l conecta. Funcționează pe rețelele IP moderne; operatorii care rulează infrastructură mai veche de tip TDM/SS7 necesită mai întâi upgrade de rețea.

ANRCETI a publicat în august 2025 un Ghid detaliat pentru combaterea CLI Spoofing, falsificarea numărului afișat al apelantului, cu recomandări tehnice inclusiv STIR/SHAKEN, liste de blocare și un mecanism de validare a apelurilor internaționale. Problema nu este absența recomandărilor. Problema este că ghidul are caracter orientativ, implementarea rămâne la discreția fiecărui operator. **Niciun operator nu este obligat legal să blocheze nimic.**

Legea nr. 72/2025 privind comunicațiile electronice, în vigoare din ianuarie 2026, permite ANRCETI să impună blocarea apelurilor frauduloase. Normele de aplicare pentru această prevedere nu au fost adoptate.

Șapte măsuri recomandate



1. ANRCETI să transforme Ghidul CLI Spoofing din august 2025 în regulament obligatoriu, prin normele de aplicare ale Legii 72/2025. Cadrul legal există și ghidul tehnic există. Lipsește forța juridică.

2. ANRCETI să publice trimestrial, în format deschis, datele statistice colectate deja de la operatori privind apelurile frauduloase, număr de apeluri blocate, tipuri de atac, distribuție pe rețele. Mecanismul de colectare există prin Hotărârea Consiliului de Administrație ANRCETI nr. 36 din 1 octombrie 2024. Datele rămân interne.

3. ANRCETI să implementeze baza de date națională DNO (Do Not Originate, numere care nu ar trebui să inițieze niciodată apeluri), menționată în ghidul CLI Spoofing ca “în analiză”, și să o pună la dispoziția tuturor operatorilor în timp real. Fără o bază centralizată, fiecare operator menține propriile liste parțiale, fără coordonare.

4. MAI și IGP să creeze o platformă unificată de raportare online a fraudelor telefonice, cu statistici publice actualizate lunar. Campania “Stop Investițiilor False!” lansată în octombrie 2025 arată că există voință instituțională. Lipsește un sistem sistematic de colectare și publicare a datelor, comparabil cu Action Fraud din Marea Britanie.

5. Moldova să utilizeze canalele SELEC (Centrul pentru Aplicarea Legii în Europa de Sud-Est), organism în care este membră cu drepturi depline, pentru schimb sistematic de informații privind frauda telefonică. Cooperarea prin SELEC s-a concentrat până acum pe trafic de persoane și contrabandă. Frauda telefonică, cu creșteri de 59% pe an, justifică un grup de lucru dedicat în cadrul aceleiași structuri existente.

6. BNM (Banca Națională a Moldovei) să impună băncilor licențiate un protocol tehnic de verificare pentru transferurile de valoare ridicată inițiate în urma unui apel telefonic nesolicitat, confirmare pe canal independent (aplicație bancară sau SMS pe numărul înregistrat la bancă) înainte de executarea tranzacției. Schema „cont de siguranță” rămâne mecanismul central al fraudei telefonice documentate în Moldova: victima este convinsă să transfere banii pe un cont „protejat”. Un pas de confirmare pe canal separat întrerupe această schemă. Practica este standard în sistemul bancar european. BNM are competența de reglementare a serviciilor de plată. Nu necesită legislație nouă.

7. Zona transnistreană creează două vulnerabilități distincte: tranzit financiar și un unghi mort în autentificarea apelurilor. Pe latura financiară, SPCSB (Serviciul pentru Prevenirea și Combaterea Spălării Banilor) să includă explicit frauda telefonică printre categoriile de risc ridicat în evaluarea națională AML și să elaboreze, cu BNM (Banca Națională a Moldovei), protocoale de monitorizare a fluxurilor care tranzitează spațiul în care supravegherea bancară moldovenească nu se aplică. Pe latura telecom, problema este structurală: operatorul regional Interdnestrcom folosește planul moldovenesc de numerotare (+373), ceea ce face ca apelurile originate din rețeaua sa să apară ca apeluri domestice, invizibile pentru filtrele dedicate traficului internațional suspect. IDC a migrat la VoLTE (voce peste IP), ceea ce face tehnic posibilă autentificarea STIR/SHAKEN la punctul de interconectare. ANRCETI să includă în condițiile tehnice de interconectare, negociate prin Protocolul din 2017 cu Tiraspolul, obligativitatea marcării apelurilor originate din rețeaua IDC ca neautentificate de către operatorii moldoveni, și să includă plajele de numere IDC în baza de date DNO națională. Cadrul de negociere există din 2017.

În 2025, moldovenii au pierdut 211 milioane de lei în fraude online documentate oficial. Suma reală este mai mare: cea mai mare parte a victimelor nu raportează. Industria funcționează pentru că prinde mai rar decât operează. Moldova nu poate reglementa rețelele rusești sau ucrainene. Poate face ghidurile obligatorii, poate publica datele pe

care le are deja, poate construi o bază de numere blocate, poate crea un sistem de raportare și poate folosi o organizație în care e deja membră.

Surse: GI-TOC „Scammers' Paradise" (aprilie 2026); OCCRP „Scam Empire" (5 martie 2025); Eurojust (9 decembrie 2024); Europol operațiunea PANDORA (aprilie 2024); Mediazona (ianuarie 2025); FSB/TASS, Ministerul de Interne al Federației Ruse, Sberbank (2024); Sberbank „Investigation of Scam Call Centers' Operations", capitolul 2 (2021); FSIN, declarație publică (2021); adjunctul șefului poliției din Moscova (2021); The Moscow Times / The Record (9 decembrie 2024); DIICOT/IGP operațiunea TRICK (2023); IGP Moldova (mai 2026); IGP Moldova „Stop Investițiilor False!" (octombrie 2025); DFRLab (decembrie 2024); ANRCETI Ghid CLI Spoofing (august 2025); ANRCETI HCA nr. 36/01.10.2024; Ofcom (iulie 2024).